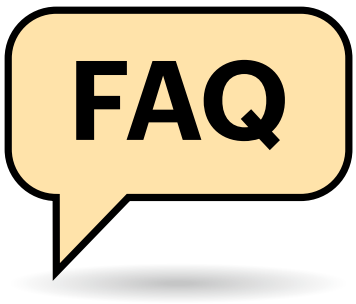


PGP-Verschlüsselung mit Thunderbird

Seit Version 78 ist die Verschlüsselung mit OpenPGP in den Mailclient Thunderbird eingebaut. Allerdings hakt es an einigen Stellen noch, was gerade altgedienten Enigmail-Nutzern Probleme bereitet.

Von Sylvester Tremmel

Hintergrund

Warum nutzt Thunderbird nicht einfach weiter das Add-on Enigmail?

Seit einigen Versionen stellt Thunderbird seine Add-on-Schnittstelle auf „MailExtensions“ um, die auf „WebExtensions“ des Browsers Firefox basieren. Mit Version 78 haben die Entwickler die Unterstützung für die alten „Legacy Add-ons“ eingestellt. Enigmail auf die neue Schnittstelle zu portieren wäre sehr aufwendig gewesen und der Entwickler des Add-ons sah sich außerstande, so viel Zeit zu investieren.

Hätte Thunderbird nicht wenigstens GnuPG nutzen können, wie Enigmail es tat? Dann müsste man keine Schlüssel migrieren.

Die Thunderbird-Entwickler wollten aus verschiedenen Gründen nicht auf eine externe Software wie GnuPG angewiesen sein. Zum Beispiel müssten Nutzer dann weitere Programme installieren, bevor sie ein in den Mailer integriertes Feature nutzen könnten. Außerdem müssten die Thunderbird-Entwickler ihre Software konstant an Änderungen in GnuPG anpassen. Das wäre aufwendig und war offenbar ein Problem, unter dem Enigmail regelmäßig zu leiden hatte.

GnuPG in den Mailclient zu integrieren war ebenfalls keine Option. Zum einen würde das zahlreiche mögliche Fehlerquellen schaffen (etwa wenn das integrierte GnuPG in Konflikt mit einer extern installierten Version gerät). Vor allem sahen die Entwickler aber Lizenzprobleme: Thunderbird und GnuPG nutzen verschiedene Open-Source-Lizenzen (MPL vs. GPL), die nur schwer zu kombinieren sind [1].

Denkbar wäre auch gewesen, dass die Thunderbird-Entwickler zwar nicht GnuPG nutzen, aber auf dieselben Dateien zurückgreifen, um Schlüssel und Einstellungen zu speichern. Das hätte aber fast zwangsläufig zu gravierenden Kompatibilitätsproblemen geführt. Diese Dateien folgen schließlich keinem offiziellen Standard, sondern beruhen auf GnuPG-Interna, die sich jederzeit ändern können.

Was nutzt Thunderbird denn, wenn es nicht GnuPG ist?

Der Mailclient nutzt die Bibliothek „RNP“ (siehe ct.de/y7t9), die kompatibel mit dem OpenPGP-Nachrichtenformat ist und unter einer passenden Lizenz (BSD) steht. Allerdings unterstützt RNP zumindest aktuell nicht alle Features von GnuPG, was zu Problemen bei der Migration und der Nutzung von Schlüsseln führen kann.

Migrationsprobleme

Bei mir hat sich kein Migrationsassistent geöffnet. Wie kann ich jetzt meine Schlüssel aus Enigmail zu Thunderbird migrieren?

Der Migrationsassistent ist eine spezielle Variante von Enigmail (Version 2.2.x), die nur mit Thunderbird 78 kompatibel ist. Das eigentliche Enigmail-Add-on trägt die Versionsnummer 2.1.x und ist mit Thunderbird 78 nicht kompatibel. Idealerweise geschieht der Umstieg folgendermaßen:

1. Thunderbird 68 hat Enigmail 2.1.x installiert.
2. Nach einem Upgrade auf Version 78 erkennt Thunderbird, dass Enigmail 2.1 nicht kompatibel ist, aber Version 2.2 für Thunderbird 78 zur Verfügung steht und aktualisiert das Add-on.
3. Enigmail 2.2 erkennt, dass noch keine Schlüssel migriert wurden, und öffnet einen Begrüßungs-Tab mit dem Migrationsassistenten.

Offenbar klemmt es in diesem Ablauf häufiger. Man sollte zuerst sicherstellen, dass tatsächlich Version 2.2.x des Enigmail-Add-ons installiert ist. Danach kann der Migrationsassistent auch manuell über „Extras/Enigmail-Einstellungen migrieren“ aufgerufen werden. Falls Ihr Thunderbird keine Menüzeile anzeigt, finden Sie den Punkt „Extras“ im Hamburger-Menü (Schaltfläche mit drei Strichen).

Die Migration funktioniert nicht. Was jetzt?

Zunächst die gute Nachricht: Thunderbird greift bei der Migration nur lesend auf die GnuPG-Schlüssel zu. Wegen eines Migrationsfehlers kann also nichts verloren gehen, und die Migration darf ausdrücklich auch mehrfach durchgeführt werden. Es kann also helfen, die Migration einfach noch einmal zu starten (wie in der vorhergehende Frage beschrieben).

Alternativ zum Migrationsassistenten können Sie Schlüssel auch manuell migrieren. Das ist auch der Weg der Wahl, wenn Sie von einer anderen Software als Enigmail/GnuPG auf Thunderbird umsteigen wollen. Dazu exportieren Sie die eigenen und fremden Schlüssel in Dateien und importieren diese dann in Thunderbird.

Wie der Export erfolgt, hängt von Ihrer PGP-Software ab. Unter GnuPG exportieren Sie öffentliche Schlüssel – sowohl Ihre eigenen als auch die Schlüssel Ihrer Korrespondenzpartner – zum Beispiel mit folgendem Befehl:

```
gpg --export --armor > schluessel.asc
```

Ihre eigenen, privaten Schlüssel exportieren Sie folgendermaßen:

```
gpg --export-secret-keys --armor > \
  geheime_schluessel.asc
```

Auf letztere Datei müssen Sie gut achtgeben. Am besten löschen Sie sie gleich nach der Migration (auch aus dem Papierkorb).

Importieren können Sie die Dateien am einfachsten über Thunderbirds Schlüsselverwaltung, die Sie über „Extras/OpenPGP-Schlüssel verwalten“ erreichen. Das „Datei“-Menü der Schlüsselverwaltung bietet Punkte zum Import privater und öffentlicher Schlüssel. Sowohl das Einlesen der Datei als auch der eigentliche Import kann etwas dauern. Leider steht währenddessen die Programmoberfläche still, ohne dass Thunderbird einen Fortschrittsbalken oder dergleichen anzeigt.

? Der manuelle Import meiner Schlüsseldatei funktioniert nicht, Thunderbird sagt, die Datei sei zu groß.

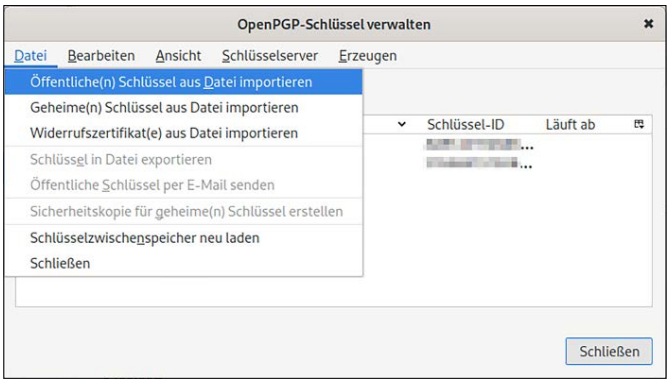
! Das tritt insbesondere beim Import einer großen Menge öffentlicher Schlüssel auf. Thunderbird kann aktuell keine Schlüsseldateien importieren, die größer als 5 MByte sind. Sie müssen daher beim Export die Schlüssel auf mehrere Dateien verteilen. (Oder doch den Enigmail-Assistenten nutzen, falls möglich.) Dem `gpg`-Befehl können Sie einfach Namen oder Mailadressen als Argumente übergeben, um den Export einzuschränken:

```
gpg --export --armor mail@domain.com \
  "Max Mustermann" > schluessel.asc
```

Schlüsselauswahl

? Die Migration hat angeblich geklappt, aber Thunderbird erlaubt mir immer noch nicht, E-Mails zu verschlüsseln.

! Vermutlich ist Ihr privater Schlüssel zwar importiert, aber noch nicht als Schlüssel für einen Account festgelegt. Thunderbird verlangt diesen Schritt, damit automatisch importierte Schlüssel nicht unbeabsichtigt genutzt werden. Öffnen Sie die Konten-Einstellungen und navigieren Sie zum Punkt „Ende-zu-Ende-Verschlüsselung“ des betroffenen Kontos. Unter „OpenPGP“ sollte Thunderbird dort Ihren Schlüssel anbieten. Wählen Sie ihn aus, um ihn nutzen zu können.



Schlüssel importiert man am einfachsten über das Menü der Schlüsselverwaltung. Leider zeigt Thunderbird nicht an, dass der Import läuft.

? Ich habe meinen privaten Schlüssel importiert, kann ihn aber nicht in meinem Konto auswählen.

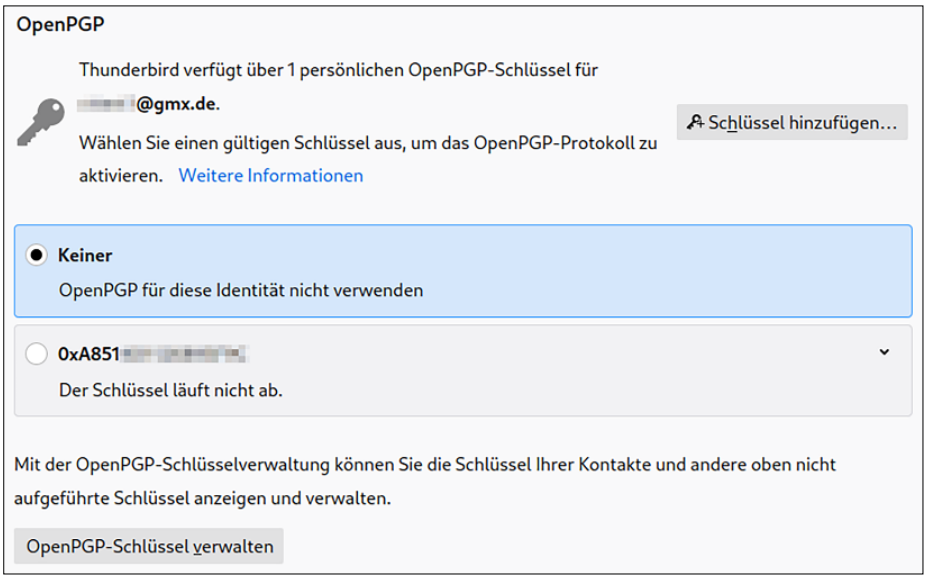
! Damit der Schlüssel für ein Konto genutzt werden kann, muss die Mailadresse des Kontos exakt mit der in der User-ID des Schlüssels übereinstimmen. Mit Schlüsseln, bei denen das nicht der Fall ist, kann Thunderbird momentan nicht umgehen, wie auch mit Schlüsseln auf einer Smartcard und mit einigen anderen Setups.

Für private Schlüssel – also beim Entschlüsseln und Signieren – bietet Thunderbird aktuell die Möglichkeit, doch eine externe GnuPG-Installation zu verwenden. Eine Erklärung dazu finden Sie im Thunderbird-Wiki (siehe ct.de/y7t9). Beachten Sie, dass so ein Setup nicht ganz trivial ist und eigentlich ausschließlich die Nutzung von Smartcard-Schlüsseln ermöglichen soll. Die Möglichkeit der GnuPG-Nutzung soll wegfallen, wenn Thunderbird selbst mit Smartcards umgehen kann. Mit OpenPGP wenig erfahrene Benutzer sind vermutlich besser damit beraten, lieber einen neuen, Thunderbird-konformen Schlüssel direkt vom Mailprogramm erstellen zu lassen.

Schlüsselverwaltung

? Beim Versenden einer verschlüsselten E-Mail meldet Thunderbird einen Fehler; es sei „kein Schlüssel vorhanden“.

! Thunderbird hat vermutlich den öffentlichen Schlüssel des Empfängers noch nicht, kann aber nach passenden Schlüsseln suchen. Klicken Sie dazu die Fehlermeldung mit „Schließen“ weg, wählen Sie im folgenden Fenster den betroffe-



Auch wenn Thunderbird einen passenden privaten Schlüssel findet (erste Zeile), wird er nicht automatisch genutzt. Dafür muss man ihn an Stelle von „Keiner“ auswählen.

nen Empfänger und klicken Sie auf „Schlüssel für gewählten Empfänger verwalten…“. Klicken Sie nun auf „Neuen oder aktualisierten Schlüssel suchen“.

Thunderbird versucht nun – leider ohne visuelle Rückmeldung – passende Schlüssel per Web Key Directory (WKD) oder auf keys.openpgp.org nachzuschlagen, was ein paar Sekunden dauert. Bei Erfolg erscheint ein Fenster mit passenden Schlüsseln zum Import. Vergessen Sie nicht, die Schlüssel auch zu akzeptieren (siehe unten).

Falls Thunderbird keinen Schlüssel findet, müssen Sie den Schlüssel irgendwie anders erhalten und über die Schlüsselverwaltung manuell importieren. Andere Suchmethoden – etwa die unsicheren SKS-Keyserver – unterstützt Thunderbird nämlich nicht. Allerdings kann der Mailer Schlüssel, die per Mail zugeschickt werden, bequem importieren.

? Ich habe den öffentlichen Schlüssel eines Empfängers importiert, aber Thunderbird behauptet trotzdem, es sei „kein Schlüssel vorhanden“.

! Thunderbird kann momentan mit diversen Schlüsselvarianten nicht umgehen. Lästig ist vor allem, dass die Mailadresse in der User-ID eines Schlüssels exakt mit der Adresse des Empfängers übereinstimmen muss. Anonyme Schlüssel, oder solche, die für Gruppen oder ganze Domains genutzt werden sollen, sind damit außen vor.

Umgehen lässt sich dieses Problem nicht. Die Entwickler arbeiten zwar daran, aber eine Lösung wird es wohl frühestens mit dem nächsten großen Versionssprung von Thunderbird geben – zumindest eine Lösung, die in die Programmoberfläche integriert ist. Ein notdürftiger Workaround könnte es vielleicht noch in eine 78.x-Version schaffen.

Wenn Sie auf die Nutzung solcher Schlüssel angewiesen sind, bleibt aktuell nur die Möglichkeit, Thunderbird 68 mit Enigmail weiterzunutzen – oder einstweilen auf einen anderen Mailclient umzustellen. Letzteres ist unter Sicherheitsaspekten die bessere Wahl.

? Ich habe den öffentlichen Schlüssel eines Empfängers importiert, kann aber keine verschlüsselten E-Mails an ihn versenden. Thunderbird sagt, der Schlüssel wäre nicht „akzeptiert“.

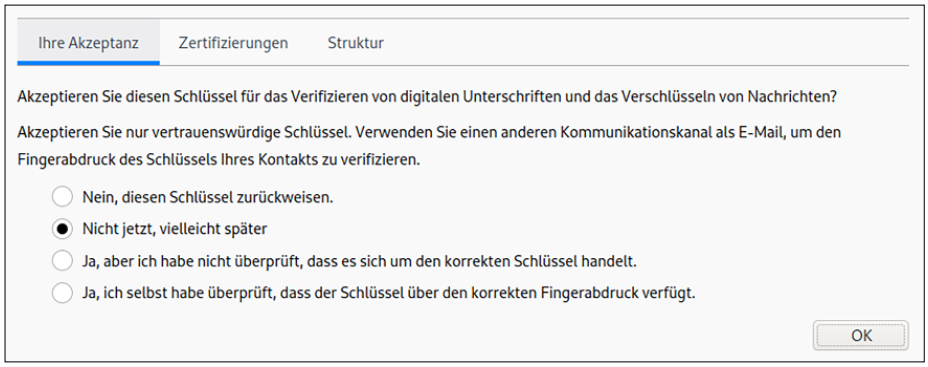
! Thunderbird setzt bewusst keine opportunistische Verschlüsselung ein und verlangt, dass man Schlüssel nicht nur importiert, sondern auch explizit akzeptiert, bevor sie verwendet werden. Diese „Akzeptanz“ entspricht in etwa dem „Vertrauen“ in einen Schlüssel unter GnuPG.

Um den Schlüssel zu akzeptieren, klicken Sie die Fehlermeldung mit „Schließen“ weg, wählen im folgenden Fenster den betroffenen Empfänger und klicken auf „Schlüssel für gewählten Empfänger verwalten…“. Wählen Sie nun – falls nötig – den nicht akzeptierten Schlüssel aus und klicken auf „Details öffnen und Akzeptanz bearbeiten…“. Im Fenster mit den Schlüsseleigenschaften müssen Sie unter „Ihre Akzeptanz“ eine der beiden Optionen mit „Ja …“ auswählen (je nachdem welche zutrifft). Danach können Sie den Schlüssel nutzen.

? Thunderbird 78 verlangt kein Passwort für meinen geheimen Schlüssel. Liegt der etwa ungeschützt auf der Festplatte?

! Das kann sein! Thunderbird verschlüsselt geheime Schlüssel zwar mit einer zufälligen Passphrase, legt diese aber einfach so auf der Festplatte ab, wenn Sie kein Masterpasswort setzen. Sie sollten daher unbedingt in den Einstellungen unter „Datenschutz & Sicherheit/Passwörter“ die Option „Master-Passwort verwenden“ auswählen und ein gutes Passwort vergeben.

Wenn ein Master-Passwort gesetzt ist, dann verschlüsselt Thunderbird damit die zufällige Passphrase, die wiederum Ihren Schlüssel schützt. Einen Time-out gibt es anders als in Enigmail aktuell leider nicht, die Passwort-Eingabe gilt, solange Thunderbird geöffnet ist.



Thunderbird verwendet nur Schlüssel, die akzeptiert wurden, bei denen also eine der beiden „Ja“-Optionen ausgewählt ist.

Re: …?

? Meine Korrespondenzpartner können mit Thunderbird versandte Mails zwar entschlüsseln, sehen aber nur drei Punkte (…) statt des Betreffs. Wenn Sie mir antworten, sehe ich ebenfalls nur noch drei Punkte (Re: …).

! Thunderbird verschlüsselt den Betreff von E-Mails. Das ist sinnvoll, schließlich finden sich oft bereits im Betreff schützenswerte Informationen. Um Kompatibilität mit Clients herzustellen, die damit nicht umgehen können, geht Thunderbird wie folgt vor: Die verschlüsselte Mail (samt dem wahren Betreff) wird als MIME-Part in eine äußere, unverschlüsselte Mail verpackt, die den Betreff „…“ bekommt. Mit der Verschachtelung können moderne Mailprogramme umgehen, aber Clients, die diese Betreffverschlüsselung nicht beherrschen, zeigen nur den nichtssagenden äußeren Betreff an.

Beim Antworten übernehmen diese Clients ebenfalls nur den äußeren Betreff, was zwar lästig ist, aber zumindest verhindert, dass so ein Client den geheimen Betreff in einer Antwort preisgibt, nur weil er keine Betreffverschlüsselung unterstützt.

Abschalten lässt sich das Verhalten von Thunderbird aktuell nicht. Besser wäre ohnehin, wenn andere Clients rasch lernten, den Betreff ebenfalls zu verschlüsseln. *(syt@ct.de)*

Literatur

[1] Sylvester Tremmel, Lizenz zum Coden, Was Open-Source-Lizenzen voneinander unterscheidet, c’t 1/2020, S. 68

Weitere Infos: ***ct.de/y7t9***