The mailbox.org HKPS key server

When using the mailbox.org web interface in combination with Guard, any OpenPGP keys needed for securely communicating with other Guard users can be retrieved automatically. For external senders using e-mail clients like Mozilla Thunderbird, we have an HKPS key server that offers verified OpenPGP-keys of mailbox.org users for import to a local key ring.

The address of our key server is as follows: ***hkps://pgp.mailbox.org***

What is different to other key servers is that ours will only distribute verified keys of mailbox.org users. It is not possible to manually upload fake keys for other e-mail addresses to our key server.

Usage with the command line interface

Using a terminal window or other CLI, you can run the program ***GnuPG 2.0 (gpg2)*** to search for OpenPGP keys of mailbox.org users on the key server (usage illustrated below):

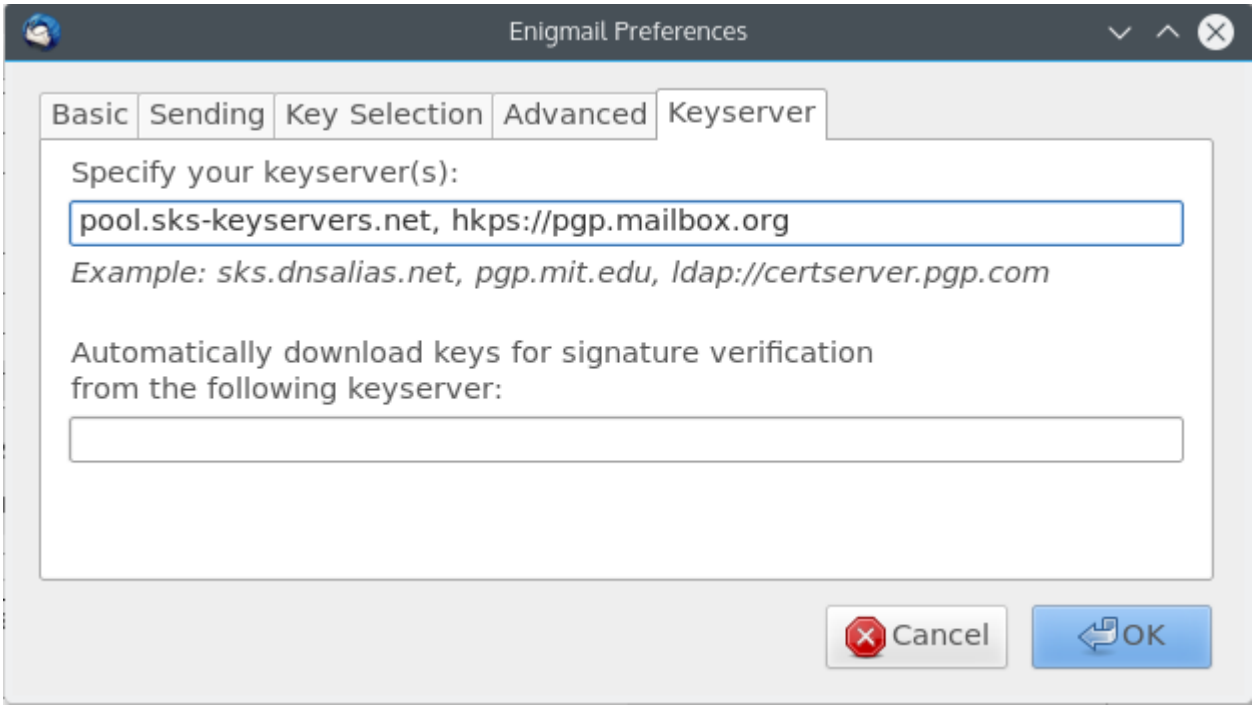
```
gpg2 --keyserver=hkps://pgp.mailbox.org --search john.doe@mailbox.org
```

Please make sure to use GnuPG 2.0 or a newer version as our key server will only accept encrypted connections. Lower versions (1.x) of GnuPG (gpg) will only support SSL encryption with the add-on module *gnupg-curl* installed.

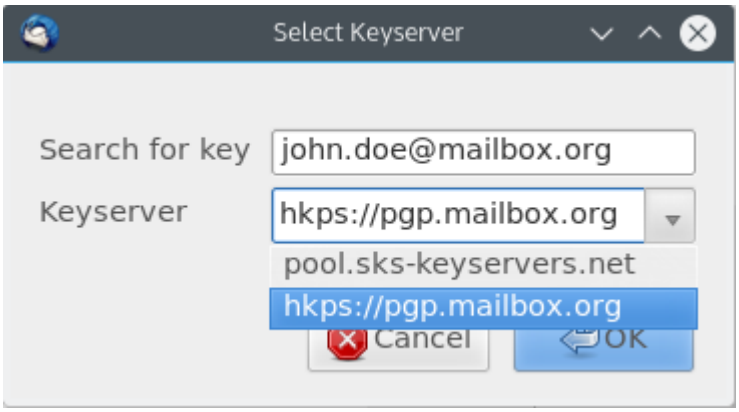
There are also binaries available for other operating systems like Windows or Mac OSX (please consult the GnuPG download page).

Usage with Enigmail for Mozilla Thunderbird

Thunderbird supports the Enigmail add-on for the management of encrypted e-mails. This add-on can access our key server if the address is specified in its configuration. To do this, open the Enigmail settings and click on the tab **Keyserver.** There, add the mailbox.org HKPS server address.



In the future, if you ever need a key of a mailbox.org user, select our key server to import a verified key to your local key ring.



Known problems with HKPS key servers

Some installations of GnuPG2 are known to have problems locating CA root certificates correctly. This is due to the SSL library being supplied by the operating system, which happens to prevent the automatic validation of our HKPS server certificate under the default configuration. In these cases, users will experience a general server error when attempting to search for keys. This problem has been noticed with GPG4WIN in particular, but may also occur on Ubuntu 16.04 and other Linux distributions.

In order to address the issue, users need to configure GnuPG and specify which CA root certificate it should use to validate the server certificate.

Ubuntu 16.04: Please use a text editor to open the configuration file located at *"$HOME/.gnupg/dirmngr.conf"* and add the following line:

```
hkp-cacert /etc/ssl/certs/SwissSign_Silver_CA_-_G2.pem
```

GPG4WIN (GnuPG versions 2.0.x): Please download the CA certificate file SwissSign_Silver_CA_-_G2.pem and save it locally on your computer.

Open the configuration file named gpg.conf and add the following line:

```
keyserver-options ca-cert-file=C://...<Path>.../SwissSign_Silver_CA_-_G2.pem
```

Make sure to edit the path so that it points to your downloaded certificate file.

Enigmail: Users of Enigmail for Mozilla Thunderbird do not need to edit any configuration files manually. Instead, the settings can be changed directly through the Enigmail configuration tool.

First, download the CA certificate SwissSign_Silver_CA_-_G2.pem and save it locally on your computer. Then, access the Enigmail configuration settings and open the tab **Advanced**. Near the bottom of the window, there is a text field titled **Additional parameters for GnuPG** into which you need to add the following line:

```
--keyserver-options ca-cert-file=<Path to>/SwissSign_Silver_CA_-_G2.pem
```

Make sure to edit the path so that it points to your downloaded certificate file.

Auto-Key-Locate

It is possible to configure GnuPG to automatically retrieve from our key server any PGP keys that are currently not available at the client side.

To do this, simply enable the *auto-key-locate* feature in the configuration file by opening gpg.conf in a text editor and adding the following line:

```
auto-key-locate keyserver keyserver-URL hkps://pgp.mailbox.org
```

On MS Windows, the file gpg.conf is usually located in "%APPDATA%\GnuPG". On Linux systems, it can be found in "$HOME/.gnupg". Users of MacOS X can simply use the tool GPGPreferences to make any changes.

We should mention that the *auto-key-locate* feature of GnuPG has been subject to critical discussion among privacy advocates. Although searching and finding of encryption keys will be automated and thus, vastly simplified, there are also possible privacy implications. A key server operator could theoretically log any connections made by individuals to the server and so create communication profiles of these individuals. The GnuPG documentation contains explicit warnings about this.

However, if key server and mail server are operated by the same organization (as is the case with mailbox.org), these privacy concerns are no longer an issue. This is because the information obtainable from the key server communications would not add anything new to what is already known to the mail server instance.

How to use our HKPS server with your own domain

If you use your own domain with mailbox.org, it is still possible to make PGP clients find and retrieve your public keys automatically from the HKPS server at mailbox.org. This requires a special SRV-DNS record to be set, like the one below for the domain example.com:

```
_hkps._tcp.example.com. IN SRV 1 1 443 pgp.mailbox.org
```

Related Articles

- How to set up Mailvelope
- PGP key management
- Activate your mailbox.org Guard
- The Encrypted Mailbox
- How can e-mails be encrypted with PGP