Send an encrypted or digitally signed message

Digital Signature

A digital signature is a mechanism by which a message is authenticated. It proves that a message is effectively coming from a given sender, much like a signature on a paper document. Once a document is signed with a digital signature, it indicates the document is safe, protected, and not tampered or changed by anyone.

Encryption and Decryption

Encryption is a mechanism by which a message is transformed so that only the sender and recipient can view the contents of the mail.

For secured email communication with digital signatures and encryption, PGP keys are used. A PGP keys consist of a pair of keys a private and a public key. The PGP keys are generated in the webmail client and are saved with the user's account data. The public key is shared by mail. The recipient of a mail with the public key attached to it will save the public key on the server as part of the recipient's account data.

Once the sender and the recipients have generated the PGP keys for their accounts and shared the public key with the recipients, they can exchange emails that are digitally signed and encrypted.

For instance, suppose Smita, Akshay, and Amit want to exchange digitally signed and encrypted mail amongst themselves. First, each one of them has to create their PGP keys and share the Public key with each other.

Now, let us see the steps to send an encrypted and digitally signed message.

Generating PGP keys

Generating a PGP key-pair is a one-time activity. A key once generated can be used to send for communication with multiple recipients. Keys should also be downloaded and saved in a safe place.

Before generating PGP keys you need to

- Create your identity which needs to be associated with PGP keys
- Configure the encryption settings from the **Preferences** > **Encryptions** section of your account settings which enables you to send encrypted emails

To generate PGP keys,

1. Go to the **Settings** screen and choose the **PGP keys** option.
2. Clicking the plus sign in the bottom section of the middle pane shows the details to be filled up to create the PGP keys.
3. Choose your identity and set the password for the keys.
4. Remember the password associated with the key. This will be required when signing messages. By default, once authenticated by specifying the password, you are allowed to read or send the digitally

signed message till you are logged in to the current session.

Share your PGP keys for secured communication

To send secured messages to your colleagues, you need to share your public key with them through an email message. Also, get their public key through email and save at your end in the list of PGP keys. It is important to save the public key at an alternate location as well, as emails encrypted using a key cannot be opened with another.

Compose an encrypted email message

Compose the email, and click on the **Encryption** icon on the top menu pane.

Choose the **Digitally sign this message** and **Encrypt this message** options from the Encryption list.

Note, to compose and send an encrypted mail,

- Enable the option to send an encrypted message from settings preferences
- The sender must have the recipients' public key stored in his account.

Receive an encrypted email message

When the recipient receives the mail, they get a notification that the mail is digitally signed. They can see the contents since the public key of the sender is stored in their account.