Person To Person™

Personal Encryption Tool

By **PTP Security**

Person To Person

Revised Tuesday, December 09, 2014.

Table of Contents

Part 1 Introduction 5

1 Welcome ... 5
2 Installation ... 5
3 Theory of Operation ... 6
4 Support ... 7

Part 2 Desktop Client 8

1 Desktop Operation ... 8
2 Contacts ... 9
3 Signing Files ... 9
4 Public Key Files ... 9
5 Encrypting Files ... 10
6 Decrypting Files ... 11
7 AutoCrypt Self-Decrypting Files ... 11
8 Data Vault ... 12
9 Database/Contact List Export/Import ... 13
10 Settings ... 13
11 Signature/Replacement Files ... 16
12 Contact Database and Windows User Name ... 17
13 Command Line Operation ... 17
14 Windows 8 ... 20

Part 3 Windows Explorer 21

1 Windows Explorer Operation ... 21

Part 4 Email Client Integration 22

1 Email Client Operation ... 22
2 Outlook Email Client Operation ... 22
3 Outlook Account Security ... 26

Part 5 About Encryption 28

1 CypherMax ... 28
2 Identity Verification ... 29
3 Changing Your Password ... 29

Part 6 Professional Edition 31

1 Professional Edition..... 31
2 Administrative User Identity..... 31
3 Sharing Contact Databases over a network..... 31
4 Sharing Settings..... 32

Index 34

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. PTP meets International and Federal security standards and supports compliance with USA security law.

Person To Person is directly integrated with Windows Explorer and optionally with Outlook to make signing, encryption or decryption quick and easy. Other email programs may be used by attaching files encrypted with the PTP client outside of the email program.

Person To Person is supported on Windows XP and later.

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

The **Free** edition allows unlimited decryption, signing of files to anyone and encryption of files for yourself. Encrypting files for yourself allows you to secure data for your personal use

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 Free edition includes the **Data Vault.** . The Data Vault is a single storage area where you can store files in an encrypted form (to yourself) and easily retrieve them later. This can be more handy than keeping important files in various locations on your computer.

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. Standard edition also includes **AutoCrypt**, which provides a less secure option to send encrypted information to persons who do not have PTP installed on their computers.

The **Email** edition adds direct integration with Outlook 2003/2007/2010/2013. 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 the Outlook integration Add-in. Selecting the 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, 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 password, 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.

AutoCrypt is the final method for secure communications. Intended for sending encrypted files to a person who does not wish to install PTP to decrypt files. In this case, the files to be sent are encrypted with standard 256-bit **AES** encryption using a password you supply and packaged into an **Self-Decrypting** executable file. The receiver of such a file simply runs that file to decrypt its contents. The self-decrypting file will prompt for the password and if verified, decrypt its contents without needing any other software installed on the recipient's computer. Secure transmission of the password to the recipient is your responsibility.

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.

The Navigation window starts in 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 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.

When dragging files from the Working Directory to the Processing List, they are "copied", that is, they will be remain in the Working Directory after encryption/decryption is completed. To move files, that is to delete them from the Working directory after encryption/decryption, press and hold the control-key as you drag the file(s). You may also select files first with the left mouse button and then drag them while holding down the right mouse button to move the files. You may drag and drop files from Windows Explorer into the Working Directory but not directly to the Processing List.

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 Contacts

Contacts are the persons you can exchange encrypted messages with. 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.

Contacts are normally created automatically by the exchange of Public Key Files. However, to facilitate the use of the AutoCrypt feature, you may create new Contacts by right-clicking on the Contacts window. Contacts created in this way may only be used when creating AutoCrypt Self-Decrypting files. The idea is to allow you store the password for the Self-Decrypting file and optionally an email address if you wish to email Self-Decrypting files. If you select a Contact before clicking the toolbar button to create a Self-Decrypting file, any recorded password will be pre-filled in the Self-Decrypting file password entry window. Same for the email address if you are creating and emailing a Self-Decrypting file.

When you create a new contact, it will be entered into your Contacts List as "New Contact". You must double click on the Contact name to change it to the actual Contact name you wish to use. Double click on the password and email areas to change them.

2.3 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 that 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 password in the signed file, you must enter the password on the Settings screen. The password is included in all files signed. The receiving user will prompted to provide the password 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.

2.4 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 senders User Identity and Public Key will be added 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 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.

2.5 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 that 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 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.

2.6 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 contents. 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).

When a .PTPZ file is on the Processing List, if right-click on it, the context menu will contain the Open command. If you click open, the .PTPZ file will be opened and the Process List will be replaced with a list of the encrypted files contained in the .PTPZ file. The Process List color will change to salmon to indicate you are looking at a listing of a .PTPZ file and the .PTPZ file name will be shown above the Processing List. The purpose of this list is two fold. It allows you to see the contents of a .PTPZ file and you can select one or more files and right-click then to open a menu of functions you can perform on them. Currently, you can decrypt the selected files from the .PTPZ file to the Working Directory.

2.7 AutoCrypt Self-Decrypting Files

Once files have been added to the Processing List, you can add them to an **AutoCrypt** Self-Decrypting File by clicking the **Encrypt to Self-Decrypting File** tool bar button above the Processing List window. Files on the Processing List are encrypted and placed into a new self-decrypting executable file with the same name as the first file on the list, but with the **.exe** 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 plan to email the .exe file outside of PTP, you may want to ZIP the .exe first as files with the .exe extension can be blocked by firewalls, anti-virus software and some email servers.

By clicking the **Encrypt to Self-Decrypting File and Mail** tool bar button, you can process the file(s) on the Processing List and have the resulting container file automatically attached to a new email message. In this case, the attached file will have the **.ptx** extension instead of .exe (**see below**). Your default email client will appear and all you have to do is fill in the Contact's email address. If you have selected a Contact in the PTP Contact list and that Contact has an email address, 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.

Password

An AutoCrypt Self-Decrypting File is an executable file (.exe), that when run, will automatically decrypt it's contained files into a selected directory. When an AutoCrypt file is created, you will be prompted for a password which is used to secure the file. The user who runs the AutoCrypt file to obtain it's contents must supply this password to decrypt the file. You do not need to have PTP installed on a computer to run (decrypt) an AutoCrypt file. This means AutoCrypt is intended for sending encrypted files to people who do not have PTP. You will have to share the password with your target users without assistance from PTP. You may enter a default password on the Settings screen to pre-fill the password prompt screen. The password prompt screen also allows you to override the file extension of the Self-Decrypting

file (see .ptx Files below) selected by PTP (not supported when encrypting from Outlook Add-In).

If you selected a Contact prior to creating the Self-Decrypting file, and that Contact has a password defined, that password will automatically be used to create the Self-Decrypting file and you will not be prompted. To enter a password for a Contact, place the cursor over the password area on the Contact's information line and double click. This will open an entry box for the password.

Additionally, when the Outlook Add-in is installed and you send email, the Add-in will look up the Outlook Contact in the Outlook address book and check the Contact User Fields for a field called **PTP Self-Decrypting Password.** If that field is found, the messages to the Contact will use Self-Decrypting files as the encryption scheme using the field value as the password. See Email Client Operation for more information.

.ptx Files

Because of the problems with .exe files being blocked by firewalls, anti-virus and some email servers, when PTP emails a Self-Decrypting .exe file it renames the **.exe** to **.ptx**. The .ptx file will pass through firewalls, anti-virus and email servers.

In order to run an AutoCrypt file that has the **.ptx** extension, you must change (rename) the **.ptx** extension to **.exe** so that Windows will execute the file. If the .ptx file was received in an email message, you must first save it to a folder before you can do the rename and execute steps. PTP creates AutoCrypt attachment files with the .ptx extension so that the files will pass through email and firewall security systems that typically block .exe files.

ptxLauncher

This renaming scheme is inconvenient for the recipient of a .ptx file because of the steps needed to decrypt it. To make decryption of .ptx files easier, the **ptxLauncher** utility was created. ptxLauncher is a simple program that can be installed on the recipients computer to automatically save, rename and execute a .ptx file. Once ptxLauncher is installed, you can just double click on .ptx files in your email client (or on disk) and the .ptx file will be saved to a temporary directory, renamed, decrypted and then a Windows Explorer instance will open to that directory so you can easily access the newly decrypted file (s). **ptxLauncher.msi** is the install file for ptxLauncher and is included in the PTP install directory so you can send it to Contacts you send AutoCrypt files to.

Note that AutoCrypt files do not use PTP's CypherMax encryption technology. AutoCrypt files use industry standard **256-bit AES** encryption.

You must have a **Standard Edition** or higher license to encrypt files with AutoCrypt.

2.8 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 right-click context menu on files in the Working Directory. Dragging files moves them from the Working Directory and control-key or right mouse button while dragging, will copy them from the Working Directory. 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. If you decrypt or 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. There are two exceptions to this manual return of the file to the Vault:

The right-click context menu will also display **Open (tracked)** and **Open with Notepad (tracked)** actions. Tracked means that PTP will decrypt the file to a hidden location and then launch the application associated with the file (or in Notepad without regard to the file's extension) and then PTP will monitor that application process and when you exit the application, PTP will automatically return the changed file back into the Vault and delete the plain text version from disk. Tracking works for Notepad and many other applications. Unfortunately, there are some applications which (due to their design) cannot be tracked. Microsoft Word and Excel are examples of such untrackable applications. If you Open a file with tracking and the associated application cannot be tracked, the application will still open. However, any changes to that file will be lost when you exit. You will be warned when you start an untrackable application and you should exit that application making no changes to the file. For such files, you will need to decrypt or open (without tracking) to the Working Directory and manage the files return to the Vault manually.

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, it's original location and the first location on the decrypt list will be shown in the tooltip for the file.

2.9 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.

2.10 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 Outlook Toolbar

Turn on or off PTP support in email clients. The email integration support (Add-in) for the Outlook email client must be installed first. See Installation.

Email Start Timeout

When using PTP with Outlook, if PTP desktop client is not running when Outlook needs it, Outlook with 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 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 with 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. Set to zero to disable the timeout.

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. Set to zero to disable the timeout.

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.

Encryption Method

You can select the encryption method used by PTP. Choose from CypherMax (RSA based), AES or TDEA encryption schemes. CypherMax is the most secure option.

Enable Outlook Contact Lookup

When using the Outlook Add-in to do encryption of outgoing messages from within the Outlook email client, the Add-in will do a lookup operation on the Outlook Contact database to determine if the target contact has User Fields defined that control how encryption is performed. This lookup can incur significant overhead. If you are not using Outlook Contact User fields, you can disable the lookup.

Encryption Expiration (Days)

You can set encrypted files to expire, that is, fail to decrypt, after some number of days added to the current date. Zero days disables this feature. Only applies to files encrypted with CyhperMax.

Signing/Default Password

When Signing a file, you may optionally include a password of up to 32 characters. Users decrypting such a Signed file will be prompted for this password. This is an optional additional security feature for Signed files. A password entered here will also be used as the default password assigned to Self-Decrypting 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.

2.11 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 be overlayed 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**. **PTPSignatureSfx.txt** is used when the email message is encrypted with AutoCrypt. 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.
[VERSION]	Version number of the PTP product.

[ICON]	HTML link to the PTP product icon.
[COPYRIGHT]	PTP copyright notice.
[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.

Note: When doing message content replacement in Outlook, PTP uses HTML formatted messages and so supports rich formatting of the replacement text. When doing email messages from the PTP client (and the Explorer context menu), PTP is unable to use HTML formatting and reverts to plain text formatting. For this reason there are two additional replacement text files: **PTPReplacementPlain.txt** and **PTPSignatureSfxPlain.txt** that provide the replacement text in simpler format, and are used by the Client.

2.12 Contact Database and Windows User Name

PTP stores your Contacts list in a "database" on your PC. This database is located in a directory under your Local User Application Data directory. As a result there is only one database, and therefore User Identity, per Windows login. You may have multiple User Identities and Contact databases on a single PC, but each must be created under a different Windows login.

2.13 Command Line 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. This will present the Graphical User Interface (windows) discussed in earlier sections of this document. It is possible to operate PTP from the Windows command line using the Command Line Interface (CLI). To access the CLI, open a Windows command prompt window in the directory where you wish to operate. Then execute PTP by typing a command of the following format:

> path to PTP install directory\ptpclient.exe /cli <command> <options>

An example of this might be:

> C:\Program Files\PTP Security\Person To Person\ptpclient.exe /cli /help

You will need to use the path to your PTP install directory or you can add the PTP directory to your system's PATH environment variable so you can just type ptpclient.exe from any location.

In CLI mode, PTP will execute the single command specified and then exit. You must specify your database password for any operation other than displaying the help.

The commands are:

/keyfile (/kf)
Generate your Public Key File in the working directory.

/keyfile-mail (/kfm)
Generate your Public Key File and attach to an email.

/sign=sourcepath (/s=sourcepath)
Sign the selected file(s).

/sign-mail=sourcepath (/sm=sourcepath)
Sign the selected file(s) and attach to an email.

/decrypt=path (/d=path)
Decrypt the selected container file into the working directory.

/encrypt=Sourcepath (/e=sourcepath)
Encrypt the selected file(s) into a container file in the working directory.

/encrypt-mail=sourcepath (/em=sourcepath)
Encrypt the selected file(s) into a container file and attach to an email.

/encryptsfd=sourcepath (/esfd=sourcepath)
Encrypt the selected file(s) into a self-decrypting file in the working directory.

/encryptsfd-mail=sourcepath (/esfdm=sourcepath)
Encrypt the selected file(s) into a self-decrypting file and attach to an email.

/list=path (/l=path)
List the contents of a **.ptpz** container file.

/help (/h, /?)
Display the help text.

The Options are:

/password=value (/pw=value)
Specify database password (required).

/workingdir=path (/wd=path)
Specify target directory for output. Defaults to source directory.

/contact=name (/con=name)
Specify target contact for encryption. Defaults to you.

/selfdecryptpassword=value (/sdpw=value)
Specify required password for self-decrypting files.

/signingpassphrase=value (/snpw=value)
Specify optional passphrase for signed files.

/encryptmethod=CypherMax|AES|TDEA (/emeth=CypherMax|AES|TDEA)
Specify encryption algorithm. Defaults to CypherMax.

/targetfile=name (/tf=name)
Specify target container file name (no path or extension) for encryption.

/deletesource (/ds)
Delete source file(s) after encryption.

/update (/u)
Update files in existing **.ptpz** container file during encryption.

/recurse (/rec)
Recurse subdirectories in the source path.

/restore (/res)
Decrypt files to their original location on disk instead of working directory.

/overwrite (/ow)
Overwrite target file when encrypting.

/select=pattern (/sel=pattern)
When listing/decrypting from **.ptpz** container file, select file(s) to decrypt from the container with pattern.

/exclude=pattern (/ex=pattern)
When encrypting/signing, select file(s) to exclude from the operation.

/format=n (/f=n)
When listing container file, sets listing format.
0 = file path then file name
1 = file name then file path

/close (/c)
When running on Windows 2000, the output of command line mode is displayed in a new window separate from the one that starts PTP. That window will remain open for viewing until closed by hitting enter. This option will automatically close that window when the command line mode operation is completed.

Notes

Value right of equal sign must be enclosed in double quotes if it contains embedded spaces.

Source paths may contain windows wild cards for multiple file operations.

The working directory defaults to the source directory for encryption and the current directory for decryption. The source directory defaults to the current directory if not specified.

When encrypting, a single source file will be encrypted into a **.ptp** container file in the working directory. The name of that file is the same as the source file but with the **.ptp** extension. You can change the working directory with the **/workingdir** option and change the target file name with the **/targetfile** option (again, no extension).

When encrypting, a multiple source files will be encrypted into a **.ptpz** container file in the working directory. The name of that file is the same as the first source file but with the **.ptpz** extension. You can

change the working directory with the **/workingdir** option and change the target file name with the **/targetfile** option (again, no extension).

When encrypting, and the source path specifies a directory instead of a file, you can use the **/recurse** option to process all subdirectories in the source directory.

When encrypting, if the target file is an existing **.ptpz** container file, that file will be updated with the encrypted files. New files are added and existing files are overwritten.

If you encrypt files using the **/contact** option to specify a Contact other than yourself, you will not be able to decrypt the resulting container file. Only the specified Contact will be able to decrypt the file.

When listing or decrypting, the path points to a single container file of type **.ptp** or **.ptpz**. When you decrypt, the decrypted files are placed in the working directory. You can use the **/restore** option to decrypt files to their original directory.

When listing or decrypting from a **.ptpz** container file, you can use the **/select** option to specify a wild card pattern to select files from the container.

2.14 Windows 8

Person To Person is compatible with Windows 8, but runs on the "desktop" where non-Metro Windows 8 applications run. The desktop is essentially Windows 7. There is no Metro version of Person To Person at this time.

When Person To Person is installed, all of the items added to the Windows Start Menu will be added as individual applications on the Metro Start Screen. We don't have control over that at this time. You can select, right-click, and unpin any of the choices you do not want on the Metro Start Screen. Such unpinned choices can still be found by right-clicking the Metro Start screen and clicking All Apps or by switching to the desktop and using Windows Explorer to locate the ProgramData\Start Menu folder. The Person To Person Start Menu is found in that folder.

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.

If you press and hold the shift-key when making a selection on the context menu, the source file(s) will be deleted after processing.

4 Email Client Integration

4.1 Email Client Operation

You may use Person To Person with any email client by simply attaching files encrypted outside the email client with the PTP client. Further, in the PTP client, you have the option to encrypt and generate an email message with the encrypted file already attached and possibly a Contact email address pre-filled. These methods operate without modifying or directly integrating with your email program.

However, these manual methods do not encrypt the body text of the email message or any other attachments. You may optionally integrate PTP directly into the **Outlook** email client for more efficient operation and to provide automatic encryption/decryption of message body text and any attachments a message may have. See the next topic for more information on Outlook integration.

4.2 Outlook Email Client Operation

You may install the optional integration component for use with Outlook during installation. If you do install this option, it will be enabled by default. You can enable/disable Outlook encryption on the PTP Settings screen.

Email integration is available for **Outlook 2003/2007/2010/2013**. You must have an **Email or Pro Edition** license to use Outlook integration.

If Outlook integration is installed and enabled, when you start your Outlook, you will see a new PTP tool bar below the regular tool bars. This tool bar, along with a menu on Outlook'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 Body

Automatically decrypt the message body on incoming email messages resulting in the message body being in clear text form. If not selected, the message body will remain encrypted, as an attachment to the message. You can click on such an attachment later to invoke the PTP program to decrypt the file on demand. You can also use the Decrypt Message toolbar button (see below) to decrypt the message body attachment.

Decrypt Attachments

Automatically 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. You can also use the Decrypt Message toolbar button (see below) to decrypt the attachments.

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) or to the sender of the currently selected email message(s). This option also appears on the Tools pull down menu and on Contact/Message context menus. 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. Outlook will submit the message recipient's name and email address to the PTP program 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 cannot be performed. In that case you will be shown a warning and given the option to send the message as a Self-Decrypting file, unencrypted or to cancel the message.

When a message or attachments are automatically decrypted 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 in the PTP program 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. 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.

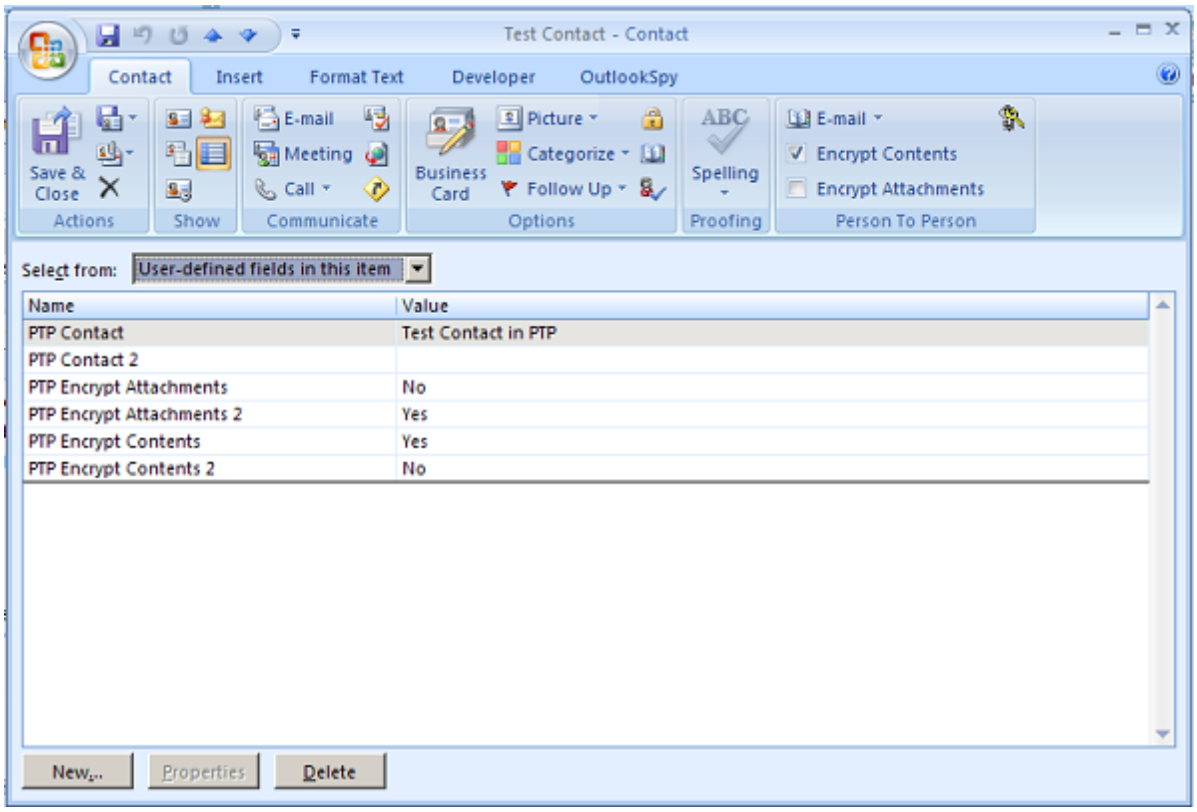
Currently, in Outlook, only Mail Messages are processed by PTP. Appointment, meeting request and task messages are not supported.

In the following discussion, **Contact** refers to an encryption Contact in the PTP programs Contact database. Lower case **contact** refers to an Outlook contact in the Outlook contact database.

In Outlook, you may create **User-Defined Fields** for Outlook contacts that will enable automatic encryption. This allows you to 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 on the global or message compose toolbar. The User-Defined Fields are:

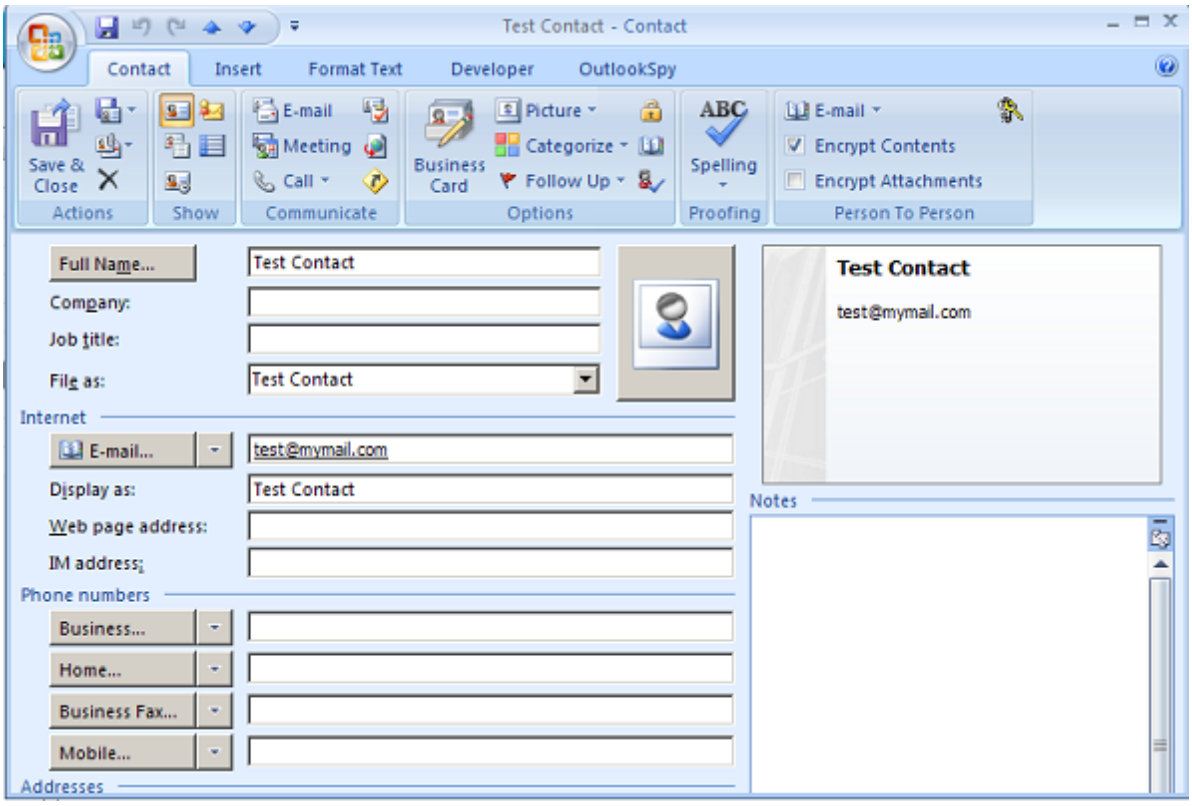
PTP Contact	Text field type. Set to name or email address that will be used to look up the encryption Contact in the PTP database. Overrides normal use of contact email address and contact name.
PTP Encrypt Contents	Yes/No field type. If Yes, messages to the contact will be fully encrypted. If No, encryption is controlled by the toolbar options selected on the compose window.
PTP Encrypt Attachments	Yes/No field type. 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.
PTP Self-Decrypting Password	Text field type. If set, messages to the contact will use Self-Decrypting files as the encryption scheme using this password.

In Outlook, there are 3 email addresses available for a contact. You can define the above User-Defined Fields for each of the 3 addresses. For example, **PTP Contact** associates with email address 1. **PTP Contact 2** associates with email address 2 and **PTP Contact 3** associates with email address 3.



In order for User-Defined Fields to be effective, PTP must search your Outlook contact database for the message recipient's contact record to see if it has User-Defined Fields and if so, determine how they will affect the encryption process. This contact lookup can take significant time if your contact database is large or if you are attached to an Exchange server. If you are not using User-Defined Fields, you can disable this lookup process on the Settings screen.

In Outlook 2007/2010, on the detailed contact window, the Ribbon Bar will contain check boxes to set the PTP Encrypt Contents/Attachments User-Defined Fields for you. Use the E-mail drop down to select which of the 3 email addresses you want to set and then check the appropriate box. In Outlook 2013, to see the detailed contact window, you must click on the **View Source** link on the basic contact display.



In Outlook, if a message to be sent is encrypted, PTP can keep a plain text copy of the encrypted message if you select **Save Original Copy to Sent Items** on the PTP section of the Tools pull down menu. If this option is selected, a plain text copy of the message to be encrypted is placed in the Sent Items folder. When the encrypted message is sent and moves to Sent Items, PTP will attach the plain text copy to the encrypted message. This provides a readable copy of the encrypted message for your records.

Please note, this function only attaches the original copy to the sent message when the message is sent using a **POP3** mail account. If the account the message is sent with is not POP3, then the original copy will be saved to a disk file in the **PTP Sent Items** folder located in your **My Documents** or **Documents** folder. See the next topic for additional information about Outlook Accounts.

4.3 Outlook Account Security

In Outlook, you can create email Accounts using various email protocols, such as POP3, IMAP, Exchange and others to connect to email servers. Please be aware there are security ramifications attached to which type of Account you use to send messages.

In short, any Account type other than POP3, may and likely will, store messages in any folder under that Account on the server. This means that any unencrypted messages will be stored in plain text on the server, including messages you delete. Additionally, messages you delete may be retained by the server if it offers undelete capability. In short, your messages will be stored in plain text form on the server for an unknown period of time and may be outside your control.

Technically, the problem comes from the fact that non-POP3 Accounts can and do store their data on the server instead of locally on your PC. This means that any messages under such an account cannot

be relied upon to be secure. Now if you encrypt a message under such an account with PTP the message will be encrypted on the server and secure, but if you were to attach an original plain text copy to the encrypted message in the Sent Items folder, that plain text copy would be moved to the server along with the encrypted part of the message. That is why PTP saves the original copy (if you select that option) to a disk file outside of Outlook with non-POP3 Accounts. Even saving messages to a different folder under a non-POP3 Account is an exposure because any message that gets deleted under a non-POP3 Account will be moved to the Deleted Items/Trash folder on the server.

Now some email servers may do their own encryption of stored messages or provide some other form of protection, but you will be relying on the server and its administrators to protect your unencrypted message content.

So with non-POP3 Accounts, there is significant security exposure for any non-encrypted message content. POP3 Accounts always store their data on the local PC and so do not have this security exposure. For that reason, we recommend always using POP3 Accounts when sending sensitive messages that you decide you want to encrypt with PTP.

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 of 384 bits and large data blocks to create an advanced more secure 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 FIPS 180-2 for Secure Hash Algorithms.

CypherMax Encryption exceeds USA 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 encryption software standards.

PTP meets or exceeds the following ISO standards:

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

ISO (International Organization for Standardization wwww.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)

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.

PTP also supports the use of the **AES** standard with a key length of 256 bits and the **TDEA** standard with a key length of 168 bits.

Person To Person and Data-in-Motion.

PTP meets the data-in-motion encryption requirements of HIPAA, GLBA, California SB-1386 and Sarbanes-Oxley.

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 Professional Edition

6.1 Professional Edition

The **Professional Edition** is intended to support using PTP in organizations. Each person in an organization will have PTP installed on their own PC and have their own Contacts database and login password. To facilitate the use of these individual PTP databases in organizations, there are two special features included in the Professional Edition. These are:

Administrative User Identity

Sharing Contact Databases over a network

6.2 Administrative User Identity

Because each user of PTP has their own Contacts database secured by their own password, access to a user's Contacts database may be lost if the user forgets their password or a user leaves the organization without leaving a record of their password.

As a solution to this problem, Pro Edition instances of PTP allow the registration of an Administrative User Identity in addition to the normal User Identity. This Administrative User Identity is licensed from your distributor and may be applied to the PTP databases in your organization. Once applied, you may login to that database using either the owner user's password or the Administrator password.

To apply the Administrator User Identity to a PTP database, the database owner user must be logged on. Then on the Help menu, select Register Administrator.

6.3 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.

6.4 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 it's 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

- . -

.exe 11
.ptx 11

- A -

Accounts 26
Administrative User 31
Administrator 31
AES 6, 11, 13, 28
ASCII 13
Attachments 22
AutoCrypt 6, 9, 11
AutoCrypt Replacement Text files 16

- B -

Backup 13
binary 13
Body text 22

- C -

Certificates 29
CLI 17
Command Line 17
Contact 9, 13, 22, 29
Contacts 8, 9
Container File 10, 17
Context Menu 21
CypherMax 13, 28

- D -

Data Vault 6, 8, 12
Database 5, 6, 17
Data-in-Motion 28
DEA 28
Decrypt Directory 13
default email account 13
default email client 8
Digital Certificates 29
DOS 17
Drag and Drop 8

- E -

Edit email address 10, 22
Editions 5
Email 6, 9, 13, 22
email account 13
Email body text replacement 16
Email body text Substitutions 16
Email Client 22
Encryption Expiration 13
Error sending email: (3) Login Failure 8
Exchange 26
Expiration 13
Export Contacts 13
Export Database 13

- F -

FIPS 28
Firewall 31

- G -

GLBA 28

- H -

HIPAA 28
Home Directory 8, 13

- I -

Identity-Code 29
Images 22
IMAP 26
Import Contacts 13
Import Database 13
Inactivity Timeout 13
install 5
ISO 28

- K -

Key Length 28

- L -

Listing .PTPz container files 11

- N -

Navigation 8
Navigation window 11, 13
Network 31, 32
Network Port 31, 32
NIST 28
Notepad 12

- O -

Original Copy 22
Outlook 22
Outlook Accounts 26
Outlook Add-in 5
Outlook contact lookup 13, 22
Outlook User-Defined Fields 22

- P -

Pass Phrase 6
Password 6, 9, 13, 28
POP3 22, 26
Port 31, 32
Private Flag 31
Private Key 6
Processing List 8, 10, 11
Professional Edition 31, 32
ptxLauncher 11
Public Key 6, 9, 29
Public Key File 22

- R -

Replacement Text files 16
RestartExplorer 5
RSA 28

- S -

Sarbanes-Oxley 28
Save Original Copy 22, 26
SB-1386 28
Selective Synchronization 32
Self-Decrypting 6, 9
Self-Decrypting file 11
Self-Decrypting File Default Password 13
Send Key File 22
Sent Items 22
Settings 13
Sharing 31, 32
Sign 9
Signature Text file 16
Signing 6
Signing Password 13
Standards 28
Start Menu 5
Start Time 13
Startup 13
Synchronizing 31, 32

- T -

Task Tray 13
TDEA 28
TDES 13
Timeout 22
Tracking 12

- U -

uninstall 5
User Identity 6, 17, 31
User Tag 8
User-Defined Fields 22

- V -

Vault Tracking 12

- W -

Windows 8 20

Windows Explorer 21
Windows Explorer reload 5
Windows Login 17
Working Directory 8, 10, 11, 12, 13, 17