GNU/Linux Administration - Support #619

Encrypting Email With Thunderbird Using Enigmail

05/22/2015 12:57 PM - Daniel Curtis

Status:	Suspended	**Start date:**	05/22/2015
Priority:	Normal	**Due date:**	
Assignee:	Daniel Curtis	**% Done:**	0%
Category:		**Estimated time:**	2.00 hours
Target version:	*nix	**Spent time:**	0.00 hour

Description

This is a guide for setting up and using Thunderbird with the Enigmail extension to encrypt email to send securely over the internet. **Thunderbird** is an open source application, so it will be available on Ubuntu, Debian, Arch, and even Windows; while the extension **Enigmail** is available from the addon section in Tools -> Add-ons.

Prepare the environment

Debian / Ubuntu

- Make sure the system is up to date:

```
sudo apt-get update && sudo apt-get upgrade
```

- Install Thunderbird and GPG

```
sudo apt-get install thunderbird gnupg
```

Arch

- Make sure the system is up to date:

```
sudo pacman -Syu
```

- Install Thunderbird and GPG

```
sudo pacman -S thunderbird gnupg
```

Install Enigmail

- Open **Thunderbird**, then go to Tools -> Add-ons
- Search for Enigmail and install the extension
  - **NOTE**: If the extension does not show up in the search, download it and install it by selecting Install Add-on from file

```
wget https://addons.mozilla.org/thunderbird/downloads/latest/71/addon-71-latest.xpi
```

Create PGP Keys

- Open **Thunderbird**, then go to Enigmail -> Key Management
- Create a new private/public key pair by going to Generate -> New Key Pair

- Select the account to generate the key pair for, as well as a password to encrypt the private key, and also the amount of time before the key pair expires.

- Click on **Generate** to generate the new key pair.
  - **NOTE**: Generating a new key pair will take a long time, make sure not to cancel or quit the process.

- When the key generation finishes, it is good practice to also create a *Revocation Certificate* in case the private key is ever compromised. Click on **Generate Certificate**. Select a path to store the Revocation Certificate and enter the password used while generating the key pair.
  - **NOTE**: Make sure to backup the Revocation Certificate to a safe place like an encrypted USB drive or container.

Upload Public Key to Keyserver

One way to share the public keys with the world is Key Servers, which Enigmail can use to search for other peoples PGP public keys (or other people can use to search for your PGP public key).

- Upload the new public key by going to Enigmail -> Key Management and then Keyserver -> Upload Public Keys. Then select a keyserver to upload the selected public key to, such as subkeys.pgp.net

Backup Private/Public Keypair

- Export the new private/public keypair to a file for backing up by going to Enigmail -> Key Management and then File -> Export Keys To File and select **Export Secret Keys**. This will prompt for a path to save the keypair file and the password set during the keypair creation.
- **NOTE**: To export just the public key go to File -> Export Keys To File and select **Export Public Keys Only**. This will promp for a path to save the public key file, and will not need a password.

Resources

- https://www.mozilla.org/en-US/thunderbird/
- https://addons.mozilla.org/en-us/thunderbird/addon/enigmail/
- https://www.enigmail.net/home/index.php

History

#1 - 04/11/2018 10:37 AM - Daniel Curtis

- Status changed from New to Suspended