Unser HKPS-Keyserver

Wenn Sie das **mailbox.org-Webinterface mit dem Guard** verwenden, dann werden die PGP-Schlüssel von anderen Guard-Nutzern **automatisch** gefunden.

Für externe E-Mail-Absender und Nutzer von E-Mail-Clients wie Thunderbird stellen wir einen HKPS-Keyserver bereit, der **verifizierte** PGP-Schlüssel von mailbox.org-Nutzern für den Import in den lokalen Schlüsselbund anbietet. Im Gegensatz zu anderen Keyservern werden beim Keyserver von mailbox.org nur verifizierte Schlüssel bereitgestellt: es ist schlichtweg nicht möglich, einen falschen Schlüssel für eine fremde E-Mail-Adresse auf unseren Keyserver zu laden.

Die Adresse unseres Keyservers ist: **hkps://pgp.mailbox.org**

Den HKPS-Keyserver über die Kommandozeile verwenden

Unter Linux können Sie mit dem Programm „**gpg2**“ über die Kommandozeile auf unserem Keyserver nach PGP-Schlüsseln von mailbox.org-Nutzern suchen. Nutzen Sie dafür folgende Befehlszeile:

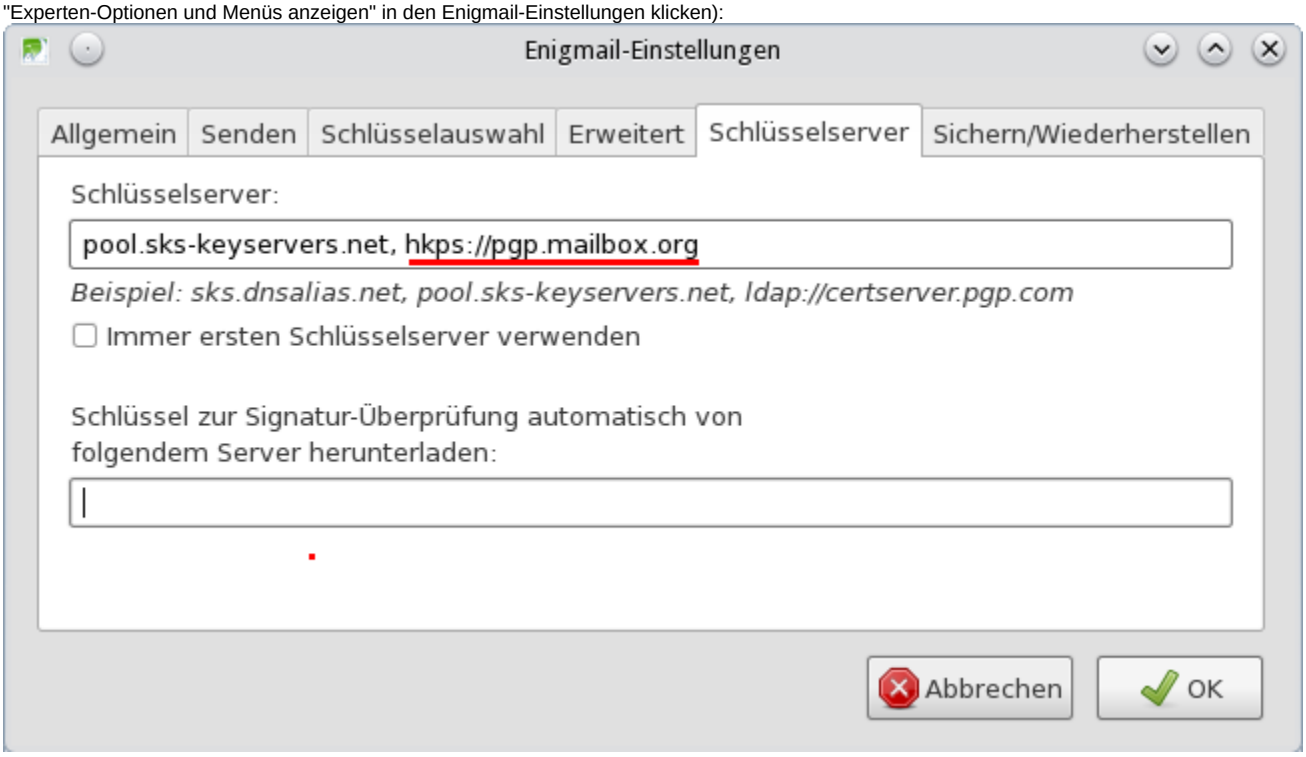
```
gpg2 --keyserver=hkps://pgp.mailbox.org --search max.mustermann@mailbox.org
```

Bitte beachten Sie, dass Sie **mindestens „GnuPG 2.0“** (**gpg2**) verwenden sollten, da unser Keyserver nur über eine SSL-verschlüsselte Verbindung erreichbar ist.
Die Versionen 1.x von „**GnuPG**“ (**gpg**) unterstützen SSL-Verschlüsselung für Keyserver **nur mit dem Zusatzmodul „gnupg-curl“.**

Es gibt GnuPG-Implementationen auch für andere Betriebssysteme. Falls Sie z.B. **Windows** oder **Mac OS** benutzen, finden Sie einen Link zu einem auf Ihrem Betriebssystem lauffähigen Programm auf der **GnuPG-Download-Seite.**

Den HKPS-Keyserver mit Enigmail für Thunderbird verwenden

Wenn Sie das Add-on „**Enigmail**“ für den E-Mail-Client Thunderbird zur Verwaltung Ihrer verschlüsselten E-Mails verwenden, dann können Sie in der Konfiguration von Enigmail im Reiter „**Schlüsselserver**“ den HKPS-Server von mailbox.org hinzufügen Diesen reiter sehen Sie, nachdem Sie auf "Experten-Optionen und Menüs anzeigen" in den Enigmail-Einstellungen klicken):



Wenn Sie dann den Schlüssel eines mailbox.org-Nutzers benötigen, können Sie bei der Suche nach seinem Schlüssel einfach diesen Keyserver auswählen, um den entsprechenden, verifizierten Schlüssel zu importieren:

Bekannte Probleme mit HKPS-Keyservern

Einige Installationen von „**GnuPG2**“ können aufgrund der verwendeten SSL-Bibliothek die vom Betriebssystem bereitgestellten CA-Root-Zertifikate nicht finden. Die Suche nach Schlüsseln wird mit einem "*Allgemeinen Serverfehler"* abgebrochen. Neben „**GPG4WIN**“ sind auch Ubuntu 16.04 sowie einige andere Linux-Distributionen betroffen.
Um das Problem zu lösen, müssen Sie „**GnuPG**“ mitteilen, welches CA-Root-Zertifikat für die Validierung des Server-Zertifikats verwendet werden soll:

- **Ubuntu 16.04:**
  Öffnen Sie die Konfigurationsdatei „$HOME/**.gnupg/dirmngr.conf**“ mit dem Texteditor Ihrer Wahl und tragen dort folgende Zeile ein:

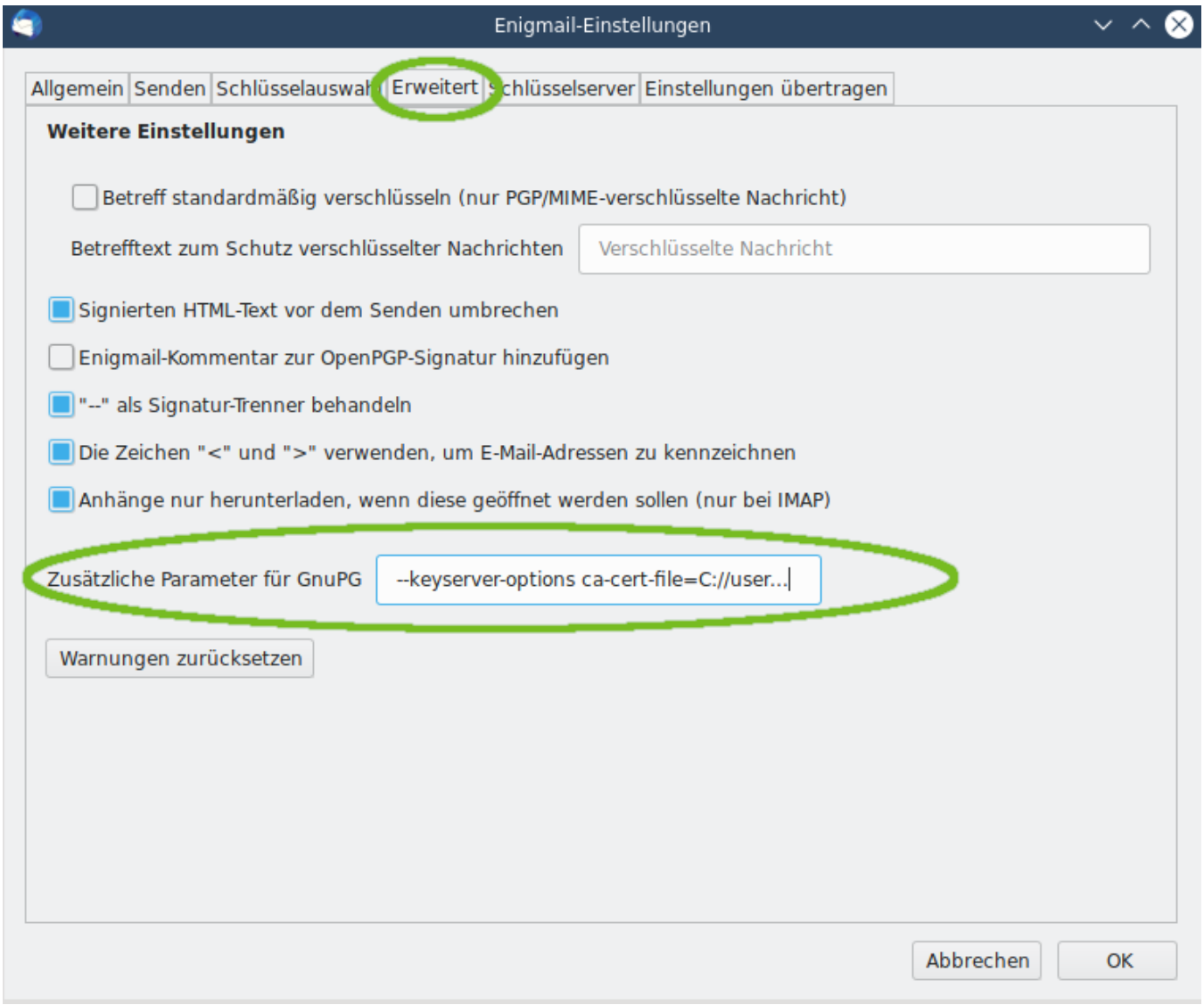
  ```
  hkp-cacert /etc/ssl/certs/SwissSign_Silver_CA_-_G2.pem
  ```

- **GPG4WIN** (u.a. Versionen mit „**GnuPG Version 2.0.x**“):
  Laden Sie dieses CA-Zertifikat SwissSign_Silver_CA_-_G2.pem herunter. In der Konfigurationsdatei „**gpg.conf**“ müssen Sie folgende Zeile hinzufügen:

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

- **Enigmail:**
  Wenn Sie Enigmail für Mozilla Thunderbird nutzen und keine Konfigurationsdateien mit einem Editor bearbeiten wollen, dann können Sie die Einstellungen auch in der Konfiguration von Enigmail vornehmen. Laden Sie folgende Datei herunter: SwissSign_Silver_CA_-_G2.pem. Öffnen Sie die Einstellungen von Enigmail und gehen zum Reiter „**Erweitert**“. In dem Textfeld „**Zusätzliche Parameter für GnuPG**“ fügen Sie folgenden Parameter hinzu:

```
--keyserver-options ca-cert-file=<HIER PFAD EINFÜGEN>/SwissSign_Silver_CA_-_G2.pem
```



Auto-Key-Locate

Sie können „**GnuPG**“ auch so konfigurieren, dass automatisch auf unserem Keyserver ein passender Schlüssel gesucht wird, falls dieser fehlt. Diese Funktion heißt „**auto-key-locate**“. Um diese zu aktivieren, müssen Sie die Konfigurationsdatei „**gpg.conf**“ mit einem Texteditor Ihrer Wahl bearbeiten (**Mac OS**-Nutzer können das Programm GPGPreferences nutzen, um die Änderung in der Konfiguration durchzuführen). Die Datei „**gpg.conf**“ finden Sie

- unter **Linux** im Verzeichnis „$HOME/**.gnupg**“
- unter **Windows** im Verzeichnis „%APPDATA%**GnuPG**“

Tragen Sie folgende Zeile in die „**gpg.conf**“ ein, um „**auto-key-locate**“ zu aktivieren:

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

Die „**auto-key-locate**“-Funktion von GnuPG wird unter Privatsphäreenthusiasten kontrovers diskutiert. Neben einer Vereinfachung bzw. Automatisierung der Schlüsselsuche hat es prinzipiell einige Implikationen in Sachen Privatsphäre. Der Betreiber des Keyservers könnte Zugriffe protokollieren und somit Profile erstellen, wer mit wem kommuniziert. GnuPG selbst weist in der Dokumentation auf diese Implikationen hin.
Wenn der Betreiber des Keyservers auch der Betreiber des Mailservers ist (wie bei mailbox.org), dann **sind dieses Implikationen aber gegenstandslos**, weil der Mailserver keine Mehrinformationen durch die Schlüsselsuche gewinnt, da er automatisch alle aktiven E-Mail-Kontakte des Nutzers kennt.

Unseren HKPS-Server für eine eigen Domain verwenden

Wer die E-Mails seiner eigenen Domain über mailbox.org eingebunden hat, kann PGP-Clients ermöglichen, den zuständigen PGP-Server von mailbox.org automatisch finden zu können, um die Schlüssel von dort zu beziehen. Dazu muss ein spezieller „**SRV-DNS-Record**“ eingetragen werden, wie hier im Beispiel der Domain example.com:

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

Verwandte Artikel

- Welche PGP-Standards Guard unterstuetzt
- Das temporaere Postfach fuer externe Nutzer
- Das verschluesselte Postfach
- Verschluesselte Nachrichten lesen
- Verschluesselung im Drive