

PIE (Client) – Private Information Encryptor - Overview

PIE (Private Information Encryptor) is a program that enables sensitive information to be shared between participating parties, across an insecure medium such as the Internet or to simply encrypt computer files on a disk to preserve their confidentiality.

PIE encrypts/decrypts files using PGP (Pretty Good Privacy) which is a well-known encryption/decryption system that is highly trusted and used worldwide by thousands of businesses and government agencies.

The system is based on what are known as PUBLIC and PRIVATE Key pairs which are essentially just text files. The PUBLIC and PRIVATE Key file pairs are mathematically related to each other and can be easily created by PIE by selecting 'Create Key Pair' from PIE's 'Keys' menu.

A PUBLIC Key file is not secret and can be given to anyone. Typically, a person, or a business, would only have one pair of PUBLIC and PRIVATE Key files.

PRIVATE Key files must be kept secret and not shared.

PIE is typically used to:

- Encrypt files prior to attaching them to an email for onward transmission over the Internet.
- Encrypt files on disk thus preserving their confidentiality.

PIE Versions

The PIE system has the following two versions:

- Professional – This version has more options and allows users to create Public and Private Key file pairs.
- Client – For users responsible for just sending and receiving encrypted information/files.

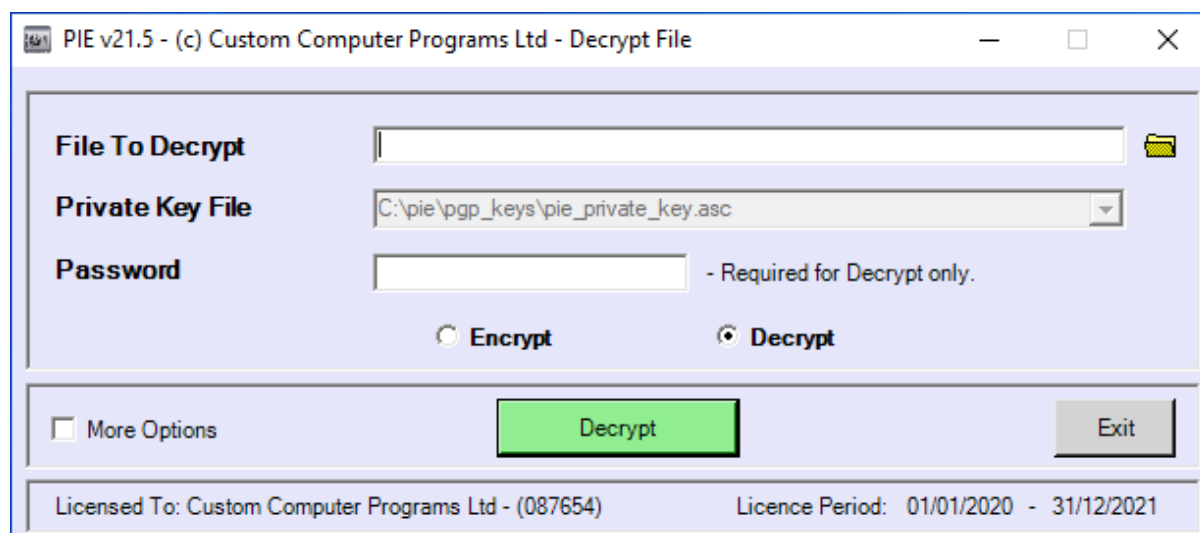
PIE Design Objectives

A major design objective of the PIE Client version was to simplify the system as much as possible and that's why the options available are limited.

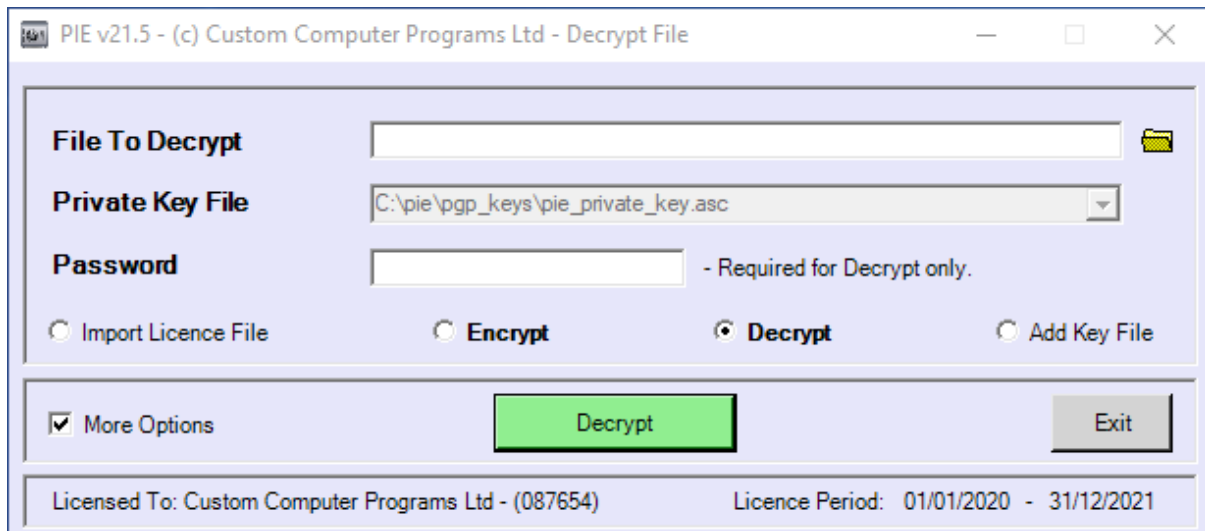
The design of the Client version has been targeted at those who are responsible for the sending and receiving of encrypted information/files. The Client version does not provide an option to create a Public and Private Key pair but this functionality is available within the Professional version.

PIE Screens

On starting PIE, the following screen is displayed, although the licence details will be different:



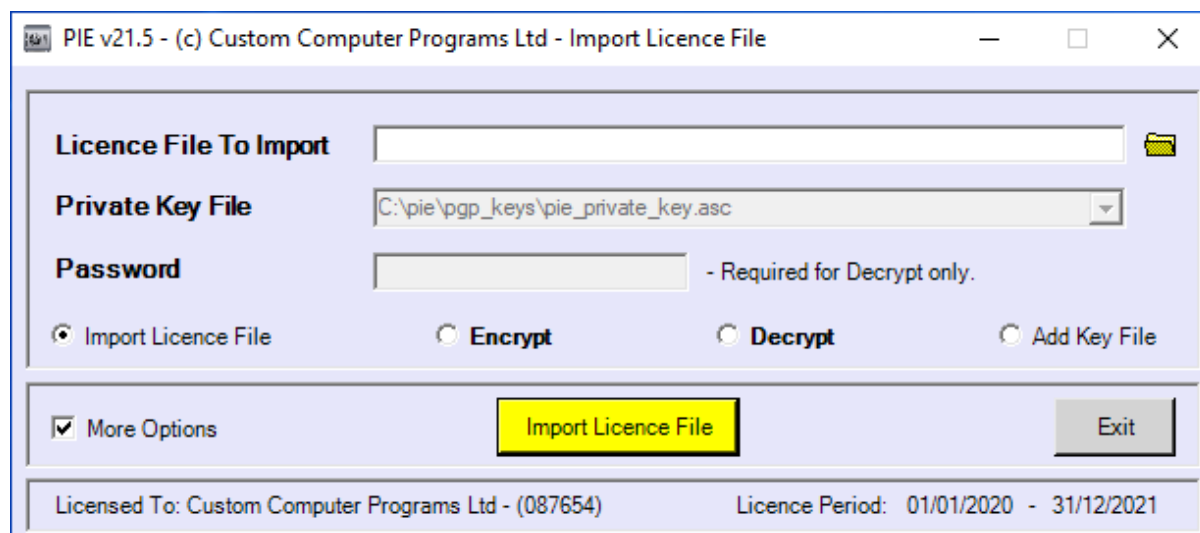
The screen above shows the 'Encrypt' and 'Decrypt' options which are the two options that will be predominately used. However, on checking the 'More Options' checkbox, the screen offers the 'Import Licence File' and 'Add Key File' options as shown below:



On selecting one of the four radio buttons displayed, the screen fields change in accordance with the option selected. The following describes the screen displayed when each one of the four radio buttons are selected.

Selecting Import Licence File

On selecting the 'Import Licence File' radio button, the following screen is displayed:



The screenshot shows a Windows-style dialog box titled "PIE v21.5 - (c) Custom Computer Programs Ltd - Import Licence File". The dialog has a light blue background and contains the following elements:

- Licence File To Import:** A text input field with a folder icon on the right.
- Private Key File:** A dropdown menu showing the path "C:\pie\pgp_keys\pie_private_key.asc".
- Password:** A text input field with the note "- Required for Decrypt only." to its right.
- Radio Buttons:** Four radio buttons are present: "Import Licence File" (which is selected), "Encrypt", "Decrypt", and "Add Key File".
- More Options:** A checkbox labeled "More Options" which is checked.
- Buttons:** A yellow "Import Licence File" button and a grey "Exit" button.
- License Information:** A footer area containing "Licensed To: Custom Computer Programs Ltd - (087654)" and "Licence Period: 01/01/2020 - 31/12/2021".

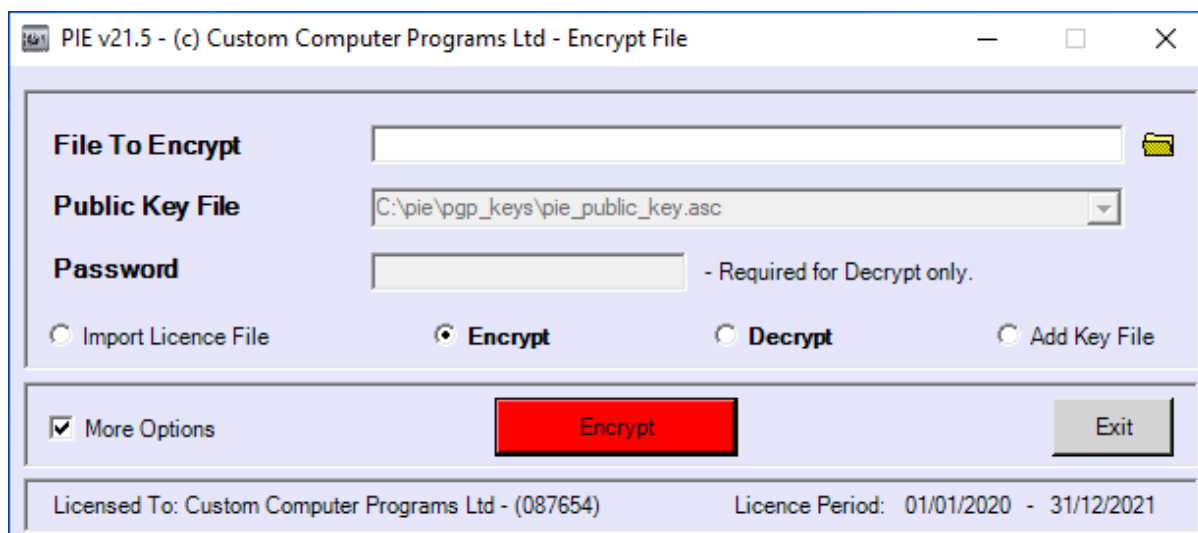
The screen above shows how the screen labels have changed in accordance with the radio button selected. For example, the first screen label changed to 'Licence File to Import'. The label of the main button, displayed in yellow, has also changed to show 'Import Licence File' and on selecting this button the user is prompted to select a licence file to import.

On importing a licence file, assuming it is valid, PIE updates the screen accordingly showing any licence information that may have changed such as the licence period dates. If the PIE's license becomes invalid then PIE will disable all radio buttons except the radio button 'Import Licence File'. This is expected behaviour and allows a user to use PIE to import a new licence file and get PIE fully functional again.

PIE, and PIE Client, are licensed on an annual basis and when the active license becomes within about 10 days of its expiration date, the user receives a warning indicating how many licensed days remain. License files are simple text files which can be received via email as an attachment and can be easily installed as just described.

On Selecting Encrypt

On selecting the 'Encrypt' radio button, the following screen is displayed:



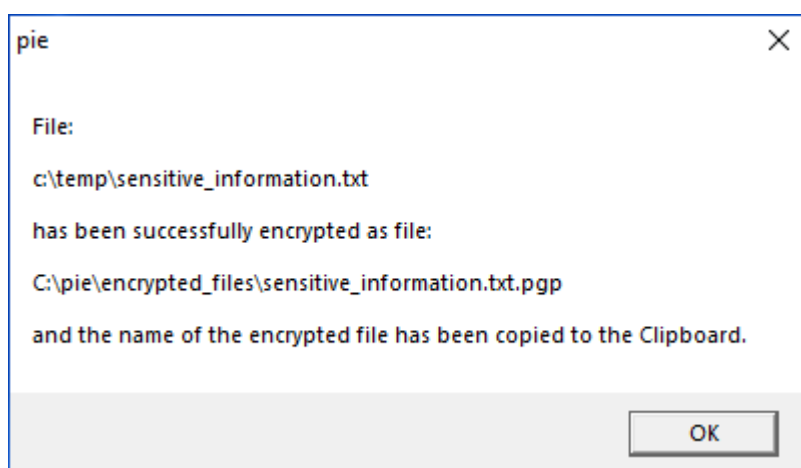
Again, the screen labels change in accordance with the radio button selected and now the user is prompted to select a 'File to Encrypt'.

Files are encrypted using a Third Party's Public Key which must already be installed in PIE. The mechanism of adding a Third Party Public Key to PIE is described under the heading 'Selecting Add Key File' described later on in this document.

The dropdown box, opposite the label 'Public Key File', contains a list of all of the Public Keys that PIE has access to and which, by default, are stored in the following directory:

`<installed drive>:\pie<version number>\pgp_keys'`

Once a file to encrypt, and the appropriate Public Key, have both been selected, the file is encrypted by selecting the red 'Encrypt' button and once the file has been encrypted a notification, similar to the following, is displayed:



In the example above, the file:

`c:\temp\sensitive_information.txt`

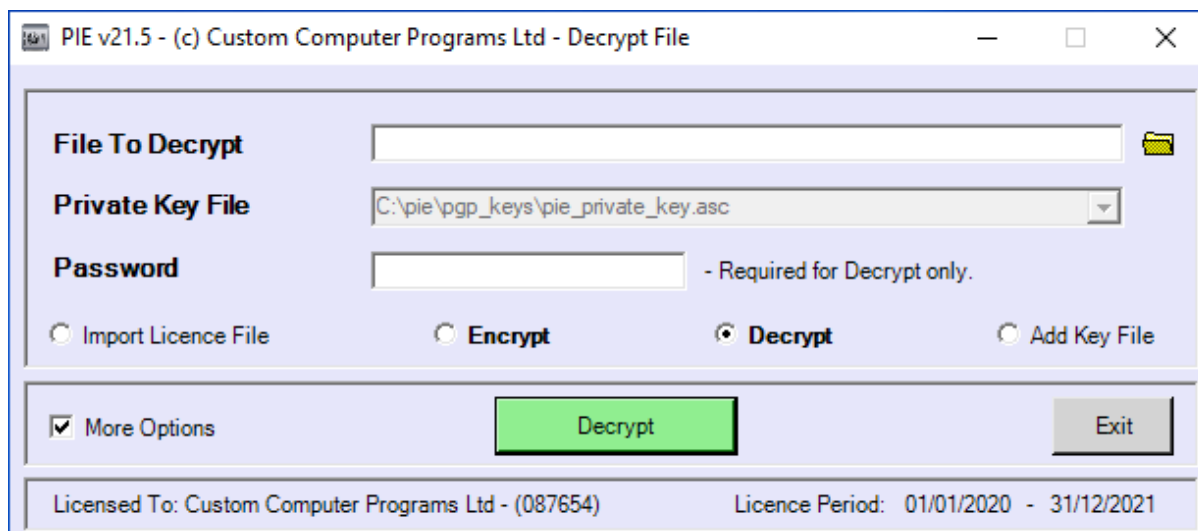
was encrypted and written to:

`c:\pie\encrypted_files\sensitive_information.txt.pgp`

When PIE encrypts a file, it appends the '.pgp' suffix to the filename. Conversely, when PIE decrypts a file, it writes the decrypted file to disk and removes the '.pgp' filename suffix.

On Selecting Decrypt

On selecting the 'Decrypt' radio button, the following screen is displayed:



Again, the screen labels change in accordance with the radio button selected and now the user is prompted to select a 'File to Decrypt'.

Files are decrypted using a Private Key file and, in order for the decryption to work successfully, the file to be decrypted must have been encrypted using the Private Key's associated Public Key. Typically, a Public Key is distributed to a number of Third Party's whereupon it would be used to encrypt a file and send to the person holding the associated Private Key.

Third Party's Public Key which must already be installed in PIE. The mechanism of adding a Third Party Public Key to PIE is described under the heading 'Selecting Add Key File' described later on in this document.

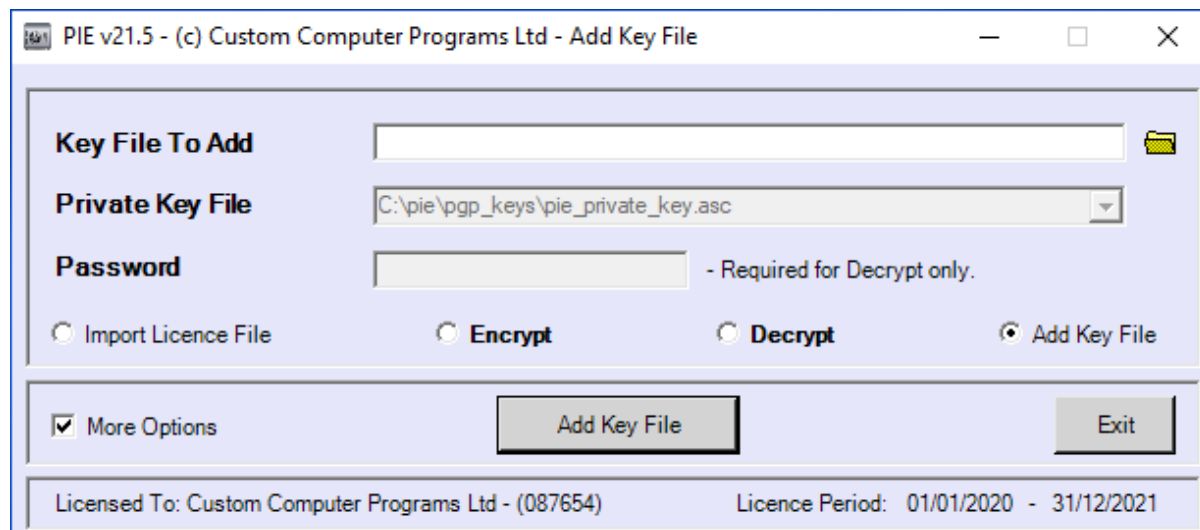
The dropdown box, opposite the label 'Public Key File', contains a list of all of the Public Keys that PIE has access to and which, by default, are stored in the following directory:

'<installed drive>:\pie<version number>\pgp_keys'

Once a file to encrypt, and the appropriate Public Key, have both been selected, the file is encrypted by selecting the red 'Encrypt' button and once the file has been encrypted a notification, similar to the following, is displayed:

On Selecting Add Key File

On selecting the 'Add Key File' radio button, the following screen is displayed:



As mentioned previously, PIE encrypts and decrypts by using Public and Private keys respectively and it has been designed to encrypt and decrypt files between an unlimited number clients.

In order to encrypt a file, destined for a specific Third Party, PIE needs the specific Third Party's Public Key.

After installing PIE, it will not have any Third Party Public Keys installed but they can be added to PIE by selecting the 'Add Key File' radio button.

On selecting the 'Add Key File' radio button, the screen shown above is displayed whereupon a Third Party Public Key (file) can be added by selecting the 'Key File to Add' file icon, selecting the file and then selecting the 'Add Key File' button.

It should be noted that both Public and Private Key files can be added using this method and the added Key files are written to PIE's 'pgp_keys' directory.

