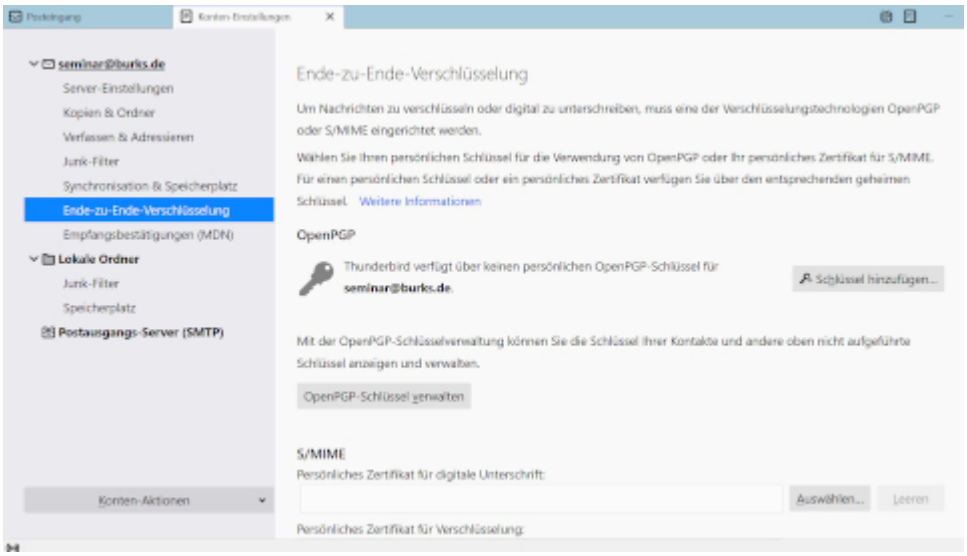
Verschlüsseln mit Thunderbird 78.0 (Windows)

Am 13.10.20 schrieb ich hier über die Grundlagen der Verschlüsselung und die verschiedenen Methoden – mit und ohne E-Mail-Programm oder gar per Browser. Nun folgt ein Tutorial, wie man E-Mails verschlüsselt ab Version 78 des E-Mail-Programms Thunderbird. Im Gegensatz zu den älteren Versionen bringt Thunderbird *jetzt sein eigenes Verschlüsselungsprogramm „ab Werk" mit. Wir benötigen also weder* GnuPG *noch ein Add-on wie* Enigmail*. Auf der obigen Skizze ist das heutige Thema grau unterlegt.*

Alle Funktionen, die man braucht, in nur einem Programm – die Sache sollte also einfacher sein als vorher. Überraschenderweise stimmt das auch. Es gibt natürlich wie immer ein paar Fallstricke.

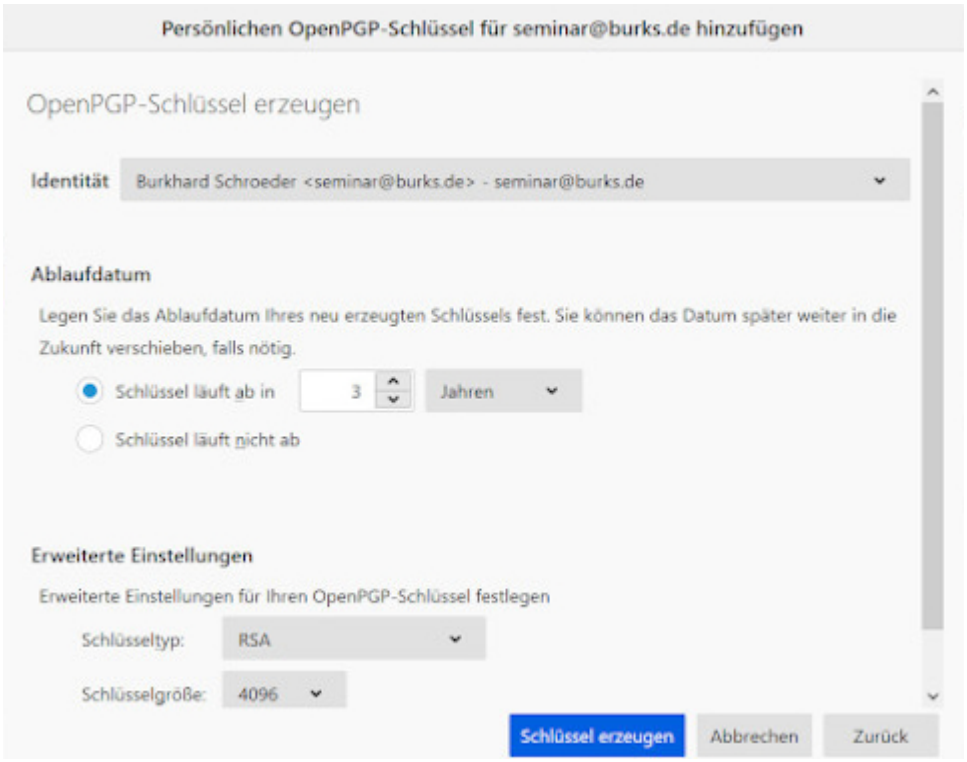


1. Schritt: Ein Schlüsselpaar erzeugen

Die Funktionen zum Ver- und Entschlüsseln verstecken sich in den *Konteneinstellungen* unter dem Menü *Ende-zu-Ende-Verschlüsselung* (vgl. Screenshot oben – zum Vergrößern klicken). Bevor wir loslegen, müssen wir ein so genanntes *Schlüsselpaar* erzeugen. Wer so etwas schon hatte, kann diese Schlüssel per Button *OpenPGP-Schlüssel verwalten* importieren. Wählen wir den Button *Schlüssel hinzufügen* – womit *erzeugen* gemeint ist (aber warum sollte man sich verständlich ausdrücken?) -, erzeugt das Programm einen *geheimen* und einen

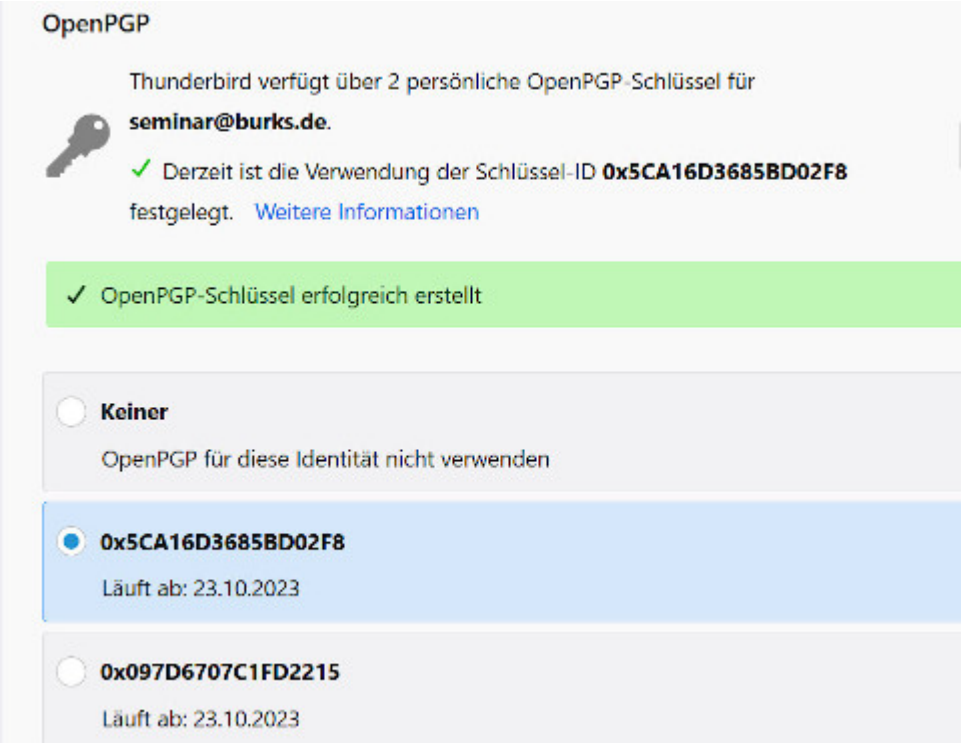
öffentlichen Schlüssel – das *Schlüsselpaar*. [Das sind schlicht zwei Dateien im ascii-Format: American Standard Code for Information Interchange.]

Die verschiedenen Optionen, die angeboten werden (vgl. Screenshot unten, wie lange gültig usw.), sind Kür – man kann alles so lassen, wie es schon eingestellt ist. Ich bin sportlich-paranoid und nehme natürlich immer den „längsten“ Schlüssel – hier 4096 Bit.



Das Ergebnis – hier nur ein „Dummy“: Ein Schlüssel (aus zwei Teilen), der eine unverwechselbare Kennung hat – die ID 0x5CA16D3685BD02F8. Diese ID kann man nicht fälschen. Man

erkennt einen Schlüssel an der E-Mail-Adresse, die man zu Beginn definiert hat *und* an der Kennung.

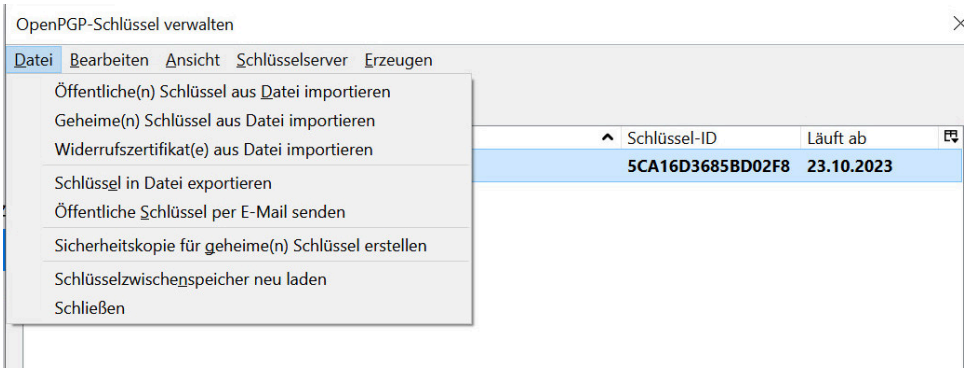


Ich kann natürlich einen Schlüssel Olga_Kurylenko@007.com nennen und ihn benutzen, aber die ID kann man nicht selbst bestimmen – das ist reine Mathematik. Wir sehen schon, dass die Authentizität eines Schlüssels nicht so einfach festgestellt werden kann. Das Problem können und müssen wir sofort lösen, weil das Programm später meckerte, wenn wir eine verschlüsselte E-Mail schreiben wollten.

Wir gehen wieder in *Konteneinstellungen* zum Menü *Ende-zu-Ende-Verschlüsselung* und schauen uns *OpenPGP-Schlüssel verwalten* an. Da dürfte nur das gerade von uns erzeugte Schlüsselpaar zu sehen sein. Ein Mausklick zeigt uns dessen *Akzeptanz* – wir müssen noch einmal kräftig virtuell nicken und bestätigen, dass wir diesen Schlüssel verwenden wollen.

2. Schritt: Den öffentlichen Schlüssel exportieren und importieren

Wer blutiger Anfänger ist und jetzt die Sache mit den „Schlüsseln“ (einer? mehrere? Paare?) nicht versteht, sollte kurz in das Tutorial „E-Mails verschlüsseln in 30 Minuten“ schauen – ab *Schritt 5*. Dort wird das Prinzip kurz und bündig erklärt.



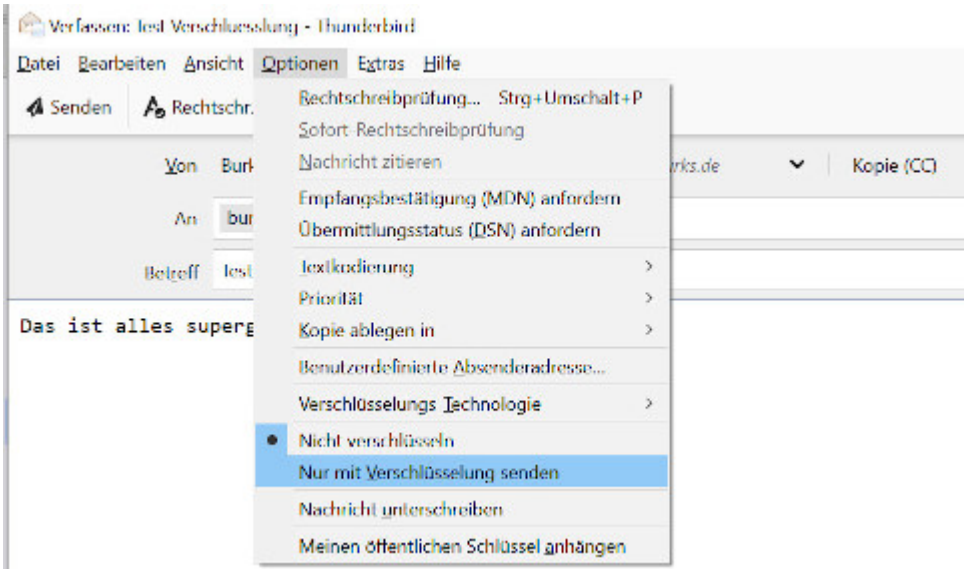
In der *Schlüsselverwaltung* unter dem Menü *Datei* haben wir alles hübsch beisammen: Importieren, exportieren, ein Widerrufszertifikat erzeugen (wenn unser Schlüssel später ungültig wird und wir ihn optional auf einen Schlüsselserver hochgeladen hatten) usw.. Wir brauchen nur den Export und den Import, alles andere kann warten. *Export*: unseren *offentlicher* Schlüssel müssen alle diejenigen bekommen, mit denen wir verschlüsselte E-Mails austauschen wollen. (Vorsicht: *Nicht* den *geheimen* exportieren – der bleibt immer schön auf unserem

Rechner – nur für ein Backup des Schlüsselpaares ist dieses Feature nützlich).

Wir müssen auch jeweils deren *öffentliche* Schlüssel importieren. Haben wir das getan, erscheinen „fremde“ öffentliche Schlüssel in unserem „Schlüsselbund“ (*OpenPGP-Schlüssel verwalten*).

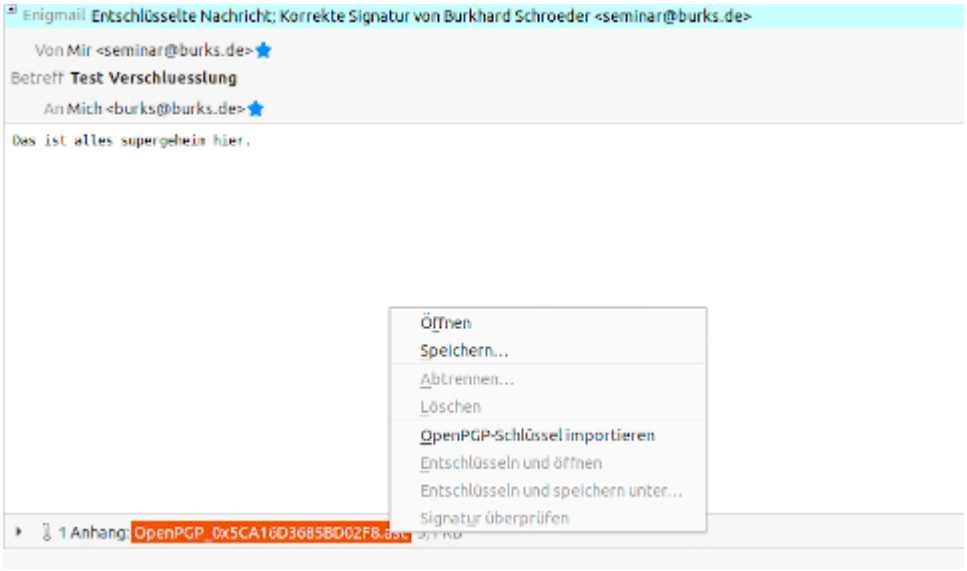
3. Schritt: Eine verschlüsselte E-Mail schreiben und versenden

Mehr müssen wir nicht tun. Wir schreiben jetzt eine schrecklich geheime E-Mail im Klartext, drücken dann im Menü *Optionen* und aktivieren dort *nur mit Verschlüsselung senden*. Später kann man so genannte Empfängerregeln erstellen, mit wem man im Klartext schreibt und mit wem nicht – um nicht immer wieder die Optionen bemühen zu müssen.



In diesem Beispiel hat der Dummy mit der E-Mail-Adresse seminar@burks.de an mich (burks@burks.de) geschrieben, *nachdem* er sich meinen öffentlichen Schlüssel vom Impressum meiner Webseite geholt und importiert hat. Das Ergebnis kann sich sehen lassen. Der Screenshot unten zeigt *mein* Thunderbird (Linux). Ich musste nur mein Passwort eingeben (was optional ist) und der kryptische Datensalat verwandelte sich in Klartext. Der *öffentliche Schlüssel* des Dummys ist als Attachment auch gleich mitgekommen, falls ich den noch nicht

hatte. Den brauche ich, um zu antworten.



Man kann dazu noch Stunden dozieren, aber zuerst sollte man ein Erfolgserlebnis haben, bevor man zum Kleingedruckten und zu Features kommt, die etwas komplizierter sind als oben Gezeigte.