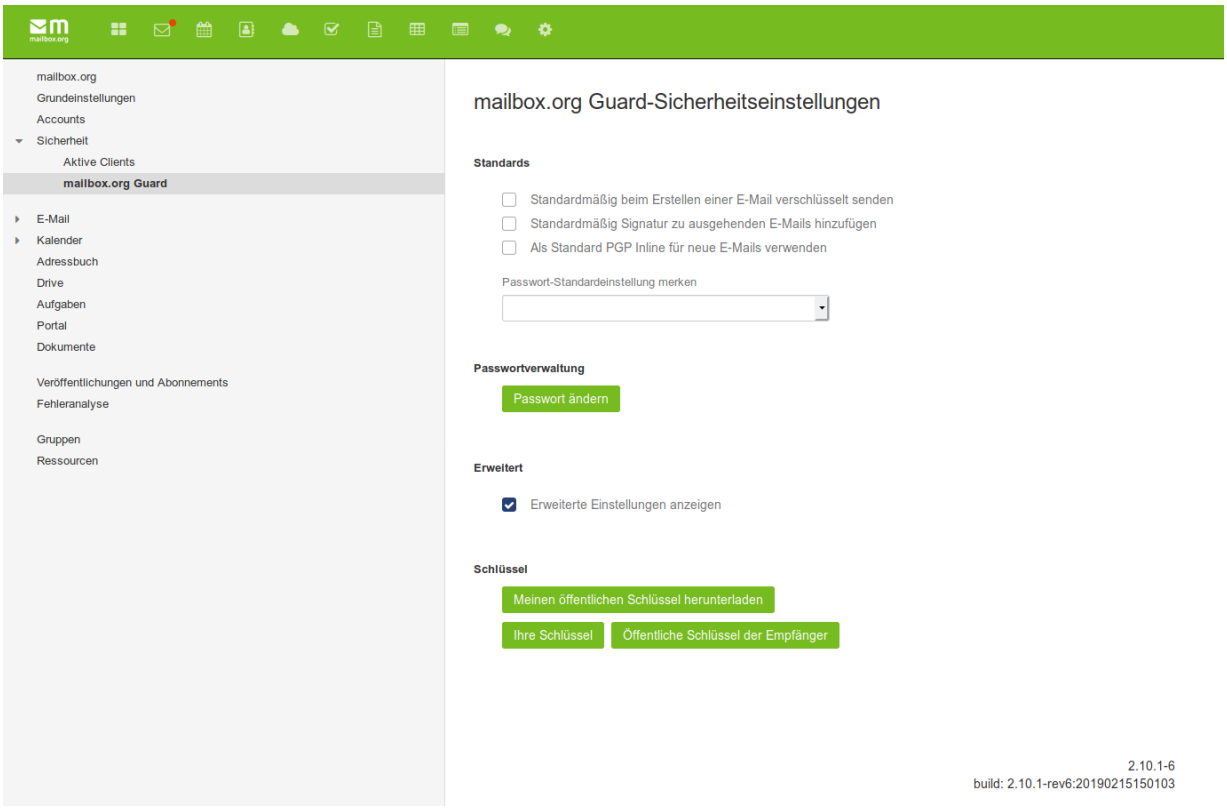
Verwaltung der PGP-Schluessel

Anmerkung: um die in diesem Artikel beschriebenen Funktionen zu nutzen, müssen Sie den mailbox.org-Guard aktiviert haben.

Hinweis: Der mailbox.org-Guard ist für die Arbeit mit ihrer Haupt-E-Mail-Adresse konzipiert. **Die Verwendung in Kombination mit Aliassen ist nicht vorgesehen.**

Der mailbox.org Guard bietet eine Verwaltung für Ihre eigenen PGP-Schlüssel und die öffentlichen PGP-Schlüssel Ihrer Kommunikationspartner. In ihrem mailbox.org-Office finden Sie diese Verwaltung unter „**Einstellungen -> mailbox.org Guard-Sicherheit -> Guard-PGP-Einstellungen**“:



Mit der Aktivierung des Guard werden automatisch zwei Schlüsselpaare für Ihre Hauptadresse erzeugt. Damit ist der mailbox.org Guard bereits voll funktionsfähig. Wenn Sie Details interessieren, finden Sie in der Schlüssel-verwaltung die automatisch erzeugten zwei Schlüsselpaare:

1. Der Hauptschlüssel (der obere Schlüssel im Bereich „**Ihre Schlüsselliste**“) wird zum Signieren (Unterschreiben) von E-Mails genutzt. Er kann auch zum Beglaubigen bzw. Unterschreiben von anderen PGP-Schlüsseln genutzt werden (Web of Trust) - diese Funktion ist aber im mailbox.org-Guard bisher nicht implementiert.
2. Der Unterschlüssel wird zum Ver- und Entschlüsseln der E-Mail-Kommunikation und von Dateien im Drive verwendet.

Sie können in der Schlüsselverwaltung die auf unserem Server erzeugten Schlüssel(-paare) herunterladen und - falls vorhanden - in Ihre lokale PGP-Installation bzw. Ihren lokalen Mailclient importieren. So können Sie sowohl im Webclient, als auch in Ihrem lokalen Mailclient auf die verschlüsselten E-Mails zugreifen.

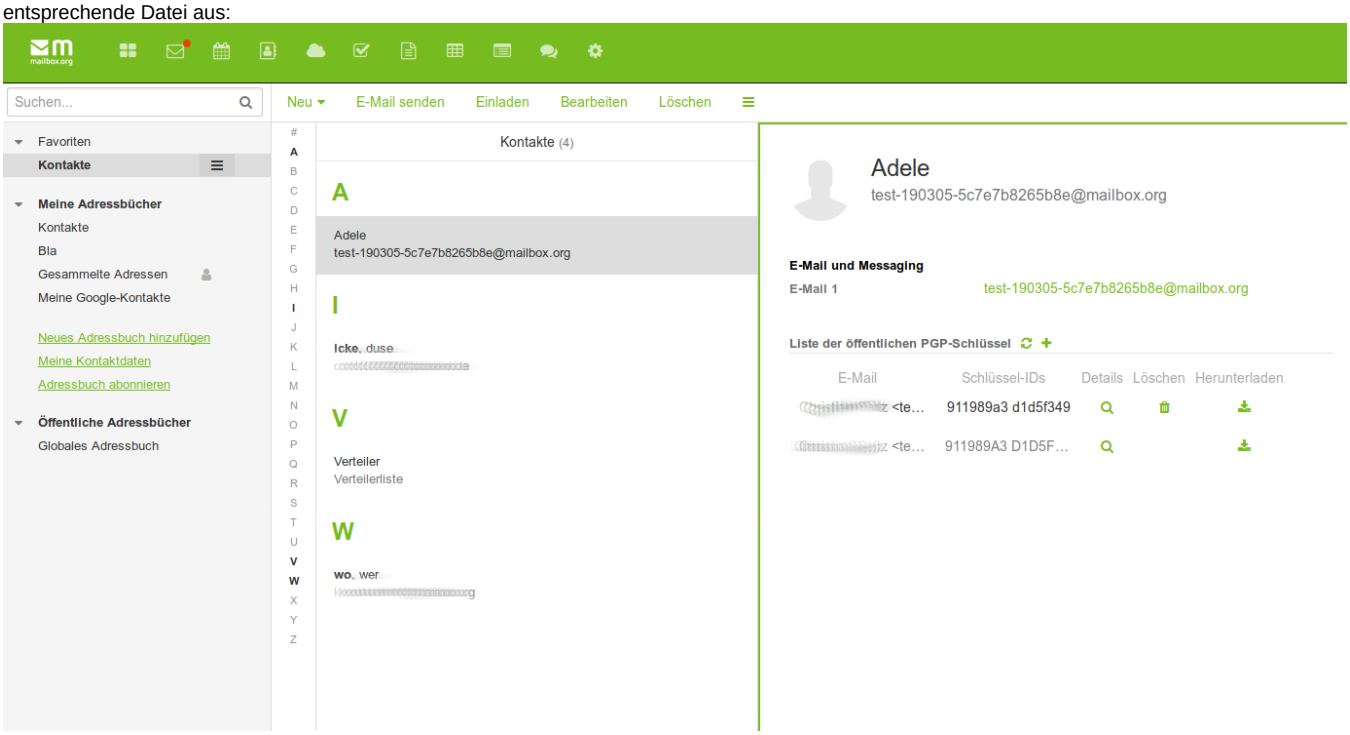
Eigene Schlüssel verwenden

Sie können die automatisch erzeugten Schlüssel auch durch ein eigens, bereits vorhandenes Schlüsselpaar ersetzen. Dieses Schlüsselpaar muss mindestens Ihre aktive E-Mail-Adresse von mailbox.org als UID enthalten. Sie können dabei selbst entscheiden, ob Sie nur einen öffentlichen Schlüssel hochladen wollen (um ihn anderen Guard Nutzern zur Verfügung zu stellen) oder auch den privaten Schlüssel auf unserem Server speichern wollen, um verschlüsselte Inhalte im Webinterface lesen zu können.

Hinweis: das Lesen verschlüsselter E-Mails im Webinterface und das Öffnen von verschlüsselten Dateien im Drive sind nur möglich, wenn der entsprechende, gültige private Schlüssel auf dem Server vorhanden ist.

Öffentliche Schlüssel der Kommunikationspartner

In der Schlüsselverwaltung können Sie auch den Schlüsselbund mit den öffentlichen Schlüssel Ihrer Kommunikations-partner verwalten. Sie finden die Liste unter „**Einstellungen -> mailbox.org Guard-Sicherheit -> Guard-PGP-Einstellungen -> Liste der öffentlichen PGP-Schlüssel**“. Mit einem Klick auf das „**+**“-Symbol können Sie weitere öffentliche Schlüssel (z.B. als .pgp oder .asc-Datei) hochladen.
Weiterhin können Sie die Schlüssel Ihrer Kommunikationspartner im Adressbuch verwalten. Zu jedem Eintrag im Adressbuch können Sie die zugehörigen PGP-Schlüssel hochladen. Öffnen Sie dafür einen Kontakt in Ihrem Adressbuch im mailbox.org-Office. Um einen neuen PGP-Schlüssel zu diesem Kontakt hinzuzufügen, klicken Sie im rechten Fenster in der „**Liste der öffentlichen PGP-Schlüssel**“ auf das „**+**“-Symbol und wählen anschließend die entsprechende Datei aus:



Das Hochladen von Schlüsseln - maximale Dateigröße

Hinweis: Sie können öffentliche Schlüssel mit einer Größe von maximal 65k hochladen. Das ist für die meisten Schlüssel ausreichend. Wenn der Schlüssel Fotos oder sehr viele Signaturen enthält und größer als 65k ist, dann kann es beim Upload der Schlüssel zu Fehlermeldungen kommen.

Um zu große Schlüssel zu verkleinern, können Sie diese in Ihre lokale Schlüsselverwaltung von „**GnuPG**“ importieren und dann mit der Option „**–export-options export-minimal**“ zum Hochladen exportieren:

```
gpg2 --armor --export-options export-minimal --export <Ihre-Schlüssel-ID> > key4upload.asc
```

Wenn Sie keine lokale Installation von GnuPG besitzen oder verwenden wollen, dann müssen Sie Ihren jeweiligen Kommunikationspartner bitten, einen solchen, minimalen Schlüssel zur Verfügung zu stellen.

Verwandte Artikel

- Fotos des Drive-Clients im Webinterface
- Uebersicht: Was ist Jabber XMPP
- Verschluesselung im Drive
- YubiKey: Webmail mit Einmalkennwoertern
- Das Add-on Mailvelope verwenden