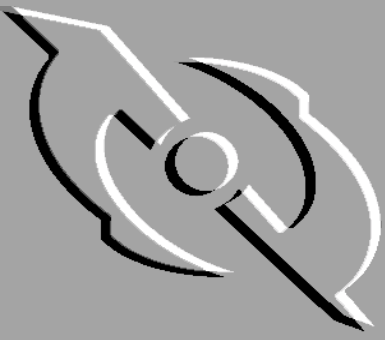


PGPwireless for Palm OS®

User's Guide

Version 2.0

PGPwireless for Palm OS*, Version 2.0

8-2001. Printed in the United States of America.

Network Associates, Inc.
3965 Freedom Circle
Santa Clara, CA 95054

(972) 308-9960 main
http://www.nai.com

LIMITED WARRANTY

Limited Warranty. Network Associates, Inc. warrants that the Software Product will perform substantially in accordance with the accompanying written materials for a period of sixty (60) days from the date of original purchase. To the extent allowed by applicable law, implied warranties on the Software Product, if any, are limited to such sixty (60) day period. Some jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you.

Customer Remedies. Network Associates, Inc.'s and its suppliers' entire liability and your exclusive remedy shall be, at Network Associates, Inc.'s option, either (a) return of the purchase price paid for the license, if any, or (b) repair or replacement of the Software Product that does not meet Network Associates, Inc.'s limited warranty and which is returned at your expense to Network Associates, Inc. with a copy of your receipt. This limited warranty is void if failure of the Software Product has resulted from accident, abuse, or misapplication. Any repaired or replacement Software Product will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer. Outside the United States, neither these remedies nor any product support services offered by Network Associates, Inc. are available without proof of purchase from an authorized international source and may not be available from Network Associates, Inc. to the extent they subject to restrictions under U.S. export control laws and regulations.

NO OTHER WARRANTIES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, AND EXCEPT FOR THE LIMITED WARRANTIES SET FORTH HEREIN, THE SOFTWARE AND DOCUMENTATION ARE PROVIDED "AS IS" AND NETWORK ASSOCIATES, INC. AND ITS SUPPLIERS DISCLAIM ALL OTHER WARRANTIES AND CONDITIONS, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, CONFORMANCE WITH DESCRIPTION, TITLE AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS, AND THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHERS, WHICH VARY FROM JURISDICTION TO JURISDICTION.

LIMITATION OF LIABILITY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL NETWORK ASSOCIATES, INC. OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL OR EXEMPLARY DAMAGES OR LOST PROFITS WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE PRODUCT OR THE FAILURE TO PROVIDE SUPPORT SERVICES, EVEN IF NETWORK ASSOCIATES, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ANY CASE, NETWORK ASSOCIATES, INC.'S CUMULATIVE AND ENTIRE LIABILITY TO YOU OR ANY OTHER PARTY FOR ANY LOSS OR DAMAGES RESULTING FROM ANY CLAIMS, DEMANDS OR ACTIONS ARISING OUT OF OR RELATING TO THIS AGREEMENT SHALL NOT EXCEED THE PURCHASE PRICE PAID FOR THIS LICENSE. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY, THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU.

Table of Contents

Preface

PGPwireless for Palm OS brings the encryption and authentication of PGP (Pretty Good Privacy) onto your handheld device.

Specifically, PGPwireless for Palm OS lets you:

- decrypt and verify encrypted text on your handheld (whether it got there via email, HotSync from your PC, or otherwise)
- encrypt, sign, or encrypt and sign plaintext you are going to send via email from your handheld or store on your handheld
- securely wipe sensitive data from your handheld so that it can never be retrieved
- encrypt the data from any application on your handheld, thus protecting it if your handheld is lost or stolen
- securely store important information in the Vault

PGPwireless for Palm OS can work as a standalone application on your handheld or in conjunction with PGP Corporate Desktop (on Windows PCs only), which allows you to easily move keys you have on your PC onto your handheld to use for encrypting, decrypting, and signing.

Using PGPwireless for Palm OS in conjunction with PGP on your PC also lets you view and edit the contents of the Vault on your PC.

IMPORTANT: Because the processors used in handhelds are limited in speed, you will get optimal performance of PGPwireless for Palm OS if you use 1024-bit RSA keys. Using larger keys will increase the time taken by PGP functions on your handheld.

Who should read this User's Guide

This User's Guide is for anyone who will be using PGPwireless for Palm OS on their handheld.

What we assume about you

We assume that you have sensitive data on your handheld and want it protected or that you are using email on your handheld and you want to have the security provided by PGP to protect your messages. We assume that you have a basic familiarity with PGP, but we will also explain everything that's going on.

This User's Guide

The chapters and appendices in this User's Guide are:

- Chapter 1, "Introducing PGPwireless for Palm OS," tells you about PGPwireless for Palm OS.
- Chapter 2, "Installation," tells you how to install PGPwireless for Palm OS onto your Windows PC and onto your handheld.
- Chapter 3, "Initial Setup," tells you how to get PGPwireless for Palm OS ready for use once it is installed.
- Chapter 4, "Moving keys onto your handheld," tells you how to get PGP keys onto your handheld so that PGPwireless for Palm OS can use them.
- Chapter 5, "Working with Keys," describes how to get properties of a key, beam a key, check a key's self signature, and delete a key.
- Chapter 6, "Using PGPwireless for Palm OS," tells you how to encrypt, decrypt, verify, and sign using PGPwireless for Palm OS.
- Chapter 7, "Wiping," tells you how to wipe sensitive data off of your handheld so that it cannot ever be retrieved.
- Chapter 8, "Database encryption," describes the database encryption feature, which lets you encrypt all of the data for specific applications on your handheld.
- Chapter 9, "Using the Vault," describes the Vault feature, which lets you securely store private data on your handheld, and tells you how to use it.
- Appendix A, "About PGPwireless for Palm OS," describes the About PGP screen.
- Appendix B, "Troubleshooting," describes some common PGPwireless for Palm OS problems and their solutions.

There is also a Glossary and an Index.

Resources

The following resources, in addition to this User's Guide, are available to help you understand your PGPwireless for Palm OS application, PGP, and cryptography in general:

- *An Introduction to Cryptography* is for anyone who wants to know about cryptography starting from the beginning. It is a high-level overview of the terminology, concepts, and processes used by PGP. It includes a chapter on security by PGP's creator, Phil Zimmermann. If you are using PGPwireless for Palm OS in conjunction with PGP Corporate Desktop, it was installed onto your Windows PC when PGP was installed.
- *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, copyright © 1999 by Simon Singh, Anchor Books. ISBN: 0-385-49532-3.
- *Secret and Lies: Digital Security in a Networked World*, copyright © 2000 by Bruce Schneier, John Wiley & Sons, Inc. ISBN: 0-471-25311-1.
- Search the Internet for "PGP," "cryptography," or "security."

How to contact PGP Security and Network Associates

Customer service

Network Associates continues to market and support the product lines from each of the new independent business units. You may direct all questions, comments, or requests concerning the software you purchased, your registration status, or similar issues to the Network Associates Customer Service department at the following address:

Network Associates Customer Service
4099 McEwen, Suite 500
Dallas, Texas 75244
U.S.A.

The department's hours of operation are 8 A.M. to 8 P.M. Central time, Monday through Friday.

Other contact information for corporate-licensed customers:

Phone:	(972) 308-9960
Email:	services_corporate_division@nai.com
Web:	http://support.nai.com/

Other contact information for retail-licensed customers:

Phone: (972) 308-9960

Email: cust_care@nai.com

Web: http://www.pgp.com/

Technical support

PGP Security and Network Associates are famous for their dedication to customer satisfaction. The companies have continued this tradition by making their sites on the World Wide Web valuable resources for answers to technical support issues.

PGP Security encourages you to make this your first stop for answers to frequently asked questions, for updates to PGP Security and Network Associates software, and for access to news and virus information.

Web: http://support.nai.com/

If the automated services do not have the answers you need, contact Network Associates at one of the following numbers Monday through Friday between 8 A.M. and 8 P.M. Central time to find out about Network Associates technical support plans.

For corporate-licensed customers:

Phone: (972) 308-9960

For retail-licensed customers:

Phone: (972) 855-7044

To provide the answers you need quickly and efficiently, the Network Associates technical support staff needs some information about your computer and your software.

Please include the following information in your correspondence:

- Program name and version number
- Computer brand and model
- Any additional hardware or peripherals connected to your computer
- Operating system type and version numbers
- Network name, operating system, and version
- Network card installed, where applicable
- Modem manufacturer, model, and bits-per-second rate, where applicable

- Relevant browsers or applications and their version numbers, where applicable
- How to reproduce your problem: when it occurs, whether you can reproduce it regularly, and under what conditions
- Information needed to contact you by voice, fax, or email

Download support

To get help with navigating or downloading files from the Network Associates Web sites or FTP sites, call:

Corporate customers	(801) 492-2650
Retail customers	(801) 492-2600

Network Associates training

For information about scheduling on-site training for any PGP Security or Network Associates product, call Network Associates Customer Service at (972) 308-9960.

Comments and feedback

PGP Security appreciates your comments and reserves the right to use any information you supply in any way it believes appropriate without incurring any obligation whatsoever. Please send any documentation comments to **pgpdocs@nai.com**.

Introducing PGPwireless for Palm OS 1

This chapter is an overview of the PGPwireless for Palm OS product.

What is PGPwireless for Palm OS?

PGPwireless for Palm OS is an application that runs on handheld devices that run Palm OS 3.1 or greater. It brings the security of PGP (Pretty Good Privacy) to your handheld.

PGPwireless for Palm OS works in one of two ways: in conjunction with PGP on your PC (Windows only) or standalone.

Using either method, you can:

- decrypt and verify PGP-encrypted text—so you can read PGP-encrypted email messages on your handheld knowing they haven't been tampered with
- encrypt, sign, or sign and encrypt text on your handheld—so you can communicate from your handheld with security.
- wipe data on the Clipboard or any Memo Pad record, wipe the data in the Vault, and wipe free memory on the handheld—so the data you want deleted won't ever come back
- encrypt all of the data for specific applications on your handheld—the data cannot be accessed without the passphrase, thereby protecting your data in the event your handheld is lost or stolen
- securely store important information in the Vault—so your private data is always private, even if your handheld is lost or stolen

The advantages to using PGPwireless for Palm OS in conjunction with PGP on your Windows PC are that:

- getting PGP keys onto your handheld is easier
- you can view and edit the data in your Vault on your PC

The advantage to using PGPwireless for Palm OS standalone is that:

- you can install it from platforms other than Windows; Macintosh and Linux, for example

Where does the text come from?

PGPwireless for Palm OS can operate on any editable text that you can get onto your handheld.

Ways of getting editable text onto your handheld include:

- receiving it via a modem or wireless connection
- moving it onto your handheld during a HotSync
- entering it yourself

The only requirement for the text is that it is editable; that is, that you can select it and cut, copy, and paste it (not that you have to do this with email messages, for example, but it must be possible).

Supported algorithms

PGPwireless for Palm OS supports the following algorithms:

- RSA
- DSS
- Diffie-Hellman (ElGamal)
- The new AES algorithm, Rijndael
- CAST
- IDEA
- TripleDES
- SHA-1
- MD5

PGPwireless for Palm OS does ***not*** support the Twofish algorithm.

Supported hardware platforms

PGPwireless for Palm OS is hardware independent; that is, it will run on any handheld that runs Palm OS 3.1 or greater.

Handhelds that run Palm OS 3.1 or greater include all Palm handhelds, Handspring's Visor, Sony's CLIÉ, and Kyocera Wireless Corp.'s pdQ Smartphone (formerly from Qualcomm).

Compatibility notes

There are a few applications that run on the Palm OS that don't fully support PGPwireless for Palm OS.

NOTE: Because of its quality, widespread use, and its compatibility with PGPwireless for Palm OS, we recommend using MultiMail Pro, developed by Actual Software (www.actualsoft.com), a part of Palm, Inc. (www.palm.com).

Applications that don't fully support PGPwireless for Palm OS include:

- Web-clipping-based applications—based on limitations imposed by the Web-clipping framework, PGPwireless for Palm OS is not compatible with these applications.
- Eudora for Palm—this application prevents the PGP Popup menu from directly grabbing or inserting text into its messages. To use this application you must encrypt or decrypt the text on the Clipboard and then paste it into Eudora for Palm. Also, when copying incoming messages to the Clipboard, Eudora for Palm truncates messages at 1000 bytes without notifying you. Please contact Qualcomm for any updates to fix these bugs.
- Palm OS Mail—the conduit supplied by Palm for synchronizing the desktop email client with the Mail application on the Palm removes line endings from transferred messages. Any PGP encrypted and/or signed messages transferred using this conduit will be corrupted.
- Applications based on the Palm OS Mail interface—applications that copy their user interface from the basic Palm OS Mail application (including Mail, iMessenger, Corsoft Aileron, and Osmail, to name a few) do not allow the PGP Popup menu to directly grab the text of incoming messages. To get around this, copy the text to the Clipboard and then use the PGPwireless for Palm OS Clipboard capabilities on it. For incoming messages that are too big to copy to the Clipboard, "reply" to the message (which copies the text to a new window) and then use the PGP popup menu to grab the text from the reply.
- Limited-size text fields—some text fields in applications that run on the Palm OS have size limitations (for example, entries in the To Do application cannot exceed 255 characters). Encrypting text in fields with size limitations, even though the text is under the limitation before encryption, can result in encrypted text that exceeds the limitation. The only solution is to make the text smaller or break it into two or more fields.

Installation 2

This chapter tells you how to install the PGPwireless for Palm OS application onto your handheld and how to install the conduit needed to use PGPwireless in conjunction with PGP on your Windows PC. It also tells you how to update from a previous version of PGPwireless for Palm OS to version 2.0. It starts off with PGPwireless system requirements.

PGPwireless for Palm OS is distributed as a Zip file. It includes the following:

- the PGPwireless.prc file: needed to install PGPwireless for Palm OS onto your handheld, whether you are going to be using PGPwireless standalone or in conjunction with PGP on your Windows PC
- the PGPwirelessWindowsConduit application: needed to install the conduit for using PGPwireless in conjunction with PGP on your Windows PC
- the PGPwireless for Palm OS User's Guide: a PDF file of this document
- the ReadMe file: includes last minute information about PGPwireless
- the License file: includes information about how you can legally use PGPwireless

System requirements

PGPwireless for Palm OS installs onto your handheld, and you can also install the conduit needed to use PGPwireless in conjunction with PGP on your PC:

- To install PGPwireless for Palm OS onto your handheld, you must have Palm OS 3.1 or greater (3.5 or greater to use the new database encryption feature) and at least 220 KB of free memory on your handheld for the PGPwireless for Palm OS application.
- To install the conduit onto a Windows PC (so that you can use PGPwireless in conjunction with PGP on your Windows PC), you must have your Palm desktop software and PGP Desktop Security 7.0.1 or greater or PGP Corporate Desktop 7.1 or greater already installed.

NOTE: If you have individual PGP products installed, you must have PGPmail, PGPdisk, or PGPvpn installed; PGPwireless for Palm OS will not work on conjunction with PGP on your Windows PC if you only have PGPfire installed.

Installing for use with PGP

If you are going to use PGPwireless for Palm OS in conjunction with PGP on your Windows PC, you need to run the PGPwirelessWindowsConduit application on the PC (it installs the PGPwireless for Palm OS conduit and adds two menu items to PGPkeys) and then install the PGPwireless.prc file onto your handheld.

NOTE: If you plan to use PGPwireless for Palm OS in conjunction with PGP, you must install PGP 7.0.1 or greater onto your PC ***before*** you install PGPwireless for Palm OS.

To install the PGPwireless for Palm OS desktop software:

1. Extract the files from the **PGPwirelessforPalmOS.zip** file to a known location on your computer.
2. Double click the **PGPwirelessWindowsConduit.exe** application.
3. Follow the on-screen instructions.
4. When the installation is complete, click **Finish**.
5. Move the **PGPwireless.prc** file to the Add-on folder in the Palm folder on your computer, then open the Palm desktop software on your computer and use the Install tool to specify that **PGPwireless.prc** should be installed onto your handheld when you next perform a HotSync.

   (Another way to do this is to double click the **PGPwireless.prc** file.)
6. Put your handheld is in its cradle.
7. Make sure your HotSync software is active.
8. Press the HotSync button on the cradle.
9. When the synchronization process is complete, remove your handheld from its cradle and read the message:

   If the message says you need to reset your handheld, the HotSync was successful. Tap the **Reset** button.

   If the message says that the HotSync failed, read the Log file and refer to Appendix B, “Troubleshooting,” for more information.
10. When your handheld resets, return the handheld to its cradle.
11. Press the HotSync button on the cradle again.

A second HotSync is needed to take the time zone information from your desktop and move it onto your handheld. Refer to "Time zone" on page 25 for more information.

12. When the synchronization process is complete, PGPwireless for Palm OS is ready for use.

Installing for standalone use

The following procedure describes how to install the PGPwireless.prc file onto your handheld. If you need more information, please refer to the documentation that came with your handheld.

To install PGPwireless for Palm OS for standalone use:

1. Extract the files from the **PGPwirelessforPalmOS.zip** file to a known location on your computer.
2. Move the **PGPwireless.prc** file to the Add-on folder in the Palm folder on your computer, then open the Palm desktop software on your computer and use the Install tool to specify that **PGPwireless.prc** should be installed onto your handheld when you next perform a HotSync.

   (Another way to do this is to double click the **PGPwireless.prc** file.)
3. Put your handheld is in its cradle.
4. Make sure your HotSync software is active.
5. Press the HotSync button on the cradle.
6. When the synchronization process is complete, remove your handheld from its cradle and read the message:

   If the message says you need to reset your handheld, the HotSync was successful. Tap the **Reset** button.

   If the message says that the HotSync failed, read the Log file and refer to Appendix B, "Troubleshooting," for more information.

   When your handheld resets, the PGPwireless for Palm OS application is installed and ready for use.

Upgrading

Upgrading PGPwireless for Palm OS from a previous version to version 2.0 is slightly different depending on whether you were using PGPwireless in conjunction with PGP on your Windows PC or standalone.

IMPORTANT: You ***must*** install the version 2.0 **PGPwireless.prc** file over the existing version of the **PGPwireless.prc** file on your handheld. If you uninstall PGPwireless for Palm OS from your handheld, your keys and your Vault data will be deleted, making conversion impossible.

This section describes both upgrade procedures.

WARNING: Do ***not*** install older versions of PGPwireless for Palm OS over version 2.0. You risk the loss of your existing PGP data.

Upgrading when used in conjunction with PGP

If you were using your previous version of PGPwireless for Palm OS in conjunction with PGP on your Windows PC, your keys and Vault data will be automatically converted when you upgrade to version 2.0.

To upgrade to version 2.0 when used in conjunction with PGP:

1. Perform a HotSync so that your most recent data is backed up on your computer.
2. Uninstall the PGPwireless Windows Conduit application from your PC.
3. Extract the files from the **PGPwirelessforPalmOS.zip** file to a known location on your computer.
4. Move the **PGPwireless.prc** file to the Add-on folder in the Palm folder on your computer, then open the Palm desktop software on your computer and use the Install tool to specify that **PGPwireless.prc** should be installed onto your handheld when you next perform a HotSync.

   (Another way to do this is to double click the **PGPwireless.prc** file.)
5. Perform a HotSync. (This installs PGPwireless 2.0 onto your handheld.)
6. Reset your handheld, then open PGP on your handheld and make sure your data was correctly converted.
7. Double click the **PGPwirelessWindowsConduit.exe** application.

8. Follow the on-screen instructions.
9. When the installation is complete, click **Finish**.
10. Perform another HotSync. (This backs up your converted data to your PC.)

Upgrading when used standalone

If you were using your previous version of PGPwireless for Palm OS standalone, your keys and Vault data will be automatically converted when you upgrade to version 2.0.

To upgrade to PGPwireless for Palm OS version 2.0:

1. If you were using a third-party backup program, use it to back up your data.
2. Extract the files from the **PGPwirelessforPalmOS.zip** file to a known location on your computer.
3. Move the **PGPwireless.prc** file to the Add-on folder in the Palm folder on your computer, then open the Palm desktop software on your computer and use the Install tool to specify that **PGPwireless.prc** should be installed onto your handheld when you next perform a HotSync.

   (Another way to do this is to double click the **PGPwireless.prc** file.)
4. Perform a HotSync. (This installs PGPwireless 2.0 onto your handheld.)
5. Reset your handheld, then open PGP on your handheld and make sure your data was correctly converted.

Initial Setup 3

The first thing you should do once the PGPwireless for Palm OS application is installed on your handheld is to configure your preferences.

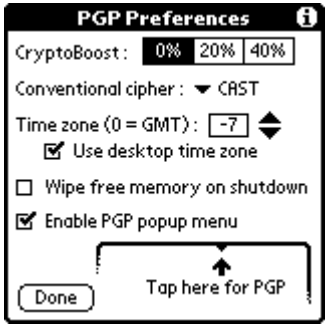
Displaying preferences

PGPwireless for Palm OS preferences let you decide whether to use overclocking, select the cipher algorithm that will be used for conventional encryption and encrypting the Vault, establish your time zone, automatically wipe free memory, and control the PGP popup menu.

To display PGPwireless for Palm OS preferences:

1. With PGPwireless for Palm OS open, tap the **Menus** icon .
2. When the menus display, tap **Options**.
3. Tap **Preferences**.

   The PGP Preferences screen appears.



   The following sections describe each preference.

4. When you have finished making your selections, tap **Done**.

> **NOTE:** If you are using PGPwireless for Palm OS in conjunction with PGP on your Windows PC, and you have HotSynced at least once since you installed PGPwireless, then a checkbox called **Use desktop time zone** appears under the Time zone field. Otherwise, this checkbox is hidden.

CryptoBoost

The CryptoBoost feature can speed up some PGPwireless for Palm OS operations by overclocking your handheld's CPU.

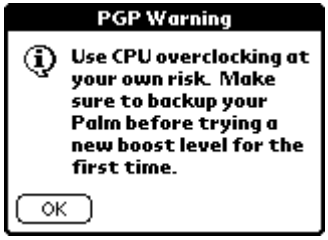
WARNING: Overclocking works well on most handhelds, but some devices cannot be overclocked (the Palm m505, for example). Enabling CryptoBoost (it is off by default) can result in unexpected operation of PGPwireless for Palm OS and, in rare instances, may potentially cause damage to your handheld. Symptoms that your handheld is not compatible with CryptoBoost include: lockups, fatal errors, and unusual lines on the screen during PGP operations. If you see these problems while using PGPwireless for Palm OS, reset your handheld and then turn CryptoBoost off. Also, use of CryptoBoost is not recommended if you are already using other overclocking software on your handheld.

To use CryptoBoost:

1. On the PGP Preferences screen, tap either the **20%** or the **40%** box.

   The box you tapped highlights.

   When you exit from Preferences, a warning message will appear.



2. Read the message and tap **OK**.

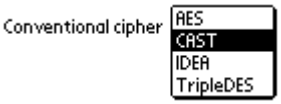
Conventional cipher

The conventional cipher preference lets you specify which cipher algorithm will be used for conventional encryption operations, for encrypting the Vault, and for the database encryption feature. Your options are: AES (Rijndael), CAST (the default), IDEA, or TripleDES.

To select a conventional cipher:

1. On the PGP Preferences screen, tap the triangle next to the active cipher algorithm.

   The list of ciphers appears.



2. Tap the cipher you want to be active.

Time zone

Because PGPwireless for Palm OS time stamps certain operations, it needs to know what time zone you are in, relative to Greenwich Mean Time (GMT).

If you are using PGPwireless for Palm OS in conjunction with PGP on your Windows PC, you can have PGPwireless automatically retrieve the time zone information from your PC.

NOTE: If you are using Palm OS 4.0 or later, the **Use desktop time zone** checkbox does not display. Instead, PGPwireless for Palm OS uses the time zone information set in the Palm OS preferences.

To do this, simply do another HotSync ***after*** the PGPwireless for Palm OS application has been installed on your handheld.

When you do this, the **Use desktop time zone** checkbox appears on the PGP Preferences screen and the time zone information from your PC will be active.

If you are using PGPwireless for Palm OS standalone (that is, not in conjunctions with PGP on your Windows PC), you need to enter the appropriate time zone information yourself.

Time zone offsets to the west of Greenwich are expressed as negative numbers of hours; for example, New York is -5. Time zone offsets to the east are expressed as positive numbers of hours: for example, Tokyo is +9.

To set your time zone offset:

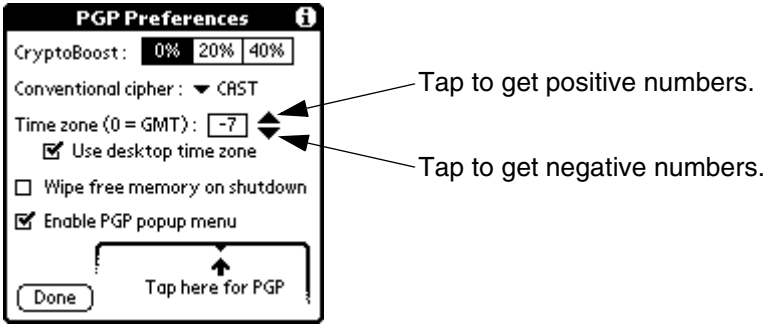
1. Use the table below to determine your time zone offset.

   The following table lists the time zone offsets for many cities worldwide.

Honolulu: -10	Vancouver: -8	Los Angeles: -8
Calgary: -7	Chicago: -6	Mexico City: -6
New York: -5	Bogota: -5	Quebec: -5
Brasilia: -3	London: 0	Casablanca: 0
Paris: +1	Lagos: +1	Rome: +1
Cape Town: +2	Jerusalem: +2	Cairo: +2
Moscow: +3	Riyadh: +3	Islamabad: +5
Calcutta: +5.5	Saigon: +7	Singapore: +8
Tokyo: +9	Vladivostok: +10	Sydney: +10

NOTE: These offsets are for standard time. If daylight savings time is in effect where you live, your offset will be one hour different. For example, during daylight savings time in Los Angeles, the offset is -7 instead of -8. Adjust as necessary for your location.

2. On the PGP Preferences screen, on the triangles next to the **Time Zone** box, tap the top triangle for positive numbers and the bottom triangle for negative numbers.



3. Continue tapping until you reach the correct offset for your location.

Wipe free memory on shutdown

PGPwireless for Palm OS lets you automatically wipe your handheld's free memory on shutdown, thereby protecting against any chance that fragments of sensitive data left in free memory will be retrievable.

If you decide to automatically wipe your free memory on shutdown, you will see the PGP Progress screen telling you that free memory is being wiped every time you press the Power button to turn your handheld off.

- **To automatically wipe free memory on shutdown:** On the PGP Preferences screen, make sure there is a checkmark next to **Wipe free memory on shutdown**.
- **To disable wiping of free memory on shutdown:** On the PGP Preferences screen, clear the checkmark next to **Wipe free memory on shutdown**.

NOTE: You can wipe your handheld's free memory at any time whether or not you are automatically wiping it on shutdown. To do this, open the Wipe menu and select **Free memory**. For more information, refer to "Wiping free memory" on page 50.

Enable PGP popup menu

The PGP popup menu gives you quick access to PGPwireless for Palm OS functions without having to open the application. It is enabled by default.

The hotspot for activating the PGP popup menu is the top division mark in the Graffiti writing area.

- **To enable the PGP popup menu:** On the PGP Preferences screen, make sure there is a checkmark next to **Enable PGP popup menu**.
- **To disable the PGP popup menu:** On the PGP Preferences screen, clear the checkmark next to **Enable PGP popup menu**.

Moving keys onto your handheld 4

Having PGP keys available in PGPwireless for Palm OS lets you use them for encrypting, decrypting, verifying, and signing.

There are three ways you can get PGP keys onto your handheld:

- If you are using PGPwireless for Palm OS in conjunction with PGP on your Windows PC, you can move your PGP keys onto your handheld using the PGPkeys application.
- You can import your PGP keys as text files.
- You can beam PGP keys onto your handheld from another PGPwireless for Palm OS user.

NOTE: We recommend removing unnecessary user IDs and signatures from a key before you move it onto your handheld. This keeps the size of the key to a minimum, saving space on your handheld. And if you are importing a key, the smaller size reduces the chance that the text of the key will be truncated by the Clipboard's 1Kb or Memo Pad record's 4Kb size limitation.

The following sections describe these methods.

IMPORTANT: Because the processors used in handhelds are limited in speed, you will get optimal performance of PGPwireless for Palm OS if you use 1024-bit RSA keys. Using larger keys will increase the time PGP functions take on your handheld.

Moving keys onto your handheld using PGPkeys

The following procedure tells you how to move PGP keys onto your handheld using the PGPkeys application on your Windows PC.

To move PGP keys onto your handheld using PGPkeys:

1. On your PC, open PGPkeys.

   The PGPkeys window appears.

2. Pull down the **File** menu and select **Open PGPwireless for Palm OS Keyring**.

   The PGPwireless for Palm OS Keyring window appears.

3. Position the two windows so that you can see both.

4. Drag the keys you want to be on your handheld from the PGPkeys window to the PGPwireless for Palm OS Keyring window.

5. Close both windows

6. Perform a HotSync.

7. Open PGPwireless for Palm OS on your handheld.

   The keys you dragged to the PGPwireless for Palm OS Keyring window appear. They are ready to be used.

Importing keys

If you are using PGPwireless for Palm OS standalone; that is, not in conjunction with PGP on your Windows PC, then the easiest way to get PGP keys onto your handheld is by importing them as text and using the Import command on them.

This lets you import PGP keys from all platforms (Windows, Macintosh, and Linux, for example) as well as keys from OpenPGP-compliant applications (like GnuPG).

The general procedure is simple:

1. Move the key (or keys), as text, onto your handheld.

2. Use the Import command (Tools menu, Import from Memo or Import from Clipboard commands) or the PGP popup menu (PGP Import selection) to import the key(s).

3. Check the key (Key Properties screen, Check button) to make sure it passes the self-signature check.

   This isn't actually part of the import process, but you should always check a new key as soon as you bring it onto your handheld.

NOTE: We recommend removing unnecessary user IDs and signatures from a key before you move it onto your handheld. This keeps the size of the key to a minimum, saving space on your handheld. It also reduces the chance that the text of the key will be truncated by the Clipboard's 1Kb or Memo Pad record's 4Kb size limitation.

Let's look at some examples of how you can import keys:

- Import a public key using a Memo Pad record
- Import a public key using email and the PGP popup menu
- Import a private key

Importing a public key using a Memo Pad record:

1. Open the Palm desktop software and PGPkeys on your computer.
2. In PGPkeys, select the key you want to move to your handheld, then pull down the Edit menu and select **Copy**.

> **NOTE:** You can move multiple public keys (make sure not to select a private key) simply by selecting them all in this step. Keep in mind that if you select too many keys at one time, the text may be truncated when it gets on your handheld and so none of the keys will be usable.

3. In your Palm desktop software, create a new Memo Pad record, then pull down the Edit menu and select **Paste**.

   The text of the public key block is inserted into the Memo Pad record.

4. In your Palm desktop software, pull down the File menu and select **Save**.

   The Memo Pad record with the public key block is saved.

5. Exit from your Palm desktop software and from PGPkeys.
6. Perform a HotSync. Make sure the Memo Pad conduit is set to **Synchronize the files** or **Desktop overwrites handheld**.
7. On your handheld, open PGPwireless for Palm OS.
8. Tap the Menus icon, then select **Import from Memo** from the Tools menu.
9. On the Select Memo screen, tap the record labelled ----BEGIN PGP PUBLIC KEY BLOCK----, then tap **OK**.
10. On the PGP screen, tap **OK** to import the key.
11. On the PGP Warning screen, tap **OK**.
12. On the Key Properties screen, tap **Check**.
13. When the key passes the self-signature check, tap **OK**. The Keys screen appears, showing the key you just imported.

If the key fails the self-signature check, you should delete it. For more information, refer to "Checking a key's self signature" on page 39.

Importing a public key using email and the PGP popup menu:

1. Open your email application and PGPkeys on your computer.
2. In your email application, open a new message and address it.
3. In PGPkeys, select the key you want to move to your handheld, then pull down the Edit menu and select **Copy**.

NOTE: You can move multiple public keys (make sure not to select a private key) simply by selecting them all in this step. Keep in mind that if you select too many keys at one time, the text may be truncated when it gets on your handheld and so none of the keys will be usable.

---

4. In your email application, put the insertion point into the body of your message, pull down the Edit menu, and select **Paste**.

   The text of your public key block is pasted into the message.

5. Send the message.
6. Pick up the message with your public key block in it on your handheld, open it, tap the PGP popup menu, then tap **PGP Import selection**.
7. On the PGP screen, tap **Yes** to import the key.

   The email message displays.

8. Exit from your email program and then open PGPwireless for Palm OS. The new key will be listed with any other keys you already had on your handheld.
9. Tap the new key.
10. On the PGP Warning screen, click **OK**.
11. On the Key Properties screen, tap **Check**.
12. When the key passes the self-signature check, tap **OK**. The Keys screen appears, showing the key you just imported.

    If the key fails the self-signature check, you should delete it. For more information, refer to "Checking a key's self signature" on page 39.

Because losing a private key is such a breach of security, it's intentionally harder to get them out of PGP than it is to get public keys. Specifically, you must use the Export command and export your private key to a file instead of just cutting and pasting it, like you can do with public keys.

IMPORTANT: Only export one private key at a time! PGPwireless may fail to import correctly if multiple keys are exported.

The following procedure takes you through the process.

Importing a private key using a Memo Pad record:

1. Open the Palm desktop software and PGPkeys on your computer.
2. In PGPkeys, select the private key you want to move to your handheld, then pull down the Keys menu and select **Export**.

   Make sure to select only ***one*** private key!
3. On the Export Keys to File screen, select a name and a location for the ASCII key file, and *make sure* to check the **Include private key(s)** checkbox.

   This checkbox is not checked by default, and if you forget to do it, the private portion of the key will ***not*** be exported.
4. Open the ASCII key file using a text editor and copy the entire text of the file. As you can see, the public and the private parts of the key have their own sections.
5. In the Palm desktop software, open a new Memo Pad record and paste the text of the ASCII key file into it, then save the Memo Pad record.
6. Exit from your Palm desktop software and from PGPkeys.
7. Perform a HotSync. Make sure the Memo Pad conduit is set to **Synchronize the files** or **Desktop overwrites handheld**.
8. On your handheld, open PGPwireless for Palm OS, tap the Menus icon, and select **Import from Memo** from the Tools menu.
9. On the Select Memo screen, tap the record labelled ----BEGIN PGP PRIVATE KEY BLOCK----, then tap **OK**.
10. On the PGP screen, tap **OK** to import the key.
11. On the PGP Warning screen, tap **OK**.
12. On the Key Properties screen, tap **Check**.

13. When the key passes the self-signature check, tap **OK**. The Keys screen appears, showing the key you just imported. The name of the key should be bold, indicating that the private part of the key was successfully imported.

    If the key fails the self-signature check, you should delete it. For more information, refer to "Checking a key's self signature" on page 39.

Beaming keys onto your handheld

If you know someone who is also using PGPwireless for Palm OS on their handheld, you can beam public keys onto their handheld from yours. And vice versa; they can beam public keys from their handheld to yours.

NOTE: You cannot beam your ***private*** key to another handheld. You can, however, beam the public portion of your private key to someone else. Just beam your key; the private portion will ***not*** be beamed, only the public portion will.

Beaming a key is a one-way process. You can beam to another handheld, and another handheld can beam to you, but not both at the same time. Also, you can beam only one key at a time.

Beaming keys between different versions of PGPwireless for Palm OS is also allowed, with one exception:

- You can beam from version 1.0 to version 1.5 or 2.0
- You can beam from version 1.5 to version 2.0
- You can beam from version 2.0 to version 1.5
- You ***cannot*** beam from version 1.5 or 2.0 to version 1.0

NOTE: The PGPwireless for Palm OS application must be running on the handheld that is *receiving* the beamed key. If it is not the active application, a message will display telling you that you need to run PGPwireless for Palm OS in order to receive beamed keys.

To beam a key to another handheld:

1. On the PGPwireless for Palm OS screen, tap the key you wish to beam.

   The Key Properties screen appears for the key you tapped.

2. Point the IR port of your handheld directly at the IR port of the other handheld.

   Generally speaking, the handhelds should be from four to 36 inches apart, with no obstacles in between. For details, consult your handheld's documentation.

3. Tap **Beam**.

   The Beam dialog appears.

   When the beam is done, the PGPwireless for Palm OS screen appears.

   On the other handheld, the Beam dialog opens when the beam is received, and the user is prompted as to whether or not they want to receive the beamed key.

4. Tap **Yes** to accept the key.

   The Key Properties screen for the new key appears.

Working with Keys 5

This chapter tells you some things you can do with PGP keys on your handheld other than encrypt, sign, or decrypt and verity text. You can:

- view the Key Properties screen for a key
- beam a public key to another PGPwireless for Palm OS user
- check a key's self signature
- delete a key

NOTE: User IDs and signatures on keys take up extra memory on your handheld. If you are concerned about saving memory on your handheld, consider using PGPkeys on your Windows PC to remove unnecessary User IDs and signatures from the keys you bring onto your handheld.

Unlike desktop versions of PGP, PGPwireless for Palm OS only performs partial checking of the integrity of the public and private keys on its keyring. If you are concerned that the keys on your handheld have been compromised, you can:

- upload the keys to your Windows PC (using the "Handheld overwrites Desktop" setting in the HotSync Manager) and run PGPkeys to verify the keys on your handheld.
- overwrite the keys on your handheld with known verified copies from PGP on your Windows PC by selecting "Desktop overwrites Handheld" in the HotSync Manager.
- perform a self-signature check ("Checking a key's self signature" on page 39) on each suspect key. If the key passes the self-signature check, verify the fingerprint of the key with a known good copy.

The Key Properties screen

The first thing you can tell about a PGP key in PGPwireless for Palm OS is whether it is a private or a public key: private keys are shown in bold text on the PGPwireless for Palm OS screen, while public keys are shown in normal text.

More information about a key is available on the Key Properties screen, which you can display simply by tapping the key you want information about on the PGPwireless for Palm OS screen.

To get information about a key:

1. On the PGPwireless for Palm OS Keys screen, tap the key you want more information about.

   The Key Properties screen appears.

2. Tap **Done** when you are finished.

   The information about a key on the Key Properties screen includes:

   - The key's name
   - The key's fingerprint, in hexadecimal format
   - The key's identification number (Key ID)
   - The key's type
   - The key's size
   - The key's creation date
   - The key's expiration date
   - The key's cipher preferred algorithm

Beaming

If you know someone who is also using PGPwireless for Palm OS on their handheld, you can beam public keys onto their handheld from yours. And vice versa; they can beam public keys from their handheld to yours.

NOTE: You cannot beam your ***private*** key to another handheld. You can, however, beam the public portion of your private key to someone else. Just beam your key; the private portion will ***not*** be beamed, only the public portion will.

Beaming a key is a one-way process. You can beam to another handheld, and another handheld can beam to you, but not both at the same time. Also, you can beam only one key at a time.

Beaming keys between different versions of PGPwireless for Palm OS is also allowed, with one exception:

- You can beam from version 1.0 to version 1.5 or 2.0
- You can beam from version 1.5 to version 2.0
- You can beam from version 2.0 to version 1.5
- You ***cannot*** beam from version 1.5 or 2.0 to version 1.0

NOTE: The PGPwireless for Palm OS application must be running on the handheld that is *receiving* the beamed key. If it is not the active application, a message will display telling you that you need to run PGPwireless for Palm OS in order to receive beamed keys.

To beam a key to another handheld:

1. On the PGPwireless for Palm OS screen, tap the key you wish to beam.

   The Key Properties screen appears for the key you tapped.

2. Point the IR port of your handheld directly at the IR port of the other handheld.

   Generally speaking, the handhelds should be from four to 36 inches apart, with no obstacles in between. For details, consult your handheld's documentation.

3. Tap **Beam**.

   The Beam dialog appears.

   When the beam is done, the PGPwireless for Palm OS screen appears.

   On the other handheld, the Beam dialog opens when the beam is received, and the user is prompted as to whether or not they want to receive the beamed key.

4. Tap **Yes** to accept the key.

   The Key Properties screen for the new key appears.

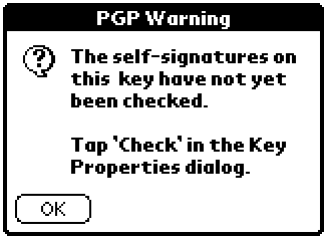
Checking a key's self signature

PGP automatically and transparently checks the self signatures of keys when you import them. However, with PGPwireless for Palm OS, you won't necessarily be getting keys that have been checked; instead, you could have imported the key (refer to "Importing keys" on page 28) or beamed the key (refer to "Beaming" on page 37).

In these cases, it is extremely important that you check the self signatures of these keys on your handheld ***before*** you use them. When a key passes the self-signature check, it assures you that the key has not been tampered with or corrupted since it was generated. In other words, the key is intact.

NOTE: Once a key has passed the self-signature check, and you therefore know it is intact, you should then check its fingerprint to make sure that it is authentic; that is, it really came from the person or entity that it purports to be from.

Because it is important to do the self-signature check of a key before you use it, PGPwireless will display a warning message if you try to use a key before the self signature has been checked.



To check the self signature of a key:

1. On the PGPwireless for Palm OS Keys screen, tap the key whose self signature you want to check.

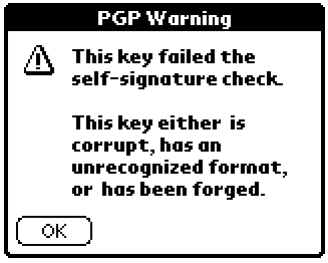
The Key Properties screen appears for the key you tapped.

2. Tap **Check**.

   The PGP Progress dialog appears.

   If the key passes the self-signature check, the PGP screen appears.

   If the key fails the self-signature check, the PGP Warning screen appears.



   If a key fails the self-signature check, you should delete it.

3. Tap **OK**.

   The Keys screen appears.

Deleting

If you no longer need a particular PGP key on your handheld, you can delete it.

To delete a key:

1. On the PGPwireless for Palm OS screen, tap the key you wish to delete.

   The Key Properties screen appears for the key you tapped.

2. Tap **Delete**.

   A dialog box displays, asking you to confirm the deletion.

3. Tap **OK**.

   The key is deleted from your handheld and the Keys screen appears.

Using PGPwireless for Palm OS 6

This chapter describes the core PGPwireless functionality: decrypting and verifying, encrypting, signing, and encrypting and signing.

You can do all of these things to email messages, and you can do all of them to text on the Clipboard or in a Memo Pad record.

NOTE: During the procedures in this chapter you may be asked to tap in a box on your handheld to provide random data. This random data is needed to make sure your data is completely safe. You should only have to do this once after your handheld is reset.

Decrypting and Verifying

Decrypting and verifying is the process of unencrypting PGP-encrypted text (in an email message, for example) using either conventional or public-key encryption, then verifying that the text wasn't modified since it was encrypted.

A quick overview of conventional and public-key encryption:

- With **conventional encryption**, both the person doing the encryption and the person doing the decryption use the same passphrase; the encryptor when she is encrypting the message, the decryptor when he is decrypting the message. Naturally, the encryptor needs some way of communicating the passphrase to the decryptor.
- With **public-key encryption**, the encryptor first gets the public key of the person they are sending the message to and then they encrypt the message using that public key. The decryptor uses their private key (mathematically linked to the public key, but not the same) to decrypt the message. With public-key encryption, the task of communicating the passphrase is not needed.

PGPwireless for Palm OS knows whether encrypted text was encrypted with conventional or public-key encryption. If the former, it prompts you for the passphrase; if the latter, it checks your handheld for the private key the message was encrypted to using the corresponding public key.

Decrypting and verifying text

The following procedure tells you how to decrypt and verify text on your handheld.

To decrypt and verify text on your handheld:

1. Access the text you wish to decrypt and verify:

   If the text is an email message: On your handheld, open the email message, tap the PGP popup menu, then tap **PGP Decrypt/Verify selection**. If the text was encrypted using public-key cryptography, the key it was encrypted to is displayed; click **Decrypt**. If the text was encrypted using conventional cryptography, the screen tells you it was encrypted to a passphrase; click **Decrypt**.

   NOTE: Although all of the text of the message is selected, not just the PGP-encrypted text, PGPwireless for Palm OS knows to decrypt just the encrypted text; it won't try to decrypt the other parts of the message.

   If the text is in a Memo Pad record: In PGPwireless for Palm OS, tap the Menus icon, select **Decrypt/Verify Memo** from the Tools menu, tap the Memo Pad record you want to decrypt/verify on the Select Memo screen, then click **OK**. If the text was encrypted using public-key cryptography, the key it was encrypted to is displayed; click **Decrypt**. If the text was encrypted using conventional cryptography, the screen tells you it was encrypted to a passphrase; click **Decrypt**.

   If the text is on the Clipboard: In PGPwireless for Palm OS, tap the Menus icon, then select **Decrypt/Verify Clipboard** from the Tools menu. If the text was encrypted using public-key cryptography, the key it was encrypted to displays; click **Decrypt**. If the text was encrypted using conventional cryptography, the screen tells you it was encrypted to a passphrase; click **Decrypt**.

The PGP Progress dialog box displays, and then you are prompted for the appropriate passphrase.

(For information about the passphrase screen, tap the **i** in the upper right corner of the screen.)

2. If you are using public-key cryptography, enter the passphrase for your private key and tap **OK**.
3. If you are using conventional cryptography, enter the passphrase you received from the person who encrypted this message and tap **OK**.

   The PGP Progress dialog displays. Depending on the speed of the processor in your handheld and the size of the key, this could take several minutes. Tap **Cancel** if you wish to cancel the decryption.

NOTE: If the PGP Error dialog box appears, telling you that the text contained corrupt data, this means that the encrypted text was modified since it was encrypted.

The PGP Results screen displays, showing the decrypted text. You can copy the results to:

- **Nowhere** to delete the results from your handheld
- **Memo** to copy the results to a new Memo Pad record that it creates
- **Clipbrd** to copy the results to the Clipboard, so that you can paste the results into another application
- **Popup** to copy the results to the PGP Popup buffer (which has a greater capacity than the Clipboard)

NOTE: If you copy the results to the PGP Popup buffer, you must wipe or insert and wipe the PGP popup buffer before you can use the PGP popup menu again.

4. Tap the appropriate button.

Encrypting

Encryption is the process of making text unreadable except to the intended recipient. PGPwireless for Palm OS can encrypt email messages, text on the Clipboard, or text in a Memo Pad record.

NOTE: The following procedure uses the MultiMail email application.

To encrypt text on your handheld:

1. Access the text you wish to encrypt:

   If the text is an email message: On your handheld, open your email application, create a new message, enter the text. When the text is complete, tap the PGP popup menu, then tap **PGP Encrypt selection**.

   If the text is in a Memo Pad record: In PGPwireless for Palm OS, tap the Menus icon, select **Encrypt Memo** from the Tools menu, tap the Memo Pad record you want to encrypt on the Select Memo screen, then click **OK**.

   If the text is on the Clipboard: In PGPwireless for Palm OS, tap the Menus icon, then select **Encrypt Clipboard** from the Tools menu.

   The Select PGP Encrypt Keys screen displays.

2. To encrypt the message to someone's public key, tap the key you want to use, then tap **Public Key Encrypt**.

3. To encrypt the message using conventional encryption, tap **Conventional Encrypt**, enter a passphrase, and tap **OK**.

NOTE: Use the **Replace original text** checkbox with caution. When checked, it overwrites the plaintext with the encrypted text. When unchecked, it doesn't overwrite what you've encrypted; instead, it lets you delete the results or copy them to a Memo Pad record, the Clipboard, or the PGP Popup buffer.

The PGP Progress dialog appears.

Depending on the speed of the processor in your handheld and the size of the key, the encryption could take several minutes. Tap **Cancel** if you wish to cancel the encryption.

When the encryption is done, the existing text is overwritten with the encrypted text.

Signing

Signing is the process of using your private key to sign a message so that when the recipient verifies the message with your public key, they know that you're the only person who could have signed it (using your private key).

PGPwireless for Palm OS can sign email messages, text on the Clipboard, or text in a Memo Pad record.

NOTE: The following procedure uses the MultiMail email application.

To sign text on your handheld:

1. Access the text you wish to sign:

   If the text is an email message: On your handheld, open your email application, create a new message, and enter the text. When the text is complete, tap the PGP popup menu, then tap **PGP Sign selection**.

   If the text is in a Memo Pad record: In PGPwireless for Palm OS, tap the Menus icon, select **Sign Memo** from the Tools menu, tap the Memo Pad record you want to sign on the Select Memo screen, then click **OK**.

   If the text is on the Clipboard: In PGPwireless for Palm OS, tap the Menus icon, then select **Sign Clipboard** from the Tools menu.

   The Select PGP Signing Key screen displays.

2. Tap your private key to select it and then tap **Sign with Key**.

   (If you are signing text in an email message, the **Replace original text** checkbox displays. When checked, it overwrites the plaintext with the signed text in the body of the message. When unchecked, it doesn't overwrite what you've encrypted; instead, it lets you delete the results or copy them to a Memo Pad record, the Clipboard, or the PGP Popup buffer.)

   The Phrase screen for your private key appears.

3. Enter the passphrase to your private key, then tap **OK**.

   The PGP Progress dialog appears. Depending on the speed of the processor in your handheld and the size of the key, the signing could take several minutes. Tap **Cancel** if you wish to cancel.

   If you signed text in an email message and kept the **Replace original text** checkbox checked, the signed text overwrites the plaintext of the message when the signing is done. The message is ready to be sent.

   If you signed a Memo Pad record or the contents of the Clipboard, or if you signed the text of an email message and *unchecked* the **Replace original text** checkbox, the PGP Results screen displays, showing the signed text. You can copy the results to:

   - **Nowhere** to delete the results from your handheld
   - **Memo** to copy the results to a new Memo Pad record that it creates
   - **Clipbrd** to copy the results to the Clipboard, so that you can paste the results into another application
   - **Popup** to copy the results to the PGP Popup buffer (which has a greater capacity than the Clipboard)

   NOTE: If you copy the results to the PGP Popup buffer, you must wipe or insert and wipe the PGP popup buffer before you can use the PGP popup menu again.

   ---

4. Tap the appropriate button.

Encrypting and signing

Encrypting and signing is simply doing both (encrypting the text with either conventional encryption or public-key encryption and signing the text with your private key) at the same time. When a person receives a message that is both encrypted and signed, they know that the contents were protected and that the message came from who it is purported to have come from.

PGPwireless for Palm OS can encrypt and sign email messages, text on the Clipboard, or text in a Memo Pad record.

NOTE: The following procedure uses the MultiMail email application.

To encrypt and sign text on your handheld:

1. Access the text you wish to encrypt and sign:

   If the text is an email message: On your handheld, open your email application, create a new message, and enter the text. When the text is complete, tap the PGP popup menu, then tap **PGP Encrypt & Sign selection**.

   If the text is in a Memo Pad record: In PGPwireless for Palm OS, tap the Menus icon, select **Sign Memo** from the Tools menu, tap the Memo Pad record you want to sign on the Select Memo screen, then click **OK**.

   If the text is on the Clipboard: In PGPwireless for Palm OS, tap the Menus icon, then select **Sign Clipboard** from the Tools menu.

   The Select PGP Encrypt Keys screen displays.

2. To encrypt the message to someone's public key, tap the key you want to use, then tap **Public Key Encrypt**.

3. To encrypt the message using conventional encryption, tap **Conventional Encrypt**.

NOTE: Use the **Replace original text** checkbox with caution. When checked, it overwrites the plaintext with the encrypted text. When unchecked, it doesn't overwrite what you've encrypted; instead, it lets you delete the results or copy them to a Memo Pad record, the Clipboard, or the PGP Popup buffer.

The Select PGP Signing Key screen displays.

4. Tap your private key to select it and then tap **Sign with Key**.

   (If you are signing text in an email message, the **Replace original text** checkbox displays. When checked, it overwrites the plaintext with the signed text in the body of the message. When unchecked, it doesn't overwrite what you've encrypted; instead, it lets you delete the results or copy them to a Memo Pad record, the Clipboard, or the PGP Popup buffer.)

   The Phrase screen for your private key appears.

5. Enter the passphrase to your private key, then tap **OK**.

6. If you selected conventional encryption, the Enter Passphrase screen appears. Enter a passphrase and click **OK**.

   The PGP Progress dialog appears. Depending on the speed of the processor in your handheld and the size of the key, the signing and then the encrypting could take several minutes. Tap **Cancel** if you wish to cancel.

   If you signed text in an email message and kept the **Replace original text** checkbox checked, the signed text overwrites the plaintext of the message when the signing is done. The message is ready to be sent.

   If you signed a Memo Pad record or the contents of the Clipboard, or if you signed the text of an email message and *unchecked* the **Replace original text** checkbox, the PGP Results screen displays, showing the signed text. You can copy the results to:

   - **Nowhere** to delete the results from your handheld
   - **Memo** to copy the results to a new Memo Pad record that it creates
   - **Clipbrd** to copy the results to the Clipboard, so that you can paste the results into another application
   - **Popup** to copy the results to the PGP Popup buffer (which has a greater capacity than the Clipboard)

   NOTE: If you copy the results to the PGP Popup buffer, you must wipe or insert and wipe the PGP popup buffer before you can use the PGP popup menu again.

7. Tap the appropriate button.

Wiping 7

Wiping is the process of completely deleting from your handheld a Memo Pad item, the contents of the Clipboard, free memory on your handheld, or the contents of the Vault.

IMPORTANT: Once wiped, this data cannot be recovered by *any* means.

Wiping a Memo Pad record

Wiping Memo Pad records, which make them completely unrecoverable, lets you protect private data such as decrypted email or personal information.

To wipe a Memo Pad record:

1. Open PGPwireless for Palm OS and make sure you are in **Keys** mode.
2. Tap the **Menus** icon.

   The Tools menu appears.
3. Tap **Wipe**.

   The Wipe menu appears.

4. Tap **Memo Item**.

   The Select Memo screen appears, showing the memo items on your handheld.
5. Tap the Memo Pad record you want to wipe and then tap **OK**.

   The PGP Wipe dialog appears, telling you this operation cannot be undone.
6. Tap **OK**.

   The Memo Pad record is wiped and the PGP screen displays.

Wiping the Clipboard

Wiping the Clipboard lets you completely remove any private data that you may have copied to it.

To wipe the contents of the Clipboard:

1. Open PGPwireless for Palm OS and make sure you are in **Keys** mode.
2. Tap the **Menus** icon.

   The Tools menu appears.
3. Tap **Wipe**.

   The Wipe menu appears.

4. Tap **Clipboard Contents**.

   The PGP Wipe dialog appears, telling you this operation cannot be undone.
5. Tap **OK**.

   The Clipboard is wiped and the PGP screen displays.

Wiping free memory

Wiping free memory securely erases all information from the free memory of your handheld.

This is important because when you delete an item from your handheld, such as a email message or a Memo Pad record, traces of that item are often left in free memory. (Free memory is memory on your handheld that is not currently being used by any application or database.)

An attacker with access to your handheld could analyze the contents of its free memory and find information that you thought was safely deleted. Wiping free memory removes this possibility.

To wipe free memory on your handheld:

1. Open PGPwireless for Palm OS and make sure you are in **Keys** mode.
2. Tap the **Menus** icon.

   The Tools menu appears.
3. Tap **Wipe**.

   The Wipe menu appears.

4. Tap **Free Memory**.

   The PGP Wipe dialog appears, telling you this operation cannot be undone.
5. Tap **OK**.

Wiping the Vault

Wiping the Vault lets you completely remove any private data you have stored there.

> **NOTE:** If you are using PGPwireless for Palm OS in conjunction with your Windows PC, it is possible to retrieve the contents of the Vault after you have wiped it on your handheld *if* you have backed it up to your PC. Refer to "Retrieving the Vault" on page 73 for more information.

To wipe the contents of the Vault:

1. Open PGPwireless for Palm OS and make sure you are in **Keys** mode.
2. Tap the **Menus** icon.

   The Tools menu appears.
3. Tap **Wipe**.

   The Wipe menu appears.

4. Tap **Vault Contents**.

   The Wipe PGP Vault dialog appears, telling you the data in the PGP Vault is about to be wiped.
5. Tap **OK**.

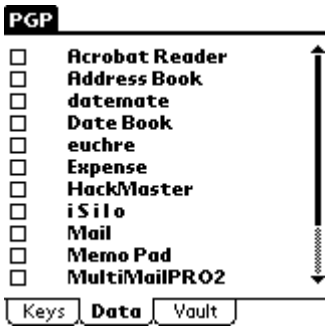
   The contents of the Vault is wiped and the PGP screen displays.

Database encryption 8

This chapter describes database encryption, a feature of PGPwireless for Palm OS that lets you encrypt the data files of applications on your handheld—the data cannot be accessed without the passphrase, thereby protecting your data in the event your handheld is lost or stolen.

Overview of database encryption

Database encryption is accessed via the Data tab in PGPwireless for Palm OS. Simply tap the Data tab and the Data screen appears.



The Data screen displays all of the applications installed on your handheld, with a checkbox next to the name of the application.

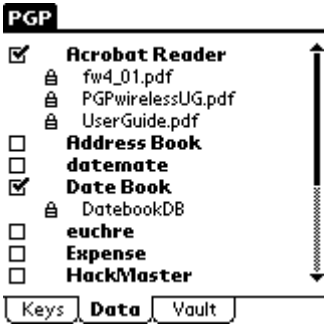
When you enable database encryption for an application (that is, you put a checkmark next to the name of the application), all the data for that application is automatically encrypted. If this is the first application you are enabling database encryption for, you will be prompted for a passphrase. This is called the database encryption passphrase, as it is the passphrase for all applications on your handheld for which you enable database encryption.

The first time you enable database encryption on your handheld, creating your database encryption passphrase also serves as entering it. Until you turn off your handheld, it goes to sleep, or it is reset (the current session ends if any of these things happen), the passphrase is stored in memory; you don't have to enter it again to access different data from the same application or to use data from any other application for which database encryption is enabled.

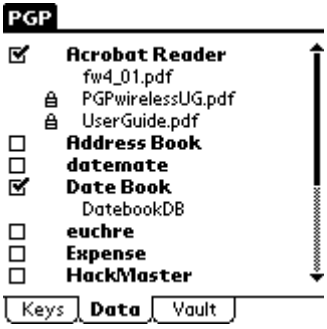
On your next session you will have to enter your database encryption passphrase again when you first use data from an application for which database encryption is enabled.

When database encryption is enabled on your handheld and you turn off your handheld, it goes to sleep, or is reset, all data from the applications for which database encryption is enabled is re-encrypted and the database encryption passphrase is wiped from memory.

When you enable database encryption for an application, the Data screen lists the databases for that application under the name of the application. Some Palm OS applications, Datebook for example, normally use only a single database, DateBookDB in this case. Other applications, Acrobat Reader for example, can have many databases; all of them are listed under the name of the application.



Databases that have not been opened this session show a padlock next to their names on the Data screen. Databases that have been opened this session don't have the padlock.



The database encryption cipher

For encrypting databases, PGPwireless uses the conventional cipher selected in the Preferences panel ***at the time that database encryption is first activated***. Once you have entered the passphrase, the cipher used for database encryption is "locked in."

Of course, you can change the conventional cipher in the Preferences panel, but this will not change the cipher used for database encryption. The only way to change the cipher used for database encryption is to deactivate database encryption and then activate it again.

Hot Syncing and encrypted databases

If you have not entered your database encryption passphrase since turning on your handheld, any encrypted databases will not be Hot Synced. You won't see a warning message during the Hot Sync, but if you view the Hot Sync log, you will see log entries indicating that synchronization of the encrypted databases failed.

Once you have entered the database encryption passphrase, you can Hot Sync normally -- all databases will Hot Sync correctly, whether they have been explicitly opened or not.

Databases that are shared by applications

Each database on your handheld is "officially" associated with, at most, one application. When you select an application for encryption, all the databases associated with that application are displayed below the name of the application. However, applications other than the one officially associated with a database can read and write to the database. This is important to know when you are selecting applications for database encryption.

For example, the "MemoDB" database, which contains the data of your MemoPad, is officially associated with the Memo Pad application. However, many other applications read this database. For example, PGPwireless (when performing operations on MemoPad entries), Datebook4, WordSmith, and many more applications read the MemoDB database. If you want the MemoDB database to be protected by PGPwireless database encryption, you must select the Memo Pad application for encryption.

This issue can lead to a situation where you think that a database is encrypted when it is not. For example, Datebook4 is a popular replacement for the built-in Datebook application. However, Datebook4 does not use its own database but works on the Datebook database DatebookDB. In order to encrypt the data for Datebook4, you must select Datebook for encryption, as well as Datebook4.

Typically this issue arises with the databases associated with the common built-in applications (MemoDB, DatebookDB, MailDB, AddressDB). Many applications provide integration or extension of built-in application functionality by accessing the databases of the built-in applications.

Applications that work on unassociated databases

Some applications work on databases that are not necessarily associated with any application. An example of this could be a text editing application which works on text databases.

If you select an application for encryption and you don't see databases listed below it that you expect, tap Data Preferences on the Options menu of the Data tab, and put a checkmark next to **List unassociated databases**. This will display, in addition to the applications listed, any databases that do not have an associated application on your device. You can then select those databases individually.

If you forget your database encryption passphrase

If you forget your database encryption passphrase, your only alternative is to deactivate database encryption, leaving all databases in their encrypted state.

To do this, select **Deactivate** from the Options menu of the Data tab. When the message asks if you know the passphrase, tap **No**. Confirm by tapping **Deactivate**. All encrypted data will remain encrypted.

IMPORTANT: Deactivating database encryption without the passphrase could cause you to lose the encrypted data.

If you have backed up your data to your desktop, be sure to select "Desktop overwrites Handheld" before your next Hot Sync.

Canceling the database encryption passphrase dialog

In certain situations, tapping the Cancel button in the database passphrase dialog can cause problems for the application which is trying to open the database. In these situations, you will see a warning message. Sometimes, if you proceed, your handheld may need to be reset. If this happens, your encrypted databases will remain safely encrypted.

Deleting applications and databases

PGPwireless prevents the deletion of any encrypted database. It also prevents the deletion of applications that have been selected for encryption. If you attempt to delete such a database or application, you will get an error message. In order to delete the database or application, launch the PGPwireless application, tap the Data tab, and uncheck the database/application in question.

Deleting or overwriting PGPwireless for Palm OS

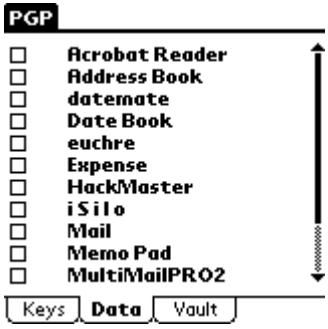
If database encryption is active, PGPwireless for Palm OS prevents itself from being deleted or overwritten. If you attempt to delete or overwrite PGPwireless without deactivating database encryption, you will get an error message. The next time you run PGPwireless for Palm OS, you will be queried if you want to deactivate database encryption. If so, you must enter the passphrase.

Using database encryption

To enable database encryption for an application:

1. On the PGPwireless for Palm OS main screen, click the Data tab.

   The Data screen appears.



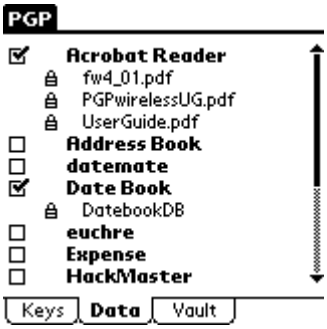
2. Locate the application you want to enable database encryption for, then tap the checkbox to the left of the name of the application.

   The PGP Data Phrase screen appears.

3. Enter your database encryption passphrase, then tap **OK**.

   (If this is the first time you are enabling database encryption on your handheld, you will be creating your database encryption passphrase and entering it at the same time.)

The Data screen re-appears, showing the application you enabled for database encryption with a checkmark next to its name and its databases listed below its name.



Database encryption is enabled for the application you selected.

NOTE: If you enable database encryption for an application that has an alarm set, the alarm will be disabled.

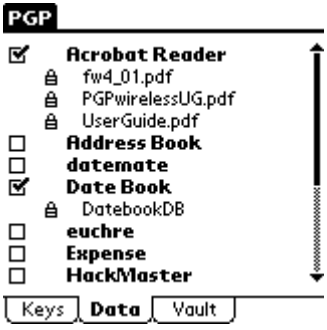
---

4. To enable database encryption for other applications on your handheld, simply repeat steps 2 and 3 for each application.
5. To use an application for which database encryption is enabled, simply access it normally. Enter your database encryption passphrase when you see the PGP Data Phrase screen.

To disable database encryption for an application:

1. On the PGPwireless for Palm OS main screen, click the Data tab.

   The Data screen appears.



2. Tap the checkmark of the application for which you want to disable database encryption.
3. If the PGP Data Phrase screen appears, enter your database encryption passphrase, then tap **OK**.

   The PGP Progress screen appears.

   The Data screen re-appears. The application you disabled database encryption for no longer has a checkmark next to its name, and its databases no longer are listed.

NOTE: You can use the Deactivate command to disable database encryption for all applications for which it is enabled. Refer to "Deactivating database encryption" on page 63 for more information.

Database encryption menus

There are two database encryption menus:

- **Tools:** lets you immediately re-encrypt any databases that have been opened this session using the Encrypt Now command
- **Options:** lets you access database encryption preferences, change your database encryption passphrase, and deactivate database encryption

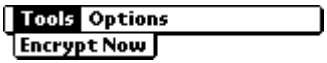
The Tools menu

The command under the Tools menu is Encrypt Now, which lets you immediately re-encrypt any databases that have been opened this session.

NOTE: The Encrypt Now command doesn't encrypt anything unless a database that is database encrypted has been opened during the current session. Opened (that is, currently unencrypted) databases are shown with no padlock icon.

To re-encrypt databases that have been opened:

1. Make sure at least one database has been opened this session.
2. Tap the Menu icon. 

   The Tools menu appears. 

3. Tap **Encrypt Now**.

The PGP Data Phrase screen appears.

4. Enter your database encryption passphrase, then tap **OK**.

   The Data screen reappears. All of your databases have been re-encrypted.

The Options menu

There are five commands under the Options menu, two of which are described elsewhere in this User's Guide. The five are:

- **Preferences:** Displays all of the PGPwireless for Palm OS preferences. Refer to Chapter 3, "Initial Setup," for more information.
- **Data Preferences:** Lets you establish preferences for database encryption only.
- **Change Passphrase:** Lets you change your database encryption passphrase.
- **Deactivate:** Lets you disable database encryption for all applications.
- **About PGP:** Displays the About PGP screen. Refer to "About PGPwireless for Palm OS" on page 75 for more information.

Changing database encryption preferences

There are two preferences that apply to database encryption only:

- **List all applications:** When checked, displays on the Data screen all currently installed applications, including those that don't currently have databases associated with them.
- **List unassociated databases:** When checked, displays on the Data screen databases that are not associated with any application.

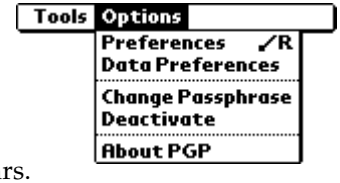
To change your database encryption preferences:

1. In PGPwireless for Palm OS, tap the Data tab.

   The Data screen appears.

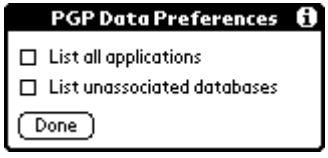
2. Tap the Menu icon, then tap **Options**.

   The Options menu appears.



3. Tap **Data Preferences**.

   The PGP Data Preferences screen appears.



4. Tap a checkbox to insert or remove a checkmark, as appropriate.
5. Tap **Done**.

   The Data screen re-appears.

Changing your database encryption passphrase

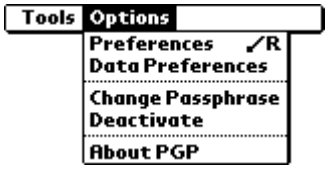
You can change your database encryption passphrase at any time.

To change your database encryption passphrase:

1. In PGPwireless for Palm OS, tap the Data tab.

   The Data screen appears.

2. Tap the Menu icon, then tap **Options**.

   The Options menu appears.

3. Tap **Change Passphrase**.

   If you haven't entered the current database encryption passphrase this session, the PGP Data Phrase screen appears.

4. Enter the current database encryption passphrase, then click **OK**.

   The New PGP Data Phrase screen appears.

5. Enter your new database encryption passphrase, then tap **OK**.

   The Confirm PGP Data Phrase screen appears.

6. Enter your new database encryption passphrase again to confirm it, then tap **OK**.

   The Data screen appears.

Deactivating database encryption

The Deactivate command disables database encryption for all applications.

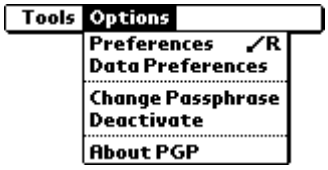
To deactivate database encryption:

1. In PGPwireless for Palm OS, tap the Data tab.

   The Data screen appears.

2. Tap the Menu icon, then tap **Options**.

   The Options menu appears.



3. Tap **Deactivate**.

   One of two Deactivate PGP Data screen appears:

   If you have entered the database encryption passphrase during this session, you are prompted to deactivate database encryption; continue with Step 4.

   If you haven't entered database encryption passphrase during this session, you are asked if you know the database encryption passphrase. If you know the database encryption passphrase, tap Yes and then enter your database encryption passphrase; database encryption will be deactivated on your handheld. If you don't know the database encryption passphrase, jump to Step 5.

4. Tap **Yes**.

   The PGP Progress screen appears.

   When the Data screen appears, database encryption is deactivated on your handheld.

5. Click **No**.

   A warning message appears.

6. Click **Deactivate**.

   When the Data screen appears, database encryption is deactivated on your handheld.

IMPORTANT: If you deactivate database encryption without providing the database encryption passphrase, the encrypted databases will not be usable. Refer to "If you forget your database encryption passphrase" on page 56 for more information.

Using the Vault 9

This chapter describes the Vault, a feature of PGPwireless for Palm OS that lets you fully protect (using encryption) the private data on your handheld. The Vault comes with multiple categories and also lets you create new ones.

The data in your Vault is automatically backed up onto your PC when you HotSync if you are using PGPwireless for Palm OS in conjunction with PGP on your Windows PC. It can be accessed from within PGPkeys (with the right passphrase, of course).

TIP: If you are using PGPwireless for Palm OS standalone—that is, ***not*** in conjunction with PGP on your Windows PC—and you are going to be storing important data in your Vault, you might want consider using a third-party backup program (BackupBuddy, for example) to back up your Vault data. In this case, your data will be backed up onto your computer in an encrypted format. If you were to lose your handheld or accidentally delete your Vault, you could restore it from the backup copy.

Opening the Vault

The Vault is opened from within PGPwireless for Palm OS. When you open the Vault for the first time, you must create a passphrase for it and then re-enter the same passphrase. When you open the Vault on subsequent occasions, you enter the passphrase only once.

NOTE: If the Random Data screen displays, tap where indicated. This random data is necessary so that PGPwireless can always re-encrypt your Vault data even if you forget to exit from the Vault.

Use caution in selecting characters for your passphrase from the International (Int'l) keyboard; it may be difficult to find the corresponding keystrokes on your PC (if you are going to be opening the Vault on your PC).

To open the Vault:

1. With PGPwireless for Palm OS open, tap the **Vault** tab at the bottom of the PGP screen.

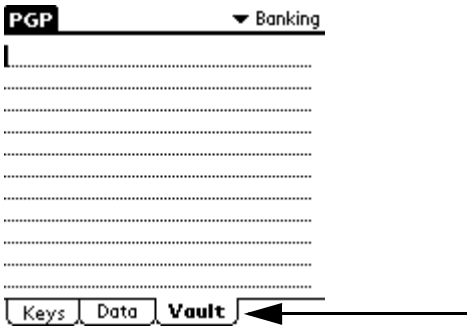
   The Enter Passphrase screen appears. (If this is the first time you are opening this Vault, the screen will be called New Vault Passphrase.)

2. Enter the passphrase and tap **OK**.

   (For information about the passphrase screen, tap the **i** in the upper right corner of the screen.)

NOTE: If you are opening the Vault for the first time, you will need to confirm the passphrase by re-entering it.

The PGP Vault screen appears.



When you are in the Vault, the Vault tab is active and **Vault** displays in bold type.

Using the Vault

The Vault can hold any text that you can get onto your handheld. You can enter text into the Vault:

- using Graffiti
- by cutting and pasting from other applications
- by using the keyboards

You can have up to 32 categories in the Vault; it comes with seven already configured. Each category can store up to 32 kilobytes of data.

Moving between categories

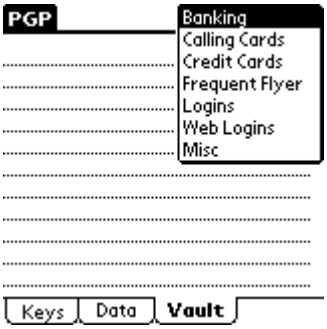
The Vault has seven default categories: Banking, Calling Cards, Credit Cards, Frequent Flyer, Logins, Web Logins, and Misc. You can also add more categories of your own.

Each category displays an empty screen when you first select it.

To move to a different category:

1. With the Vault open, tap the name of the active category.

   The list of existing categories appears.



2. Tap the category you want to be active.

Changing the Vault passphrase

If you would like to change the passphrase for your Vault, this is easy to do.

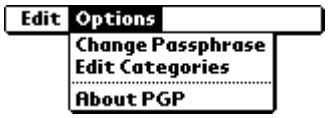
To change the Vault passphrase:

1. With the Vault open, tap the **Menus** icon.

   The Edit menu appears.

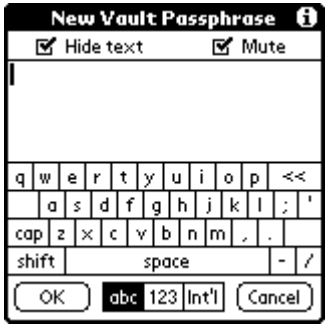
2. Tap **Options**.

   The Options menu appears.



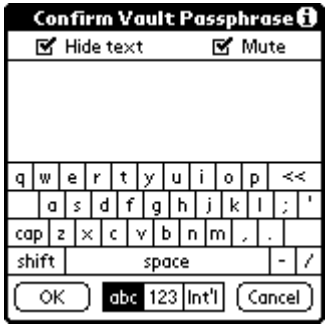
3. Tap **Change Passphrase**.

   The New Vault Passphrase screen appears.



4. Enter a new passphrase and then tap **OK**.

   The Confirm Vault Passphrase screen appears.



5. Re-enter the same passphrase and tap **OK**.

   The Vault screen displays.

Editing categories

It's easy to create new categories, or delete, rename, or duplicate existing ones.

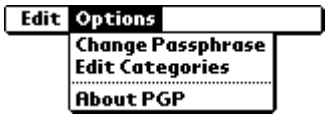
To edit Vault categories:

1. With the Vault open, tap the **Menus** icon.

   The Edit menu appears.

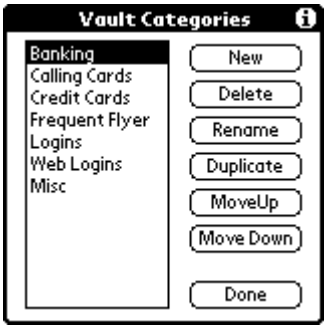
2. Tap **Options**.

   The Options menu appears.



3. Tap **Edit Categories**.

   The Vault Categories screen appears.



NOTE: The text in the tips for editing categories (tap the **i** in the upper right corner of the screen) do not apply to editing categories for the Vault.

4. To create a new category, tap **New**, enter a name for the new category, then tap **OK**.
5. To delete a category, select the category you want to delete, tap **Delete**, then tap **OK**.
6. To rename a category, tap the category you want to rename, enter the new name, then tap **OK**.
7. To duplicate a category, tap the category you want to duplicate, then tap **Duplicate**. A second category with the same name and contents is created.
8. To move a category, tap the category then tap **Move Up** or **Move Down**.
9. Click **Done** when you are finished.

Closing the Vault

To close the Vault, simply tap the **Keys** tab.

The Encrypting dialog appears, then the Keys screen appears. (If you did not make any changes to the Vault, the Encrypting dialog does not appear.)

NOTE: Even if you forget to specifically exit from the Vault, your data is protected. The Vault automatically closes and encrypts your data (or re-encrypts if you've made changes) if you open another application on your handheld, shut off your handheld, or the handheld turns itself off after the specified period of inactivity.

Backing up the Vault

To back up the contents of the Vault, simply do a HotSync. The contents of all categories of the Vault will be backed up to your PC.

Opening the Vault on your PC

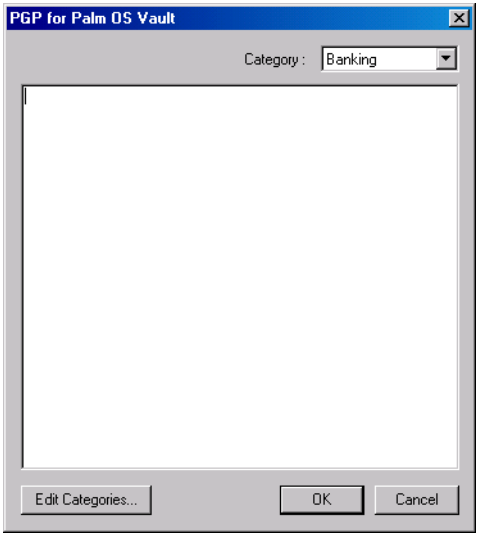
If you are using PGPwireless for Palm OS in conjunction with PGP on your Windows PC, you can open and edit the Vault on your PC (of course, you must have backed up the Vault to the PC first and you must know the passphrase).

To open the Vault on your PC:

1. On your PC, open PGPkeys.
2. Pull down the **File** menu and select **Edit PGP for Palm OS Vault**.

   The PGP Enter Passphrase dialog displays.
3. Enter the passphrase for the Vault and click **OK**.

The Vault opens.



You can make changes to the contents of the Vault in any category, and you can also edit categories. The Vault works on your PC just like it does on your handheld.

IMPORTANT: If you make changes to the data in the Vault or the categories on your PC and you want those changes moved onto your handheld, refer to "Retrieving the Vault" on page 73 for background information and the procedure.

---

4. Click **OK** when you are done.

Wiping the Vault

Wiping the Vault lets you completely remove any private data you have stored there.

NOTE: If you are using PGPwireless for Palm OS in conjunction with your Windows PC, it is possible to retrieve the contents of the Vault after you have wiped it on your handheld *if* you have backed it up to your PC. Refer to "Retrieving the Vault" on page 73 for more information.

To wipe the contents of the Vault:

1. Open PGPwireless for Palm OS and make sure you are in **Keys** mode.
2. Tap the **Menus** icon. 

   The Tools menu appears.
3. Tap **Wipe**.

   The Wipe menu appears.

4. Tap **Vault Contents**.

   The Wipe PGP Vault dialog appears, telling you the data in the PGP Vault is about to be wiped.
5. Tap **OK**.

   The contents of the Vault is wiped and the PGP screen displays.

NOTE: If you wipe the contents of the Vault on your handheld, then HotSync, the Vault data on your PC is deleted. It is not, however, wiped. If you want to wipe the Vault data, use the Wipe feature of PGP to wipe **PGPvault.*** files from the Palm/PGP folder on your PC.

Retrieving the Vault

If you are using PGPwireless for Palm OS in conjunction with your Windows PC, it is possible to retrieve the contents of the Vault after you have wiped it on your handheld—*if* you backed it up to your PC.

During normal operation, the Vault data on your handheld is automatically synchronized with the Vault data on your PC during each HotSync (assuming the Conduit Action for PGP for Palm OS is set to Synchronize the files, the default). The previous Vault data gets overwritten, with one backup of it being made (PGPvault.org).

If you have created a new category or added data to a category on your handheld, for example, that new data gets added to the Vault data on your PC. And vice versa: if you add data to the Vault on your PC and then HotSync, that data gets added to the Vault data on your handheld.

IMPORTANT: Do not make changes to Vault data on both your handheld *and* your PC since the last HotSync. The conduit cannot add Vault data from the PC to the handheld and from the handheld to the PC during the same HotSync. If this does happen to you accidentally, the Vault data on the handheld will overwrite the Vault data on the PC, but the old Vault data on the PC will be backed up to the PGPvault.org file. Also, the HotSync will generate an error message and an entry in the HotSync Log. Instructions for retrieving the Vault data that is backed up on the PC is in the Log message.

But what can you do if you mistakenly wipe the Vault on your handheld or lose your handheld?

The answer is: You can overwrite the Vault data on your (new) handheld with the Vault data on your PC. To do this, you need to change the HotSync settings for PGPwireless for Palm OS on your PC and then do a HotSync. The following procedure guides you through this.

WARNING: In the following procedure, the Vault data on your handheld gets overwritten with the Vault data on your PC. **Perform this procedure with caution.**

To overwrite the Vault data on your handheld with the Vault data from your PC:

1. On your Windows PC, click the HotSync icon in your system tray.

   The HotSync menu appears.

2. Click **Custom**.

   The Custom screen appears.

3. Highlight **PGP for Palm OS**.

4. Click **Change**.

   The PGPwireless for Palm OS screen appears.

5. In the HotSync Action for PGPwireless section, click **Desktop overwrites handheld**, then click **OK**. Note that the Desktop overwrites handheld setting applies to your keys as well as your Vault data.

   The Custom screen appears.

6. Click **Done**.

7. Perform a HotSync.

8. When the HotSync is done, check on your handheld to make sure that the Vault data from your PC has overwritten the Vault data on your handheld.

9. On your Windows PC, click the HotSync icon in your system tray, select **Custom**, and make sure the **PGP for Palm OS** action is set to **Synchronize the files**. It should have automatically reverted to this setting.

10. If the action is still **Desktop overwrites handheld**, highlight **PGP for Palm OS**, click **Change**, select **Synchronize the files**, and click **OK**. When the Custom screen appears, click **Done**.

About PGPwireless for Palm OS

A

The About PGP screen tells you the version of PGPwireless for Palm OS that you are using. It also displays the URL to the PGP Web site and copyright information.

To display the About PGP screen:

1. With PGPwireless for Palm open, tap the **Menus** icon.

   The Tools menu appears.

2. Tap **Options**.

   The Options menu appears.

3. Tap **About PGP**.

   The About PGP screen appears.

4. When you have finished reading the text, tap **OK**.

Troubleshooting B

This appendix describes some PGPwireless for Palm OS problems and their solutions.

Problem: I can't install PGPwireless on my Windows 2000 system.

Solution: Are you a "restricted user" on the system? If so, you need to have your status changed to at least "standard user." Restricted users on Windows 2000 systems don't have the necessary rights to install software.

Problem: When using PGPwireless for Palm OS in conjunction with PGP on your Windows PC, the menu items in PGPkeys don't appear.

Solution: Did you install PGP on your Windows PC *after* you installed PGPwireless for Palm OS or did you upgrade to a new version of PGP? If so, reinstall PGPwireless for Palm OS again now that PGP is installed on your Windows PC.

Problem: There aren't any PGP keys on my handheld.

Solution: Have you moved them onto your handheld from your Windows PC if you are using PGPwireless for Palm OS in conjunction with PGP? Have you imported or beamed them onto your handheld if you are using PGPwireless standalone? If not, refer to Chapter 4, "Moving keys onto your handheld" for instructions.

Problem: My PGP popup menu isn't working.

Solution: Are you running a hack called Graspeedy? If so, try disabling it or deleting it from your handheld. (Graspeedy redefines the Graffiti drawing area so that a portion is automatically capitalized; unfortunately, this behavior interferes with the PGP popup menu.)

Problem: My handheld is experiencing erratic behavior.

Solution: Are you using CryptoBoost? If so, try changing from 40% to 20%. If you are already at 20%, try turning it off. Refer to "CryptoBoost" on page 24 for more information. Are you using other software on your handheld that patches system traps (HackMaster, for example)? If so, install TrapWeaver (http://www.twilightedge.com/) or remove the software on your handheld that patches system traps.

Glossary

Address Book — a Palm OS application for keeping track of addresses and other information.

application buttons — the four physical buttons near the bottom of Palm handhelds. By default, they open (from left to right) the Date Book, Address Book, To Do List, and Memo Pad applications. These assignments can be changed.

applications launcher — the part of a Palm handheld above the application buttons and below the screen; includes four tappable icons: Applications, Menu, Calculator, and Find. Does not include the Graffiti writing area.

authentication — to prove genuine by corroboration of the identity of an entity.

cipher text — the result of manipulating either characters or bits via substitution, transposition, or both.

clear text — characters in a human readable form or bits in a machine-readable form (also called *plain text*).

contrast control — a circular control on the back of Palm handhelds that adjusts the contrast of the screen.

Cryptography — the art and science of creating messages that have some combination of being private, signed, unmodified with non-repudiation.

Date Book — a Palm OS application for scheduling your time.

decryption — the process of turning cipher text back into plain text.

Diffie-Hellman/DSS key	one of the three types of PGP keys you can create (the other two are RSA and RSA Legacy). Diffie-Hellman/DSS keys let you take advantage of many PGP key features, including Additional Decryption Key (ADK), designated revoker, multiple encryption subkeys, and photo ID.
division marks	marks in the Graffiti writing area that separate the side where you write letters (on the left) from the side you write numbers (on the right). When enabled, tapping the top division mark opens the PGP popup menu.
encryption	the process of disguising a message in such a way as to hide its substance.
flip cover	the strong plastic cover that comes with Palm handhelds.
Graffiti	the Palm OS way of entering data by writing with your styles in the Graffiti writing area. Keyboards—where you can tap letters, numbers, and characters—are available if you are uncomfortable entering data using Graffiti.
Graffiti writing area	the part of a Palm handheld you use to enter text and numbers. Located between the Applications launcher icons.
IR (infrared) port	a port at the top of Palm handhelds that uses IR technology to exchange data with other Palm handhelds or another device with a compatible IR port.
key	a means of gaining or preventing access, possession, or control represented by any one of a large number of values.
Memo Pad	a Palm OS application for storing data.
passphrase	an easy-to-remember phrase used for better security than a single password; key crunching converts it into a random key.

password	a sequence of characters or a word that a subject submits to a system for purposes of authentication, validation, or verification.
plain text	the human readable data or message before it is encrypted.
Power button	button on the front of Palm handhelds that turns the unit on and off, and controls the backlight feature.
Pretty Good Privacy (PGP)	an application and protocol (RFC 1991) for secure e-mail and file encryption developed by Phil R. Zimmermann. Originally published as Freeware, the source code has always been available for public scrutiny. PGP uses a variety of algorithms, like IDEA, RSA, DSA, MD5, SHA-1 for providing encryption, authentication, message integrity, and key management. PGP is based on the "Web-of-Trust" model and has worldwide deployment.
private key	the privately held "secret" component of an integrated asymmetric key pair, often referred to as the decryption key.
public key	the publicly available component of an integrated asymmetric key pair often referred to as the encryption key.
Reset button	a button on the back of a Palm handheld that resets the unit. A soft reset retains data; a hard reset erases all date on the handheld. Refer to the Palm documentation for more information.
RSA key	one of the three types of PGP keys you can create (the other two are Diffie-Hellman/DSS and RSA Legacy). RSA keys support for PGP features ADKs, designated revoker, multiple encryption subkeys, and photo ID. RSA keys are only fully compatible with PGP versions 7.0 and above and other open PGP applications.

RSA Legacy key	one of the three types of PGP keys you can create (the other two are Diffie-Hellman/DSS and RSA). RSA Legacy keys are only used for communication with PGP users using older versions of PGP. RSA Legacy keys do not support many of PGP key features.
screen	displays the applications and data stored on your handheld.
scroll button	the button at the bottom of Palm handhelds that scrolls the screen contents up and down if it doesn't fit on a single screen.
secret key	either the "private key" in public key (asymmetric) algorithms or the "session key" in symmetric algorithms.
sign	to electronically "sign" an encrypted message or record. Allows the authentication of information by the process of signature verification. When you sign a message or record, PGP uses your private key to create a digital code that is unique to the contents of the message and your private key. Anyone can use your public key to verify your signature.
stylus	shaped like a pen, a styles is used to tap the screen to open application or to enter data.
tap	to press on the screen of your handheld in a specific place with the tip of the stylus.
To Do List	a Palm OS application for keeping track of items to do.
wipe	to permanently erase a message or record so that it is unrecoverable by any means.
verification	to authenticate, confirm, or establish accuracy.

Index

N

P

S

T

U

V

W

Z