

Das Add-on Mailvelope verwenden

Mailvelope - eine Übersicht

„**Mailvelope**“ ist ein **Browser Add-on**, welches für Mozilla Firefox und Google Chrome verfügbar ist. 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 [Sicherheitsanalyse von Mailvelope durch Cure53 \(pdf\)](#) weist am Ende auf das Risiko von XSS-Angriffe hin. Insbesondere Nutzer von Mozilla Firefox sind dabei gefährdet, da dieser Browser **weniger Schutzmechanismen bietet** 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 von Mailvelope

Um Mailvelope mit dem mailbox.org-Office zu nutzen, müssen Sie das Add-on zuerst installieren. Alle aktuellen Versionen sind für die Nutzung mit mailbox.org geeignet.

Damit sind die Vorbereitungen bereits abgeschlossen.

Aktivierung der Mailvelope Unterstützung

Nun können Sie im Webclient unter „**Einstellungen -> mailbox.org -> PGP im Webmailer**“ zwischen dem mailbox.org Guard und Mailvelope wählen. Konfigurieren Sie abschließend das Add-On.

The screenshot shows the mailbox.org interface for configuring PGP in the webmail client. The page is titled "PGP im Webmailer".

Annotation 1: Points to the "Einstellungen" (Settings) menu in the top right corner.

Annotation 2: Points to the "Einstellungen" (Settings) menu in the top right corner.

Annotation 3: Points to the "mailbox.org" logo in the top left corner.

Annotation 4: Points to the "PGP im Webmailer" link in the left sidebar menu.

Annotation 5: Points to the "aktiviert" (activated) button at the bottom of the page.

The main content area includes:

- A warning box: "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." (Before you switch the PGP encryption method, we recommend that you back up your current PGP key. In order to be able to read your already encrypted emails, you must add this PGP key to the new encryption method you have selected.)
- Two columns of options:
 - Einfach und intuitiv mit dem Guard:**
 - Verschlüsselung von E-Mails und Dateien mit nur einem Klick
 - Funktioniert in allen Browsern mit allen Ihren Kontakten
 - Einfach anwendbar, täglich
 - Sicherheitsdetails durch uns verwaltet
 - Verschlüsselung für Experten mit Mailvelope:**
 - Verschlüsselungsoptionen für Experten verfügbar
 - Funktioniert nur in Firefox und Chrome
 - Browser-Plugin erforderlich
 - Sicherheitsdetails durch Sie selbst verwaltet
- Two paragraphs of explanatory text:
 - 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** einrichtet gemacht!
 - 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.
- Two buttons at the bottom: "aktiviert" (highlighted with annotation 5) and "jetzt aktivieren" (activate now).

Verwandte Artikel

- [Wem ich bei mailbox.org vertraue](#)
- [Die Zwei-Faktor-Authentifizierung einrichten](#)
- [Das temporäre Postfach fuer externe Nutzer](#)
- [Den Tor Browser konfigurieren](#)
- [Den Tor-Exit-Node von mailbox.org verwenden](#)