

# Installation und Verwendung Ihres persönlichen Nutzerzertifikates im Thunderbird

## Kurzbeschreibung

Durch Installation Ihres persönlichen Nutzerzertifikates ist es Ihnen möglich E-Mails zu signieren und verschlüsseln, sowie für Sie verschlüsselte E-Mails zu lesen. Hinweise zum Haupt-/Masterpasswort des Thunderbird finden Sie am Ende dieser Beschreibung.

---

## Voraussetzung

Sie haben Ihr persönliches Nutzerzertifikat wie beschrieben erstellt und können auf den Speicherort zugreifen, z.B. "\\Eigene Dateien\\datum\_emailadresse.p12")

Sie haben ihre Zertifikat-PIN das sie beim Erstellen ihrer Zertifikatsdatei vergeben haben

## Importieren Ihres persönlichen Nutzerzertifikates und Einrichten für Signieren und/oder Verschlüsseln

---

starten Sie Ihr E-Mailprogramm Thunderbird

klicken Sie auf *Extras -> Konten-Einstellungen*

es öffnet sich die Kontenansicht

klicken Sie auf *S/MIME -Sicherheit / Ende zu Ende Verschlüsselung oder S/MIME-Zertifikate-Verwalten*

Ende-zu-Ende-Verschlüsselung

Um Nachrichten zu verschlüsseln oder digital zu unterschreiben, muss eine der Verschlüsselungstechnologien OpenPGP oder S/MIME eingerichtet werden.

Wählen Sie Ihren persönlichen Schlüssel für die Verwendung von OpenPGP oder Ihr persönliches Zertifikat für S/MIME. Für einen persönlichen Schlüssel oder ein persönliches Zertifikat verfügen Sie über den entsprechenden geheimen Schlüssel. [Weitere Informationen](#)

**OpenPGP**

Thunderbird verfügt über keinen persönlichen OpenPGP-Schlüssel für **steffen.platzer@cms.hu-berlin.de**. [Schlüssel hinzufügen...](#)

Mit der OpenPGP-Schlüsselverwaltung können Sie die Schlüssel Ihrer Kontakte und andere oben nicht aufgeführte Schlüssel anzeigen und verwalten.

[OpenPGP-Schlüssel verwalten](#)

**S/MIME**

Persönliches Zertifikat für digitale Unterschrift:

[Auswählen...](#) [Leeren](#)

Persönliches Zertifikat für Verschlüsselung:

[Auswählen...](#) [Leeren](#)

[S/MIME-Zertifikate verwalten](#) [S/MIME-Kryptographie-Module verwalten](#)

**Senden von Nachrichten - Standardeinstellungen**

Ohne Ende-zu-Ende-Verschlüsselung ist der Inhalt Ihrer Nachrichten für Ihren E-Mail-Anbieter leicht zugänglich

es öffnet sich die Zertifikatsverwaltung, gehen Sie zum Reiter "Ihre Zertifikate"

klicken Sie auf *Importieren*

Zertifikatsverwaltung

**Ihre Zertifikate** Authentifizierungs-Entscheidungen Personen Server Zertifizierungsstellen

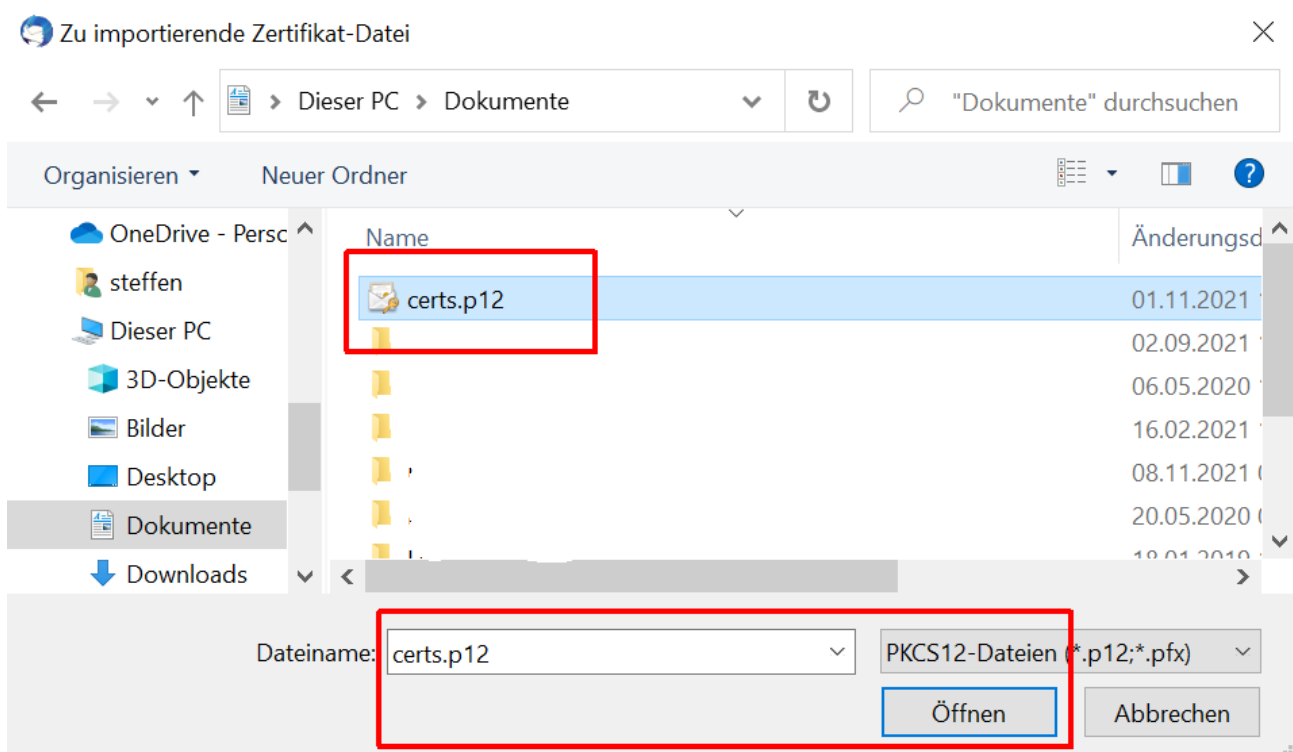
Sie haben Zertifikate dieser Organisationen, die Sie identifizieren:

Zertifikatsname	Kryptographie-M...	Gültig bis

[Ansehen...](#) [Sichern...](#) [Alle sichern...](#) [Importieren...](#) [Löschen...](#)

OK

ein Fenster zum Importieren des persönlichen Nutzerzertifikates öffnet sich



Wechseln Sie in das Verzeichnis wo Sie Ihre Zertifikatsdatei/persönliches Nutzerzertifikat während der Erstellung gespeichert haben z.B. "\Eigene Dateien\"

Markieren Sie dieses (z.B. certs.p12) und klicken auf *Öffnen*

Entweder werden Sie zur Eingabe Ihres Masterpasswortes aufgefordert (falls sie ein solches gesetzt haben), oder ...

wenn Sie das erste Mal ein persönliches Nutzerzertifikat installieren, werden Sie aufgefordert ein Masterpasswort für Ihr Kryptographie-Modul einzugeben

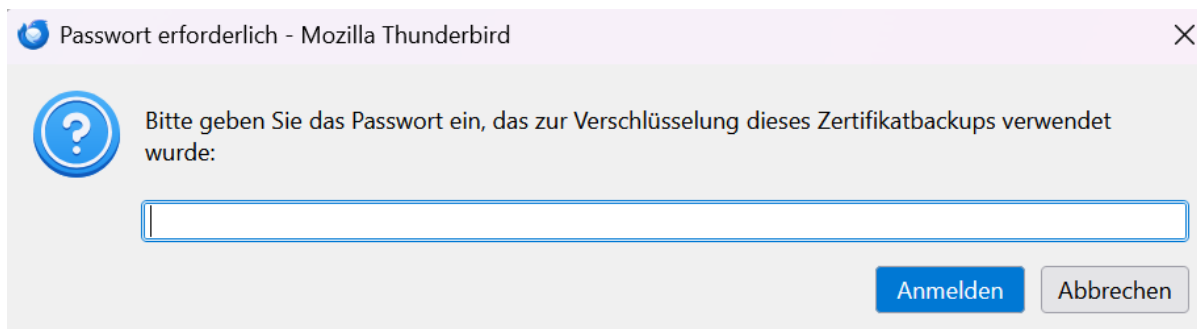


Wir empfehlen das setzen eines Masterpasswort

ACHUNG: Sie benötigen dies, wenn Sie E-Mails signieren, verschlüsseln oder entschlüsseln wollen.

Beachten Sie auch die Hinweise zum Masterpasswort am Ende der Beschreibung

danach werden Sie aufgefordert Ihre Zertifikat-PIN einzugeben welches sie beim Erstellen ihrer Zertifikatsdatei vergeben haben, bzw. angezeigt wurde.

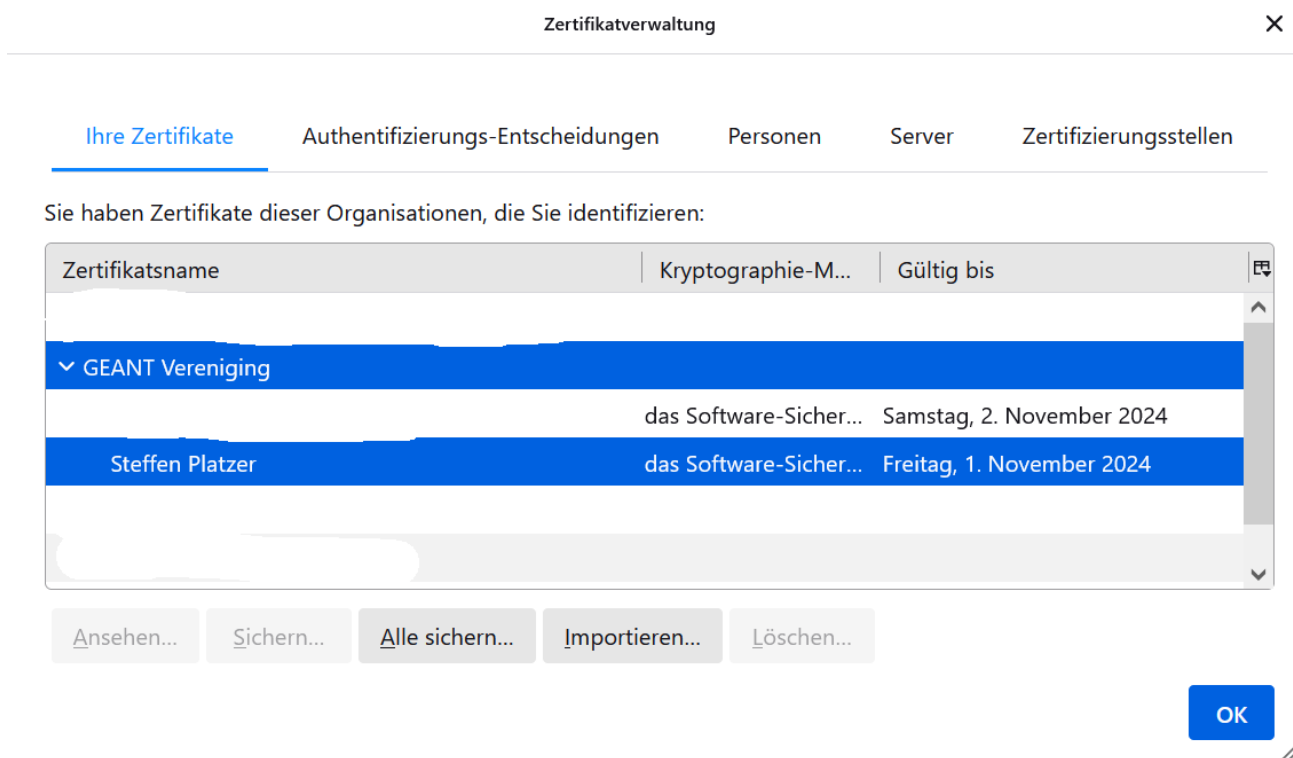


Nach korrekter Eingabe erscheint folgende Meldung.



Klicken Sie auf *OK* und Sie sehen im Zertifikatsmanager Ihr persönliches Zertifikat.

Achtung: Es kann auch vorkommen, dass der Import ohne Erfolgsmeldung erfolgt.



OK

Klicken Sie auf *OK* und Sie befinden sich wieder in der Kontenübersicht -> Ende-zu-Ende-Verschlüsselung oder S/MIME-Sicherheit.

Klicken Sie neben der Zeile digitale Unterschrift rechts auf *Auswählen*.

## S/MIME

Persönliches Zertifikat für digitale Unterschrift:

Auswählen...

Leeren

Persönliches Zertifikat für Verschlüsselung:

Auswählen...

Leeren

S/MIME-Zertifikate verwalten

S/MIME-Kryptographie-Module verwalten

## Senden von Nachrichten - Standardeinstellungen

Ohne Ende-zu-Ende-Verschlüsselung ist der Inhalt Ihrer Nachrichten für Ihren E-Mail-Anbieter leicht zugänglich und kann auch Bestandteil einer Massenüberwachung werden.

 Verschlüsselung - Standard-Ende-zu-Ende-Verschlüsselung

Ihr persönliches Zertifikat wird Ihnen zur Auswahl angeboten. Achten Sie darauf, das Zertifikat mit der längsten Gültigkeit auszuwählen.

Zertifikat auswählen

×

Zertifikat: Importiertes Zertifikat #3 [56:8D:93:3C:64:8C:57:E8:D3:B1:5F:CC:95:99:3F:AC] ▼

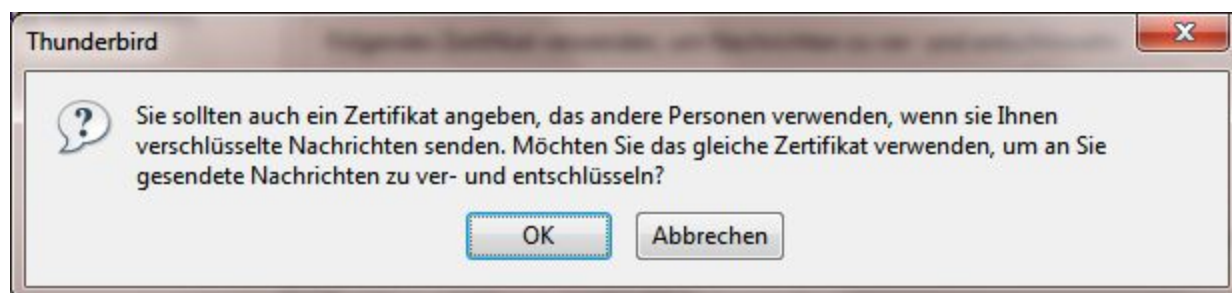
Details des ausgewählten Zertifikats:

Ausgestellt auf: CN=Steffen Platzer,O=Humboldt-Universitaet zu Berlin,C=DE,ST=Berlin,STREET=Unter den Linden 6  
56:8D:93:3C:64:8C:57:E8:D3:B1:5F:CC:95:99:3F:AC  
Gültig von Montag, 1. November 2021, 01:00:00 bis Freitag, 1. November 2024, 00:59:59  
E-Mail: steffen.platzer@cms.hu-berlin.de  
Ausgestellt von: CN=GEANT Personal CA 4,O=GEANT Vereniging,C=NL  
Gespeichert in: das Software-Sicherheitsmodul

OK

Abbrechen

Klicken Sie auf *OK*. Es wird Ihnen angeboten das gleiche Zertifikat auch für Verschlüsselung zu verwenden, klicken Sie *OK*.



## Auswahl digitale Unterschrift als Standard

### Senden von Nachrichten - Standardeinstellungen

Ohne Ende-zu-Ende-Verschlüsselung ist der Inhalt Ihrer Nachrichten für Ihren E-Mail-Anbieter leicht zugänglich und kann auch Bestandteil einer Massenüberwachung werden.

- ☒ Verschlüsselung standardmäßig nicht aktivieren
- ☐ Verschlüsselung standardmäßig verlangen

Falls Sie Verschlüsselung verwenden, benötigen Sie zum Senden einer Nachricht für jeden Empfänger dessen öffentlichen Schlüssel oder das Zertifikat.

Eine digitale Unterschrift ermöglicht den Empfängern zu überprüfen, dass die Nachricht von Ihnen gesendet sowie der Inhalt nicht geändert wurde.

- ☒ Eigene digitale Unterschrift standardmäßig hinzufügen

**Dringende Empfehlung: Sie sollten Ihre Nachrichten digital zu unterschreiben als Standard wählen. Damit verteilen Sie Ihr Zertifikat an die Empfänger und diese können es direkt für die verschlüsselte Kommunikation mit Ihnen benutzen.**

Das Einrichten/Einlesen Ihres Zertifikates in Thunderbird ist damit beendet.

[Vergessen Sie bitte nicht Ihr neues Nutzerzertifikat im HU-Adressbuch zu veröffentlichen.](#)

**Wenn bereits ein persönliches Zertifikat installiert ist sollten sie dies NICHT löschen damit sie ihre alten verschlüsselten E-Mails weiterhin lesen können.**

[Hinweise zum Haupt-/Masterpasswort](#)

[Zertifikat Backup anlegen](#)