



**Person To Person™**

Personal Encryption Tool

By **PTP Security**

## **Person To Person**

**© 2009 PTP Security. All Rights Reserved.**

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Revised Monday, March 29, 2010.

# Table of Contents

|   |           |
|---|-----------|
| <b>Part 1 Introduction</b>                      | <b>4</b>  |
| 1 Welcome .....                                 | 4         |
| 2 Installation.....                             | 4         |
| 3 Theory of Operation.....                      | 5         |
| 4 Support .....                                 | 6         |
| <b>Part 2 Desktop Client</b>                    | <b>7</b>  |
| 1 Desktop Operation.....                        | 7         |
| 2 Signing Files.....                            | 7         |
| 3 Public Key Files.....                         | 8         |
| 4 Encrypting Files.....                         | 8         |
| 5 Decrypting Files.....                         | 9         |
| 6 Data Vault.....                               | 9         |
| 7 Database/Contact List Export/Import.....      | 10        |
| 8 Settings .....                                | 10        |
| 9 Signature/Replacement Files.....              | 12        |
| <b>Part 3 Windows Explorer</b>                  | <b>14</b> |
| 1 Windows Explorer Operation.....               | 14        |
| <b>Part 4 Email Integration</b>                 | <b>15</b> |
| 1 Email Client Operation.....                   | 15        |
| <b>Part 5 About Encryption</b>                  | <b>18</b> |
| 1 CypherMax.....                                | 18        |
| 2 Identity Verification.....                    | 19        |
| 3 Changing Your Password.....                   | 19        |
| <b>Part 6 Database Sharing</b>                  | <b>20</b> |
| 1 Sharing Contact Databases over a network..... | 20        |
| 2 Sharing Settings.....                         | 20        |
| <b>Index</b>                                    | <b>22</b> |

# 1 Introduction

## 1.1 Welcome

### Welcome to Person To Person

**Person To Person** allows you to sign, encrypt and decrypt disk files, quickly and easily, facilitating secure data storage on your own computer and secure communications when you exchange files with your correspondents via email or file transfer.

**Person To Person** (PTP) uses CypherMax™ technology to securely encrypt your data without the use of digital certificates. No third party components (like certificates) are required to use PTP between yourself and other PTP users. CypherMax is based on RSA, an industry standard encryption scheme.

**Person To Person** is directly integrated with Windows Explorer and optionally with Outlook, Outlook Express and Windows Mail, to make signing/encryption/decryption quick and easy.

**Person To Person** is supported on Windows 2000 and later.

**Person To Person** is available in Free, Data Vault, Standard, Email and Professional editions.

The **Free** edition allows unlimited decryption of signed files and decryption of files encrypted to yourself.

The **Data Vault** edition adds the ability to encrypt files to yourself which can only be decrypted by you. This allows you to secure data for your personal use. The Data Vault is a single storage area where you can store files in an encrypted form and easily retrieve them later. This can be more handy than keeping important files in various locations on your computer. Data Vault edition also allows you to sign files to be sent to other PTP users. Signing is a lightweight form of encryption that is much less secure than CypherMax encryption and is intended to guarantee the identity of the sender rather than provide message security.

The **Standard** edition adds the ability to encrypt files with CypherMax to be sent to other PTP users. Such files can be exchanged by removable media, as email attachments or by FTP. Standard edition supports decryption of CypherMax files you receive from other PTP users as well. Such other users are known as Contacts.

The **Email** edition adds direct integration with Outlook 2003/2007/Express. This allows email messages themselves (and any attachments) to be encrypted or decrypted automatically when sent or received by Outlook.

Finally, the **Professional** edition adds the ability for a group of PTP users on a network to share their Contact databases.

## 1.2 Installation

You must be an Administrative level user to install **Person To Person**. On Vista, you may be prompted for permission to grant admin level access (called elevation) to the installer. If prompted, you must grant the access to proceed with the installation.

After running the PTP.msi setup program, **Person To Person** will be installed in the **PTP Security \Person To Person** directory located in your Program Files directory.

Start Menu entries will be added for all users on the system, if you install while logged on as an administrative level user. If logged on as a normal user, Start Menu entries will only be added to your personal Start Menu. Note that this only affects the Start Menu. Each different Windows user login that executes Person To Person will receive their own private database and require a separate license to use.

Note that when you install updates to Person To Person, or you choose to uninstall PTP, you will be prompted to keep your database if you are doing an update or to completely remove all parts of PTP if you are not planning to continue using Person To Person.

During the install you may be prompted to install one or both of the Outlook integration Add-ins. Selecting an add-in will install PTP hooks into Outlook allowing you to encrypt and decrypt email messages from menus and toolbar buttons inside Outlook. If you do not install an Outlook Add-in but later decide you wish to, you must first uninstall PTP (from the Control Panel) and then reinstall selecting the Outlook Add-in you desire. Your settings and database will be retained.

**Note:** When updating PTP, changes to the Windows Explorer Context Menu feature may require a reload of Windows Explorer. You can either perform a reboot of the PC or run **RestartExplorer.exe** located in the PTP install directory. Please check the **ReleaseNotes** file after an update. If a reload of Windows Explorer is needed, it will be noted in the release notes. If a reload is needed, you can run RestartExplorer or reboot your system at your convenience. RestartExplorer takes only a few moments but it does close all Windows Explorer instances.

## 1.3 Theory of Operation

**Person To Person** is a desktop application. Starting PTP will present an explorer like screen that allows you to navigate your file system and select files for signing, encryption or decryption. In Windows Explorer, you can right-click on files and see PTP actions in the context menu that allow processing of the selected files with PTP.

The **Data Vault** is a streamlined way to use PTP to maintain a repository of encrypted files for your local use. Rather than have encrypted data in various locations on your computer's disk drives, you can put files into the Data Vault and then easily retrieve them at a later time. Files placed into the Data Vault are automatically encrypted and automatically decrypted when you retrieve them.

With the **Email** edition, in Outlook, Outlook Express and Windows Mail, tool bar and menu options are available to enable the encryption of email message body text and attachments or attachments alone. You can enable automatic decryption of incoming messages that contain body text or attachments encrypted with PTP.

**Person To Person** employs a secure database to store information about you and your correspondents. When you start PTP for the first time, you will be prompted to enter a **User Identity** and **Password**. The User Identity can be any string of characters you wish to use to identify yourself to your correspondents. The Password is used to secure access to the PTP database and generate your Public/Private key pair used in the encryption process. The password you select is important because it will be difficult to change later.

Secure communications takes place between two PTP instances who know each other's Public Keys. In this way your encrypted data can only be decrypted by someone who knows your Identity. With PTP you send a **Public Key** file to your correspondents and they decrypt that file with their copy of PTP. This adds your User Identity and Public Key to their PTP database. Then when you send encrypted files to them, their PTP instance will know how to decrypt your files. Your correspondent can send their Public Key file to you, or send you an encrypted file or message, which when decrypted, makes their Public Key known to you. When you decrypt a Public Key file in an email program, the senders email address is automatically associated with their User Identity, making it

easy to send encrypted messages back to them. The key concept is that you must have received a Public Key from a contact in order to send encrypted data to them.

The Demonstration edition of PTP allows for unlimited decryption operations and a limited number of encryption operations. To continue to encrypt data after the trial period, you will need to purchase a license.

**Signing** is a less secure way of sending data to someone else. When you Sign a file with PTP, the file has your User Identity attached and the data is lightly encrypted. You may optionally include a pass phrase, which the reader of the data must know to decrypt the signed file. The main purpose of Signing is to provide the reader of the file with your identification and allows you to send files without first having exchanged Public Key files.

## 1.4 Support

For technical and sales support contact your distributor. Your distributor is shown on the About screen displayed from the Help menu.

## 2 Desktop Client

### 2.1 Desktop Operation

**Person To Person** is a Windows desktop application or "client". As such you start PTP from the Windows Start Menu or by running the PTPClient.exe file directly.

When PTP starts for the first time, you will be prompted to enter your User Identity and Password. See the next section for more details on your User Identity and Password. On subsequent start up, PTP will prompt you to enter your password. You have 30 seconds to enter your password before the login screen will be closed automatically to make sure the prompt is not left open. Once your password is validated the PTP main screen is displayed. You can change the time to login on the Settings screen.

The main screen consists of three windows, the file system **Navigation** window on the left, the **Processing List** window on the upper right and the **Contacts** (correspondents) window on the lower right. After login your known contacts will be shown in the Contacts window. Your own User Identity is listed first in the Contacts window and allows you to encrypt files which can only be decrypted by you. You may put any information you wish in the User-Tag field by double-clicking the field on a Contact line.

The Navigation window starts in the PTP your selected **Home directory** or in the last directory you visited before shutting PTP down (See Settings). You can navigate the file system with the Navigation window and select files to add them to the Processing List by drag & drop or right-click context menu. You may double-click on a file to open it. The directory displayed in the Navigation window is called the **Working Directory**. By default, when files are decrypted, the plain text version of the file will be written to this Working Directory. You can opt to have decrypted files always written to a special directory to keep unsecured files in a single known location.

If you have one or more files in the Processing List you can click on one of the buttons on the tool bar above the Processing List Window. You can delete files from the Processing List with right-click or the tool bar button to clear the Processing List. You can also delete files in the Navigation window, but be aware that this will delete the file from your disk.

Note that several toolbar and menu operations generate an email message (sign and send, encrypt and send, generate public key file and send) with the results of an encryption operation. This feature relies on there being a default email client configured on your PC. If you see the error message "**Error sending email: (3) Login Failure**" when attempting an email operation, it means you have no default email client set. In all of the email clients there is an option to set that client as the default client. This can also be done on the Windows Control Panel. After doing that, you be able to send email from PTP.

There is a button on the toolbar to toggle **Data Vault** mode. When in Data Vault mode, the Processing List and Contacts list are replaced by a display of the files contained in the Data Vault.

### 2.2 Signing Files

You may Sign files and send them to another PTP user without any previous communication. Your Contacts list is not used for signing. When another user decrypts your signed file, your identification will be added to that user's Contact list.

Once files have been added to the Processing List, you can sign them by clicking the **Sign** tool bar button above the Processing List window. If only one file is on the Processing List, it will be encrypted

into a new file with the same name but with the **.PTP** extension. This new file will be written to the working directory displayed in the Navigation window. The Processing List will be cleared when the signing operation completes.

If you have more than one file on the Processing List when you click Sign, each file is signed individually and then written to the working directory.

If you wish to include a pass phrase in the signed file, you must enter the pass phrase on the Settings screen. The pass phrase is included in all files signed. The receiving user will be prompted to provide the pass phrase at decryption time (see Settings).

By clicking the **Sign and Mail** tool bar button, you can sign the file(s) on the Processing List and have the resulting **.PTP** files automatically attached to a new email message. Your default email client will appear and all you have to do is fill in the recipient's email address.

You can select directories and add all of their contents to the Processing List. You can add files to the Processing List from different directories.

## 2.3 Public Key Files

To send encrypted files to a Contact, you must first exchange **Public Key** files. You can create a Public Key file in the current working directory (shown in the Navigation window) by clicking the appropriate tool bar button or File Menu choice. You may also create a Public Key file and automatically create an email message with the Public Key file attached. The email message will appear in your default email client and all you have to do is enter your Contact's email address.

When your Contact receives and decrypts the Public Key file with his copy of PTP, your User Identity and Public Key will be added to his Contact list and he will then be able to decrypt files you send to him. He can now send encrypted files back to you as well, which you will be able to decrypt (and will add him to your Contact list). Or your Contact can send you his Public Key file which when processed adds him to your Contact list.

When you decrypt a Public Key file, the sender's User Identity and Public Key will be added to your Contacts list and you are now able to encrypt files for that Contact.

When User Identities are created by PTP, they have a second component, called the Identity Code, associated with them. This allows for identity verification. When you receive a Public Key file from a sender, after you decrypt it, the sender's Identity Code will be shown in the Contacts Window. You can then contact that sender by alternate means and ask them for their Identity Code. Only they can know what it is. In this way you know the User Identity you have received was sent by the correct individual.

If you receive a Public Key file and decrypt it automatically in your email client, the sender's email address will be automatically recorded in the Contact list. If you have a Contact without an email address, right-click on the email address field of the Contact listing, and an entry box will appear allowing you to enter the email address.

## 2.4 Encrypting Files

Once files have been added to the Processing List, you can encrypt them by clicking the **Encrypt** tool bar button above the Processing List window. If only one file is on the Processing List, it will be encrypted into a new file with the same name but with the **.PTP** extension. This new file will be written to the working directory displayed in the Navigation window. The Processing List will be cleared when the encryption operation completes.

If you have more than one file on the Processing List when you click encrypt, each file is encrypted individually and then added to a single container file. The container file is named with the same name as the first file on the Processing List with the **.PTPZ** extension. The container file is a zip archive.

Before clicking the Encrypt button, you **must** select a target Contact in the Contacts window. At startup, your personal Contact will be automatically selected or you can automatically select the last Contact used before shutdown (see Settings).

By clicking the **Encrypt and Mail** tool bar button, you can encrypt the file(s) on the Processing List and have the resulting .PTP/.PTPZ file automatically attached to a new email message. Your default email client will appear and all you have to do is fill in the Contact's email address. If the Contact's email address is in the PTP Contact list, that address will be inserted into the email message for you. The Contact's email address may be filled in automatically during decryption of messages by Outlook or you may manually enter a Contact's email address by placing the cursor over the email address area on a Contact's information line and double clicking. This will open an entry box for the email address.

You can select directories and add all of their contents to the Processing List. You can add files to the Processing List from different directories.

You must have a **Standard edition** or higher license to encrypt files to Contacts other than yourself.

## 2.5 Decrypting Files

You may only decrypt files with the .PTP or .PTPZ extension. You may only select one .PTP file for decryption at a time. If you select a .PTP file and a .PTP file is already on the Processing List, your second selection is not added to the Processing List.

Once there is a .PTP or .PTPZ file on the Processing List, the **Decrypt** tool bar button will be enabled and you can click on it to decrypt the file. The decrypted file(s) will be written to the Working Directory shown in the Navigation window. You may also select to have files decrypted to a special more private decryption directory to avoid mixing decrypted files with regular files in the Working Directory (See Settings).

## 2.6 Data Vault

The **Data Vault** is simply a special container maintained by PTP to provide a central place for you to keep encrypted data files for your own use. When the Vault is displayed by clicking the safe icon on the tool bar, the Processing List and Contacts list will be replaced by a list of the files in the Data Vault.

Add or update files in the Vault by dragging them from the Working Directory or using the context menu options on files in the Working Directory. Dragging files copies them from the WD and shift key while dragging will move them from the WD. Note that when files are added to the Vault, they are encrypted with your personal encryption key. Only you can decrypt them.

Files in the Data Vault may be extracted to the Working Directory by selecting one or more files and right-clicking for a context menu of operations you can perform on Vault files. You may also open a single file selection in the application associated with the file or in Notepad. If you open a file directly, PTP extracts the file to the Working Directory and then starts the application with that file as input. When you exit the application, you are responsible for placing the file back into the Vault if that is what you wish to do.

When you add a file to the Vault, the original location of that file is recorded in the Vault. If you decrypt a Vault file, the disk location where the decrypted file is placed is recorded in the Vault. When the Vault is displayed, PTP checks these saved locations and if a Vault file is found to exist on your disk, that file will be shown in red. If you hover your cursor over a Vault file, its original location and the first location on the decrypt list will be shown in the tooltip for the file.

You must have a **Data Vault edition** or higher license to use the Vault. Files placed in the Vault during the demonstration period can always be decrypted.

## 2.7 Database/Contact List Export/Import

When you license PTP, you are licensing the encryption key set for your selected User Identity. This User Identity and associated Contacts are stored in the PTP Database. To facilitate the use of your PTP User Identity on more than one PC, you can Export your Database and then Import it on a different PC. You can then encrypt and decrypt on both PCs as though they were the same.

When the Contact Lists of the two (or more) Databases become different, you can synchronize them by Exporting the Contact List from one Database and importing it to the other Database.

You can Export your Database to a disk file using the Export choice on the File pull-down menu. The Database is written to a file in an encrypted form. The Database export file has the **.ptpdb** extension. You can then import such a file into another instance of PTP. **Note that the imported Database overwrites the existing Database completely.**

You can export your Contact List to a disk file using the Export choice on the File pull-down menu. Contact information is recorded in the file in an encrypted form. You can then import such a file into another PTP Database with the Import choice on the File pull-down menu. The Contact export file has the **.ptpc** extension. Note that you can only import Contacts into a Database with the same User Identity as the Exporting Database.

## 2.8 Settings

Settings allow customization of PTP behavior. Open the Settings screen from the Setting pull down menu.

The Settings available are:

### Save Main Form Location

Saves the screen position of the Main form and restores the Main form to that location on the next startup.

### Save Main Form Size

Saves the size of the Main form and restores the Main form to that size on the next startup.

### Save Working Directory

Saves the working directory in the Navigation window at shutdown and starts the Navigation window in that directory on the next startup.

### Save Last Contact

Saves the Contact currently selected at shutdown and automatically selects that Contact on the next startup.

### Minimize to Task Tray

When you minimize PTP, this option will cause PTP to not be shown in the Task Bar but to be shown as an icon in the Task Tray. You can click on that icon to redisplay the PTP Main form.

### **Encrypt to ASCII**

Encryption is normally done in a binary form. This binary form results in an encrypted file slightly larger than the original file. However, binary files may not pass through some firewalls or content scanners. With this option you can cause the encrypted data to be written as ASCII character codes. This form will pass through firewalls and content scanners more readily than binary. However, the encrypted file will significantly larger than the original.

### **Enable Email Encryption**

Turn on or off PTP support in email clients. The email integration support for your email client must be installed first. See Installation.

### **Email Start Timeout**

When using PTP with Outlook (includes Express/Windows Mail), if PTP desktop client is not running when Outlook needs it, Outlook will start it. Outlook will wait for the amount of time set in this box for the client to start and so operations can continue. If the client does not start in this amount of time, an error will be displayed and encryption/decryption will not be available. Outlook will not be responsive during the wait time.

### **Send Key File with Default Account**

When you send Public Key files from Outlook (Includes Express/Windows Mail) using the toolbar buttons or menu choices, Outlook cannot determine what email account to use to send the message containing the key file. If you check this box, the public key message will be automatically sent (placed in the outbox) with your default email account. If you uncheck this box, then public key messages will not be automatically sent. Instead the composition window for each message will display, allowing you to select the appropriate email account and then click Send.

This does not affect Public Key file messages sent from the PTP desktop client. Such messages are always shown in the default email client composition window for you to complete and send manually.

### **Login Timeout**

To protect the security of your PTP database, the Login screen is only displayed for a limited amount of time. If you do not type in the password box or click a button on the screen by the time the timer expires, the Login screen will automatically close. Use this box to set the desired time out for the Login screen.

### **Approve External Operations**

When PTP is asked to perform encrypt/decrypt operations on behalf of Windows Explorer or by clicking on an encrypted attachment in Outlook, you are prompted to approve the requested action. To disable this prompting, uncheck this setting.

### **Inactivity Timeout**

To protect the security of your PTP database, you may have PTP automatically log out of the database after this many minutes of inactivity. PTP will continue to run but you will have to log back in to the database in order to perform any functions.

### **Automatically Open Decrypted File**

When a single file is decrypted, you can have PTP open the file with whatever application is registered for the file's extension. So a decrypted .doc file will be opened in Word, a .html file will be opened in IE and so on.

### Use Dialog Box for Errors

Normally, status and error messages are displayed in the status bar area at the bottom of the main screen. If you wish to have error messages also displayed in a dialog box (making them very hard to miss), check this setting.

### Start Minimized

Normally, after the splash screen, the PTP main screen displays and the login dialog appears over that. After login, the main screen remains visible and ready for use. Check this box to have the main screen minimized after splash. The login box will appear over the desktop and after login the main screen will remain minimized. Note that the main screen will appear momentarily.

### Start When Windows Starts

If you check this box, when you accept settings changes, a short cut will be added to your Windows Start Menu Startup folder. This short cut will cause PTP to be started after Windows completes it's startup. Note that your password will be supplied automatically and so you will not be prompted to login. When combined with the Start Minimized setting, this will cause PTP to be started and sent to the task bar/tray without user interaction at Windows startup. This setting is primarily intended to support database sharing.

### Decrypt to Working Directory

By default, files are decrypted into the current Working Directory. To further protect decrypted files, you may deselect this item to have PTP decrypt all files to a special temporary directory that will contain only decrypted files. In this manner decrypted files are not mixed with regular files in the Working Directory. In addition, this special directory is erased when PTP is shut down. This setting is global in nature and may only be changed by an Administrative level user and applies to all PTP users on the PC.

### Display Data Vault on Login

By default, the encryption/decryption processing list and the Contacts list are displayed after you complete your login to the Database. Check this option to display the Data Vault after login.

### Backup Database and Data Vault on Exit

Check this option to have your Database and Data Vault backed up each time you exit PTP. You must be logged into the database at exit time for the backup to take place. Note backing up may add significant time to the shutdown process.

### Signing Pass Phrase

When Signing a file, you may optionally include a Pass Phrase of up to 32 characters. Users decrypting such a Signed file will be prompted for your Pass Phrase. This is an optional additional security feature for Signed files.

### Home Directory

This is any directory you want to use to manage encrypted/decrypted files. If you click the Home button on the toolbar it will switch the Working Directory directly to this directory. If you do not select to have PTP start with the Working Directory set to the last Working Directory visited, this Home Directory will be the starting Working Directory.

## 2.9 Signature/Replacement Files

When you encrypt and email a file, the encrypted file is attached to a new email message and submitted to your default email client for processing. The body text of that email message is read by PTP from the file **PTPSignature.txt**. The default signature file is located in the PTP install directory. You may edit this default signature file if you wish. If this file is modified, it will not be overlaid on

future installs or updates. However, PTP will look for PTPSignature.txt in your Home Directory first, so it is recommended that you copy PTPSignature.txt to your Home Directory for customization.

In the same manner, when you encrypt email message body text in Outlook (using the Outlook Add-Ins), the encrypted message body is replaced with boiler-plate text. That text is read from the file **PTPReplacement.txt**. The same customization notes described above for the signature file also apply to PTPReplacement.txt.

When processing a signature or replacement text file, PTP supports several keyword substitutions to help customize the text. These substitutions are:

|                  |  |
|------------------|--|
| [ PRODUCTTITLE ] | Full name of the PTP product.                            |
| [ OWNERID ]      | User-Id of the Owner Contact (You).                      |
| [ OWNEREMAIL ]   | Owner Contact email address.                             |
| [ DOWNLOADURL ]  | URL where PTP can be downloaded.                         |
| [ CONTACTID ]    | User-Id of the Contact to which the email is being sent. |
| [ CONTACTEMAIL ] | Recipient Contact's email address.                       |
| [ CONTACTTAG ]   | Recipient Contact's User-Tag.                            |
| [ DATE ]         | Current date and time in system short format.            |
| [ DATEL ]        | Current date and time in system long format.             |
| [ TIME ]         | Current time in system time format.                      |

When doing an encrypt & email operation in the PTP client, the following substitution is also available:

|              |   |
|--------------|---|
| [ FILENAME ] | Name of the encrypted file attached to the email message. |
|--------------|---|

## 3 Windows Explorer

### 3.1 Windows Explorer Operation

[Person To Person](#) is fully integrated with Windows Explorer. You can right-click on directories or files to display the Explorer context menu. A PTP menu will appear which lists the operations you can perform on the selected items.

When you select a PTP function, the PTP desktop program will be started if it is not already running. Explorer then submits the requested encrypt/decrypt operation and list of files to the PTP program for processing. Note that in this case, the working directory of PTP, where the resulting files will be written, is switched to the same directory that you have selected the items from in Explorer.

When you select files for encryption from the Explorer context menu, PTP cannot automatically determine which Contact you wish to use to encrypt the files. Therefore PTP will open a dialog allowing you select the Contact you wish to use.

## 4 Email Integration

### 4.1 Email Client Operation

You may install one or both of the optional integration components for use with **Outlook** or **Outlook Express/Windows Mail**. If you do install one of these options, it will be enabled by default. You can enable/disable email client encryption on the PTP Settings screen.

Email integration is available for **Outlook 2003/2007** and **Outlook Express/Windows Mail**. You must have an **Email edition** license to use Outlook integration.

If email integration is installed and enabled, when you start your email client, you will see a new PTP tool bar below the regular tool bars. This tool bar, along with a menu on the email client's Tools Menu, allow you to select the encryption/decryption operations to be performed on email messages. Selecting these options on the main toolbar sets the option for ALL messages. When sending a message, the options will appear on the toolbar of the message compose window preset according to the global options you may have selected. You can then adjust the encryption options only for the message you are composing.

You can select from the following options by clicking on the button (highlighted means the option is ON):

#### Encrypt All

Encrypt the email message body text and any attachments to the message. The body is replaced by boiler plate text. The encrypted body text is sent as an attachment.

#### Encrypt Attachments

Encrypt only the attachments to the message. The body text is left in plain text form.

#### Encrypt Images

Encrypt any images embedded or attached to the message. Images are not encrypted by default.

#### Decrypt Attachments

Decrypt attachments with the .PTP extension on incoming email messages resulting in the attachment being in clear text form. If you do not select this option, .PTP files will be left as .PTP (encrypted) files. You can click on such an attachment later to invoke the PTP program to decrypt the file on demand. Note that encrypted body text is always decrypted.

You can select from the following operations by clicking on the button:

#### Decrypt Message

This button will only appear when the currently selected message in the email client explorer window has attachments with the .PTP extension. Clicking the button will immediately decrypt all the attachments. This is useful if you turn of Decrypt Attachments and so have messages with attachments still encrypted, or, when there are problems decrypting attachments and they are left in the encrypted state.

#### Send Key File

This button will send a Public Key File to the currently selected Contact(s) (Outlook 2003/2007) or to the sender of the currently selected email message(s) (all Outlook versions). You **cannot** send key files to Contacts in Outlook Express/Windows Mail. This option also appears on the Tools pull down

menu and on Contact/Message context menus on Outlook 2007. The message may be sent with the Outlook default email account or you can manually set this on each Public Key File message. See Settings.

When a new mail message is sent, or a new message is received, if encryption or decryption operations are required, your email client will start the PTP program and communicate with it to perform the needed operations. You will be required to login if the PTP program is not already running. You will not see the PTP main screen, but you will see progress displays as operations are performed.

Once all PTP processing is complete, the new message is either sent when sending a message or placed in the Inbox when receiving a message.

When encrypting a message, a PTP Contact must be selected. The email client will submit the message recipient's name and email address to PTP which will attempt to match one of your Contacts with that information. If a Contact is matched, it is selected for the encryption operation. If no Contact is matched, the encryption operation will cannot be performed. In that case you will be shown a warning and given the option to send the message unencrypted or to cancel the message.

When a message or attachments are decrypted because you have selected Decrypt Attachments or have decrypted a message on demand (Decrypt Message button), the decrypted message body text will replace the boiler plate text in the message and attachments will be decrypted but remain as attachments. If you double click an attachment with the .PTP extension, that file will be sent to the PTP program to be decrypted as a normal file into the current working directory of the PTP program.

When a Public Key file is decrypted automatically by selecting Decrypt Attachments or you decrypt on demand with the Decrypt Message button, the Public Key file will be processed and the Contact information encoded in it will be added to the PTP Contact List. In these two cases, the email address of the person who sent the Public Key file will also be recorded in the PTP Contact List. If you receive a Public Key file and do not decrypt it with one of the above methods, no decryption action occurs. If you the double click on the Public Key file attachment in Outlook, the Public Key file will be decrypted and the information added to the PTP Contact list, but the sender's email address will not be included.

At any time, you may place the cursor over the email address area of a Contact's information line and double click to edit the Contact's email address.

When Outlook needs to use PTP to process email encryption, it will check to see if the PTP program is already running on your desktop. if it is not, it will be started. Outlook will wait only so long for the PTP program to start and if it does not start in the allotted time, Outlook will abort the encryption and report an error. You can change the startup timeout on the Settings screen.

When messages fail to encrypt, Outlook does not send the message and the message composition window remains open. Outlook Express/Windows Mail will move the message to the Drafts folder. If decryption fails, the encrypted files are ignored and remain attached to the message.

Note that with Outlook, messages that are in RTF (Rich Text Format) have encryption limitations. If a message is in RTF format and has any attachments, no encryption can be done. If the message has no attachments, then the message body can be encrypted.

Currently, in Outlook, only Mail Messages are processed by PTP. Appointment, meeting request and task messages are not supported.

In Outlook 2003/2007, you may create **Contact User Fields** to control automatic encryption. This allows you to not enable encryption at the global level (main toolbar) but instead set encryption for individual Contacts in the Outlook Contact list. This means messages to the Contact will be encrypted

as you select, automatically, without you having to worry about choosing encryption at the global or new message levels. The User Fields are:

|                                |  |
|--------------------------------|--|
| <b>PTP Contact</b>             | Set to name or email address that will be used to look up the encryption Contact in the PTP database. Overrides normal use of Contact email address and then Contact name. |
| <b>PTP Encrypt Contents</b>    | Yes/No. If Yes, messages to the Contact will be fully encrypted. If No, encryption is controlled by the toolbar options selected on the compose window.                    |
| <b>PTP Encrypt Attachments</b> | Yes/No. If Yes, messages to the Contact will have any attachments encrypted. If No, encryption is controlled by the toolbar options selected on the compose window.        |

In Outlook 2007, on the detailed Contact window, the Ribbon Bar will contain check boxes to set the PTP Encrypt Contents/Attachments fields for you. Just check the appropriate box.

## 5 About Encryption

### 5.1 CypherMax

**CypherMax™** is a proprietary data encryption technology that combines the RSA and DEA encryption standards with a large key length and large data blocks to create an advanced encryption scheme. Most commercial encryption products use a 256 bit key which less secure. This technology provides significantly more secure encryption without the use of Digital Certificates.

Digital Certificates require the involvement of a third party, the Certificate Authority, with both correspondents in a secure exchange. This creates cost and complexity and the actual guarantee of security conferred by a certificate is debatable. CypherMax uses self generated certificates and is based on manual identify verification between the correspondents.

CypherMax employs RSA **Public/Private key pairs** which are partially generated from your PTP Password. Choosing a good password contributes to improved security. Note that changing your password **invalidates your key pair** and therefore your PTP Identity. See Changing Your Password for more information.

CypherMax is not dependant on any underlying Microsoft encryption technologies.

CypherMax Signing complies with USA Federal Information Processing Standards 180-2 for Secure Hash Algorithms.

CypherMax Encryption exceeds FIPS 140-2 Security Level 3.

CypherMax Encryption quality can be shown to be excellent because its binary output is incompressible under the standard Huffman Encoding algorithm.

CypherMax is patent pending.

#### **Person To Person and international standards for encryption software.**

PTP meets or exceeds the following ISO standards:

ISO 10118-3  
ISO 18033-2  
ISO 18033-3

ISO (International Organization for Standardization [www.iso.org](http://www.iso.org)) is the world's largest developer and publisher of International Standards. ISO is a network of the national standards institutes of 159 countries, one member per country, with a Central Secretariat in Geneva, Switzerland, that co-ordinates the system.

PTP meets or exceeds the following NIST standards:

USA Federal Information Processing Standards FIPS 180-2  
USA Federal Information Processing Standards FIPS 140-2  
USA Federal Information Processing Standards FIPS 46-3

U.S. National Institute of Standards and Technology ([www.nist.gov](http://www.nist.gov))

FIPS Publications are issued by NIST after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Reform Act of 1996 (Public Law 104-106) and the Federal Information Security Management Act of 2002 (Public Law 107-347). The Computer Security Division (<http://csrc.nist.gov>) is one of six divisions within NIST's Information Technology Laboratory. The CSD mission is to provide standards and technology to protect information systems against threats to the confidentiality of information, integrity of information and processes, and availability of information and services in order to build trust and confidence in Information Technology (IT) systems.

## 5.2 Identity Verification

One of the reasons for Digital Certificates and Certificate Authorities and all the complexity that entails, is identity verification. Identity verification in PTP employs a manual method to replace certificates.

When you receive a Public Key file from a new Contact, there is a field called Identity-Code that displays in the Contact List. This Identity-Code is only known to the person who generated the Public Key file. If you wish to verify the Contact, it is assumed you know enough about them to contact them in person, by phone/fax or by regular mail and ask them for their Identity-Code. You can then compare what they tell you to what is shown in the Contacts List. If the codes do not match, then the User Identity (name) of the person in the Public Key file does not match the person you have contacted.

In order to know who on your Contact list has been verified, the Identity-Code is displayed in **orange** when a Contact has been added but not verified. After verification, you can double click on the Identity-Code value for a Contact and the Identity-Code will be displayed in **green** text. This tells you which Contacts have been verified.

## 5.3 Changing Your Password

### **WARNING!**

Your Private and Public keys are partially based on your database Password. Therefore, if you change your password, your keys will also change. This means that files encrypted with the old password can no longer be decrypted. It also means your Public Key information stored in all your Contact's databases can no longer decrypt messages sent from you and you can no longer decrypt messages sent by your Contacts with the old Public Key.

So if you wish to change your password, you must first decrypt any files you have encrypted for yourself and re-encrypt them after changing your password.

You must also send new Public Key files to your Contacts after changing your password.

For these reasons, **you should only change your password if you have reason to believe it has been compromised.**



## 6 Database Sharing

### 6.1 Sharing Contact Databases over a network

The **Professional edition** includes the ability for PTP users to share their Contact databases over a network. In this case, one PTP user will designate their instance of PTP to act as a master repository of Contacts. Other instances of PTP can then synchronize their Contact databases with the master database. This builds a master database of Contacts and disseminates those Contacts to the PTP users on the network.

So, this sharing function employs a single PTP instance as the master (or server) Contact database and is said to share it's Contacts with other PTP instances. It also employs one or more other instances of PTP on the network which synchronize with the master.

When synchronizing, a PTP instance will contact the master instance over the network and obtain the master database Contact list. The synchronizing instance will compare that list to it's local Contact database and determine which master Contacts should be downloaded and added or updated in the local database and which local Contacts should be sent to the master to be added or updated on the master database. Once the lists are made, the synchronizing instance moves the Contacts over the network and the local and master Contact databases are updated. Synchronization is requested by clicking on the synchronization button on the toolbar.

Contacts are only synchronized if they have been identity verified (Identity-Code marked ) and are not marked private (.

Contact synchronization actions are recorded in the Windows Application Event log.

**Note:** If your computer uses firewall software such as Windows Firewall or ZoneAlarm or some other network protection software, you will need to configure that software to allow access to the port number used by PTP. The port number defaults to 1088 but can be set to any value you prefer. If sharing, then the port must be allowed to accept incoming connections. If syncing, then the port must be allowed to perform outgoing connections.

### 6.2 Sharing Settings

Database Sharing is configured on the Database Sharing Settings screen. Select either Share or Synchronize.

#### Share your Contacts with other users

Select this option to share your local database with others. This makes your database the master database.

#### Password

Enter an optional password that must be supplied by any users who wish to synchronize with you.

#### Accept Contacts from sharing users

Select this option to allow synchronizing users to upload their Contacts to your database (master).

#### Synchronize your Contacts with another user

Select this option if you wish to synchronize your database with the shared master database. This causes the synchronize button to appear on the toolbar.

### System

Enter the name or IP address of the computer that is sharing its database.

### Password

Enter any password needed to connect to the sharing user.

### Send your Contacts to the sharing user

Select this option to upload your Contacts to the sharing (master) database.

### Synchronize Contacts on login

Select this option to automatically synchronize Contacts after database login.

### Select Contacts to Synchronize

Normally, all candidate Contacts are synchronized automatically. Select this option if you wish to review the candidate Contacts and manually select which Contacts are synchronized. When selected, after the candidate Contact list is obtained from the sharing user, the PTP screen will shift so that only the Contacts list is accessible and the Contact list will be replaced with a list of the synchronization candidates with check boxes. Check the Contacts you want to download to your database and click **Download**. Click **Cancel** to stop the synchronization operation. Once download is complete, the screen will return to normal display.

### Network Port

This value is the network port number used when connecting to the sharing user. This value must be the same for all PTP users on the network and typically does not need to be changed from the default value.

# Index

## - A -

ASCII 10  
attachments 15

## - B -

Backup 10  
binary 10  
body text 15

## - C -

Certificates 19  
Contact 8, 10, 15, 19  
Contacts 7  
container file 8  
Context Menu 14  
CypherMax 18

## - D -

Data Vault 5, 7, 9  
database 4, 5  
Decrypt Directory 10  
default email account 10  
default email client 7  
Digital Certificates 19

## - E -

Edit email address 8, 15  
Editions 4  
email 5, 7, 8, 10, 15  
email account 10  
Email body text replacement 12  
Email body text Substitutions 12  
Error sending email: (3) Login Failure 7  
Export Contacts 10  
Export Database 10

## - F -

FIPS 18  
Firewall 20

## - H -

Home Directory 7, 10

## - I -

Identity-Code 19  
Images 15  
Import Contacts 10  
Import Database 10  
Inactivity Timeout 10  
install 4  
ISO 18

## - N -

Navigation 7  
Navigation window 9, 10  
Network 20  
Network Port 20  
NIST 18

## - O -

Outlook 15  
Outlook Add-in 4  
Outlook User Fields 15

## - P -

Pass Phrase 5, 7, 10  
Password 5, 18  
Port 20  
Private Flag 20  
Processing List 7, 8, 9  
Professional Edition 20  
Public Key 5, 8, 19  
Public Key File 15

**- R -**

Replacement Text file 12  
RestartExplorer 4  
RSA 18

**- S -**

Selective Synchronization 20  
Send Key File 15  
Settings 10  
Sharing 20  
Sign 7  
Signature Text file 12  
Signing 5  
Standards 18  
Start Menu 4  
Start Time 10  
Startup 10  
Synchronizing 20

**- T -**

Task Tray 10  
Timeout 15

**- U -**

uninstall 4  
User Fields 15  
User Identity 5  
User Tag 7

**- W -**

Windows Explorer 14  
Windows Explorer reload 4  
Windows Mail 15  
Working Directory 7, 8, 9, 10