When to use

Key Generation: The feature is to be used by first time users or to create new key pairs in case of suspicion of key compromise. The feature is used to generate a pair of public and private key. Key pairs are used to encrypt/decrypt or digitally sign and verify documents.

Encryption/Decryption: This feature is to be used when confidential content is to be shared or stored, so that disclosure to malicious third party can be avoided.

Digital Signature: This feature is to be used to ensure the authenticity of the source and prevent forging of documents. It can also be used as a measure against unwanted modifications of content by malicious entities.

View User List: The feature is used to check the list of possible users who have key pairs assigned for use.

Revoked Keys List: This feature is used to list revoked keys and inform about them to prevent its use and avoid error triggering. It is also used to ensure the proper functioning of revoke key functionality.

Keys -> View Key Info: Used to list all information about the all the keys and export them and generate files for these keys in the local file system.

Keys -> Revoke Keys: Feature is used to revoke key pair.

PGPTools -> Help: Used to guide the user to identify need of various features and to understand the correct steps to use them.

PGPTools -> Generate Revocation Certificate: Feature is to be used in case of key pair compromise and password cannot be provided for key revocation. In short it provides an alternate path for key revocation.

PGPTools -> Exit: Used to exit from the application and close it.

How to use

Generate Key

Press the button to open its dialog box and then follow the following steps to generate key pair:

1. Enter username, email id in the corresponding fields.
2. Enter pass phrase twice to confirm.
3. Press the create button to generate key pair.
4. Press “Yes” button to continue further.
5. Select the folder to save keys generated.

To close the window without creating the key press “Cancel” button.

View Users List

Press the button to view the list of all users along with key information. To export the key from the list of keys perform the following steps:

1. Click in the corresponding cell for key export and then select folder to export the key file into.
2. Press the “Save” button to complete the export action.

Revoked Keys List

Press the button to view the list of keys that are revoked. The information displayed includes username (email id), Key ID and option to export the public keys

Encrypt File

Pressing the button opens a dialog box. The steps are as follows:

1. Press “Source File” button and select file to be encrypted.
2. Press “Target Directory” and select directory to save the encrypted file generated through the process.
3. Enter Recipient’s User Id (email id) in the text field corresponding to it.
4. Press “Encrypt” button to encrypt the file and save it in the specified directory.

Decrypt File

Press the button to open the dialog box and then follow the following steps:

1. Press “Source File” button and select file to be decrypted.
2. Press “Target Directory” and select directory to save the decrypted file generated through the process.
3. Enter Recipient’s User Id (email id) in the text field corresponding to it.
4. Press “Decrypt” button to decrypt the file and save it in the specified directory.

Digital Signature

Press the button to digitally sign or verify the document. The following steps should be followed:

1. Enter Username (email id) and password in the respective text field.

2. Select the file to be signed or verified and then press “Open” button.
3. Press the “Sign” button to digitally sign the selected file or press the “Verify” button to verify the sign already existing on the selected file.
4. Message box either indicates success in signing or verifying of the file and displays the path of the signed file (named “signed_<username>.pgp”) or it indicated the possible error in functioning.

Digital Signature/Encryption

Press the button to digitally sign and encrypt the file and follow the steps as follows:

1. Enter username (email id) and password in the respective field.
2. Enter the username of the recipient (recipient’s email id) in its corresponding field.
3. Select file to sign and encrypt and the press “Open” button.
4. Press “Sign & Encrypt” button to create a signed and encrypted file.
5. Message box either indicates success in signing and encrypting of the file and displays the path of the generated file (named “signed_encrypted_<username>.pgp”) or it indicated the possible error in functioning.

Press the button to decrypt and verify the signature of the file and follow the steps as follows:

1. Enter username (email id) and password in the respective field.
2. Enter the username of the sender (sender’s email id) in its corresponding field.
3. Select file to decrypt and verify and the press “Open” button.
4. Press “Verify and Decrypt” button to create a signed and encrypted file.

Message box either indicates success in signing and encrypting of the file and displays the path of the generated file (named “OUTPUT_<username>.txt”) or it indicated the possible error in functioning.

Revoke Keys

Go to the Keys tab and select the Revoke Keys option, then follow the following steps:

1. Enter User ID (email id) and password in the respective fields.
2. Press the “Submit” button to revoke the key.

In case password cannot be entered, press the “Import Revocation Certificate and Revoke” button. Select the Revocation Certificate created by the PGPTool Generate Revocation Certificate.

PGPTool Generate Revocation Certificate

Go to PGPTools tab and select the Generate Revocation Certificate option and press the following steps:

1. Press “Generate Revocation Certificate” button subsequent dialog.
2. Enter username (email id) and password in the respective field.
3. Press “submit” button.

Revocation Certificate is generated and saved in the path displayed by in the message box. Revocation Certificate is saved in the file named “revocation_certificate_<username>.txt”.