

# Das Add-on Mailvelope verwenden

## Mailvelope - eine Übersicht

**Mailvelope** ist ein **Browser Add-on**, das Sie in [Firefox](#), [Chrome](#) und [Edge](#) und verwenden können, um Ihre E-Mails bei **Webmail** Anbietern mit **PGP** sicher zu verschlüsseln. Wenn Sie das mailbox.org-Office mit Mailvelope verwenden, ergeben sich **folgende Vorteile** für Sie:

- Die PGP-Verschlüsselung wird in den Webclient integriert. Sie können E-Mails problemlos verschlüsseln, entschlüsseln und signieren.
- Sie können Ihre PGP-Schlüssel auf Ihrem Rechner verwalten.
- Ihre öffentlichen PGP-Schlüssel können für alle anderen Kommunikationspartner über den mailbox.org-Guard oder über unseren HKPS-Schlüsselservers bereitgestellt werden.
- Ihr privater Schlüssel kann auf verschiedene Geräte via mailbox.org sicher übertragen werden.

Gleichzeitig hat die Nutzung des Add-ons Mailvelope auch einige Nachteile in Bezug auf Sicherheit, daher **folgende Warnhinweise**:

- Plugin-Lösungen im Browser - und damit auch Tools wie Mailvelope - können bei der Verwendung von Cloud-Datenspeichern oder E-Mail-Anhängen Probleme verursachen.
- Ihre Schlüssel werden auf Ihrem Computer **im lokalen Speicher des Browsers** aufbewahrt - das hat mehrere Implikationen:
  - Da der lokale Speicher zur Schlüsselaufbewahrung verwendet wird, ist Mailvelope für den Einsatz auf fremden oder unsicheren Rechnern (z.B. in Internet-Cafés oder im Urlaub) nicht geeignet.
  - Im [HTML5 Security Cheat Sheet](#) wird vom [OWASP](#) empfohlen, keine sicherheitsrelevanten Informationen im lokalen Speicher des Browsers aufzubewahren, da diese Daten mit XSS-Angriffen kompromittiert werden könnten.
  - Die [Sicherheitanalyse von Mailvelope durch Cure53 \(pdf\) von 2013](#) weist am Ende auf das Risiko von XSS-Angriffe hin. Insbesondere Nutzer von Mozilla Firefox sind dabei gefährdet, da dieser Browser **weniger Schutzmechanismen biete** als Google Chrome. Wir empfehlen allen Firefox Nutzern deshalb, **das Add-on Mailvelope in Kombination mit dem Add-on NoScript einzusetzen**. NoScript schließt Sicherheitslücken in Firefox, z.B. durch XSS-Protection.
- Javascript wurde nicht als Programmiersprache für Kryptographieanwendungen entworfen. Funktionen, die als Best Practice für die Implementierung von Kryptografie gelten, sind mit Javascript schlicht nicht realisierbar. Was in anderen Krypto-Implementierungen als schwerer Bug gilt, muss bei Mailvelope einfach als Limitierung durch Javascript hingenommen werden - zum Beispiel:
  - ist es mit Javascript nicht möglich, einen geheimen Schlüssel nach der Benutzung sicher aus dem Hauptspeicher zu löschen ([Overwriting memory - why?](#)). Normales Verhalten bei Mailvelope wird beim [TOR-Projekt als Sicherheitslücke eingestuft](#).
  - bei der Programmierung können keine identische Ausführungszeiten für Code Verzweigungen erzwungen werden. Durch Seitenkanalangriffe ist es damit möglich, die Reihenfolge der Nullen und Einsen im privaten Schlüssel durch Beobachtung bei der Codeausführung zu rekonstruieren. In modernen Krypto-Bibliotheken ist das eine Sicherheitslücke (z.B. [CVE 2016-7056](#) in OpenSSL, LibreSSL und BoringSSL). Wie einfach Seitenkanalangriffe auf Browser möglich sind, ohne den Rechner zu kompromittieren, haben Forscher in der Arbeit [Practical Cache Attacks in Javascript \(pdf\)](#) gezeigt.

Nach unserer Einschätzung bietet Mailvelope zwar **hinreichende Sicherheit**, ist aber für hohe Sicherheitsanforderungen nicht geeignet.

## Mailvelope nutzen

### Vorbereitung und Aktivierung von Mailvelope

Um Mailvelope mit dem mailbox.org-Office zu nutzen, müssen Sie das Add-on zuerst [herunterladen](#) und dann in Ihrem Browser installieren. Beziehen Sie dieses Add-on über die Seite von Mailvelope.

Nun können Sie im Webclient unter **Symbol Einstellungen**  -> **mailbox.org** -> **PGP im Webmailer** zwischen dem mailbox.org Guard und Mailvelope wählen. Wählen Sie hier wie im Bildschirmabzug dargestellt den Punkt 4 "Jetzt aktivieren".

mailbox.org

Grundeeinstellungen  
Konten  
Sicherheit  
E-Mail  
Kalender  
Adressbuch  
Portal  
Drive  
Aufgaben  
Dokumente

Abonnements  
Fehleranalyse  
Gruppen  
Ressourcen  
Persönliche Daten herunterladen

Vertrag und Tarif  
Kontoauszug  
Guthaben einzahlen  
Rechnungskopien  
Passwort ändern  
Newsletter  
PGP im Webmailer  
Trash-Folder  
E-Mail-Aliase  
Alternative Absender  
Wegwerf-Adressen  
Verschlüsselter Versand  
Abrufen externer POP3-Mailaccounts  
Blocken unerwünschter Absender (Blacklist)  
Einstellungen  
Spam-/Virenschutz  
Have I been pwned  
Persönliche Daten  
Selbstauskunft  
Digitales Erbe

## PGP im Webmailer

Hier können Sie auswählen, welche Art der PGP Verschlüsselung im Webmailer genutzt wird.

Bevor Sie die PGP Verschlüsselungsmethode wechseln empfehlen wir Ihnen, Ihren aktuellen PGP Schlüssel zu sichern. Um Ihre bereits verschlüsselten E-Mails weiterhin lesen zu können, müssen Sie diesen PGP Schlüssel in Ihrer neu ausgewählten Verschlüsselungsmethode hinzufügen.

<p><b>Einfach und intuitiv mit dem Guard</b></p> <ul style="list-style-type: none"> <li>✓ Verschlüsselung von E-Mails und Dateien mit nur einem Klick</li> <li>✓ Funktioniert in allen Browsern mit allen Ihren Kontakten</li> <li>✓ Einfach anwendbar, täglich</li> <li>✓ Sicherheitsdetails durch uns verwaltet</li> </ul> <p>Wenn Sie nicht über eine tiefe Kenntnis der Verschlüsselung verfügen, jedoch Ihre Kommunikation mit Ihren Freunden oder Geschäftskontakten auf einfachem Weg sichern möchten, ist diese Option optimal für Sie. Sichere E-Mail, einfach gemacht!</p> <p>aktiviert</p>	<p><b>Verschlüsselung für Experten mit Mailvelope</b></p> <ul style="list-style-type: none"> <li>✓ Verschlüsselungsoptionen für Experten verfügbar</li> <li>✗ Funktioniert nur in Firefox und Chrome</li> <li>✗ Browser-Plugin erforderlich</li> <li>✗ Sicherheitsdetails durch Sie selbst verwaltet</li> </ul> <p>Wenn Sie ein Verschlüsselungsexperte sind und alle Verschlüsselungsdetails selbst verwalten möchten, passt diese Option am besten für Sie. Sie müssen ein Drittanbieter-Browser-Plugin installieren, um mit der Experten-Verschlüsselung zu arbeiten.</p> <p>jetzt aktivieren</p>
---	--

## Fragen und erste Schritte mit Mailvelope

Um Mailvelope mit ihrem mailbox.org-Office zu nutzen, sei auf die umfangreiche Dokumentation des Add-on verwiesen. <https://mailvelope.com/de/help#installation>

Falls Sie noch keine PGP Verschlüsselung verwenden, folgen Sie dieser Anleitung, um ein Schlüsselpaar zu erstellen.

siehe [https://mailvelope.com/de/faq#key\\_administration](https://mailvelope.com/de/faq#key_administration).

So können sie beispielsweise das Schlüsselpaar, das vom mailbox.org-Guard erstellt wurde oder auch ein selbst erzeugtes Schlüsselpaar benutzen.

Bei Verwendung von Mailvelope finden Sie im mailbox.org-Office die entsprechenden Einstellungen unter **Einstellungen -> Sicherheit -> Mailvelope**.

### Abfrage des Schlüsselpassworts

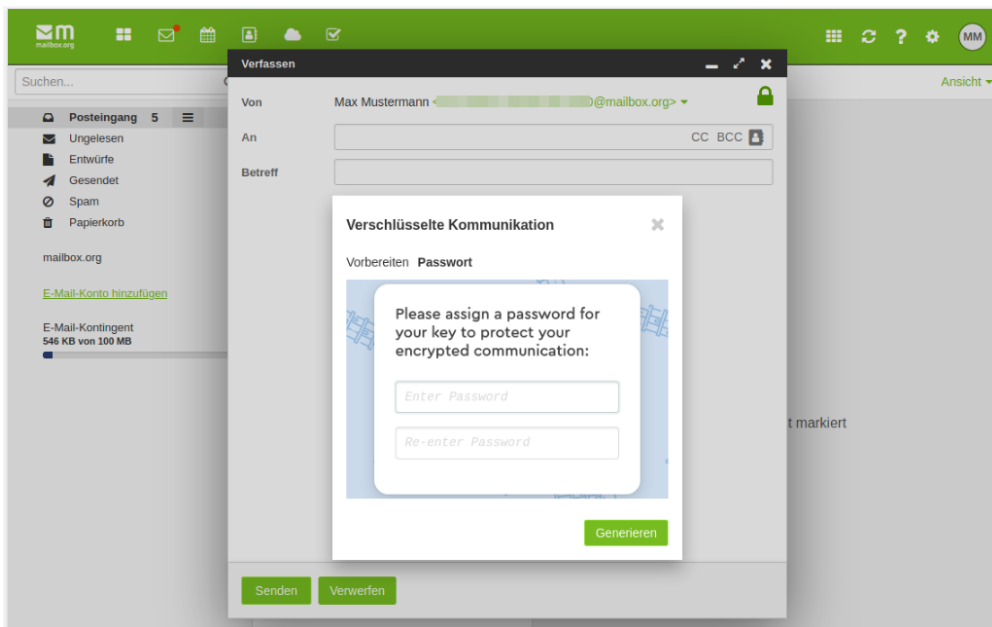
Wenn Sie nach dem Einrichten ihres Schlüsselpaares erstmalig auf das Schlosssymbol gehen, also ihre erste verschlüsselte E-Mail senden wollen vergeben Sie ein Schlüsselpasswort.

Merken Sie sich das Passwort gut, es kann nicht wieder hergestellt werden.

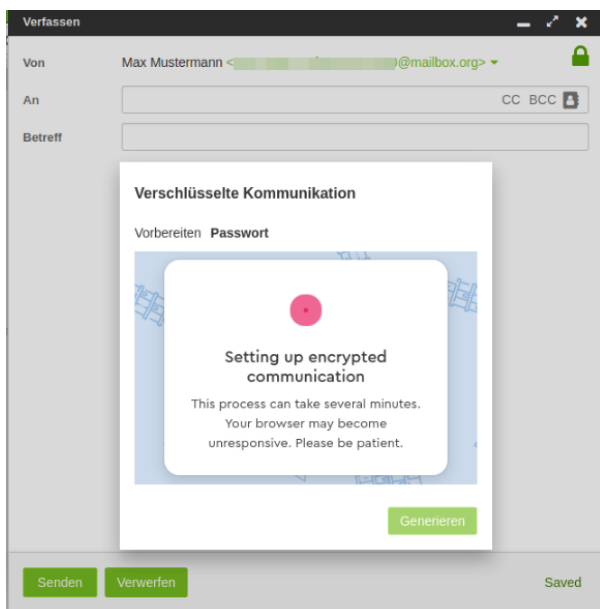
siehe [https://mailvelope.com/de/faq#key\\_administration](https://mailvelope.com/de/faq#key_administration).

So können sie beispielsweise das Schlüsselpaar, das vom mailbox.org-Guard erstellt wurde oder auch ein selbst erzeugtes Schlüsselpaar benutzen.

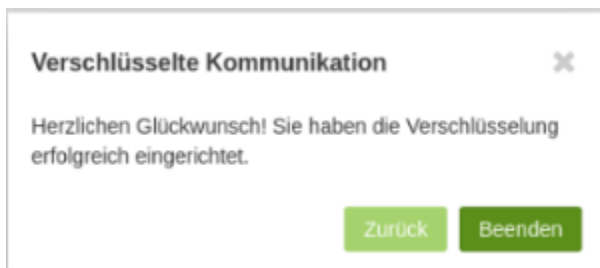
Sobald Sie ihre erste verschlüsselte E-Mail senden wollen, und sobald Sie auf das Schlosssymbol gehen vergeben Sie ein Schlüsselpasswort. Aber Achtung, merken Sie sich das Passwort gut, es kann nicht wieder hergestellt werden.



Merken Sie sich das **Passwort gut**. Es kann **nicht** wieder hergestellt werden!



Das Add-on werkelt eine gute Weile, **unterbrechen Sie keinesfalls diesen Vorgang**.



Um nun verschlüsselt zu Kommunizieren benötigen Sie wie immer den Public-Key ihrer Kommunikationspartner, [wie das geht ist auch gut dokumentiert, siehe oben](#).

Um anschließend eine **verschlüsselte** E-Mail zu schreiben, gehen Sie ähnlich wie bei der Benutzung vom Guard vor. Klicken Sie einfach auf das Schlosssymbol im E-Mail verfassen Dialog. Das nun aber der Mailvelope-Editor benutzt wird erkennen Sie an dem farbenfrohen individualisierbarem Hintergrund von Mailvelope, den Sie schon von den ersten Schritten mit Mailvelope kennen.