

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\certs.p12)"

Sie haben ihr Passwort 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*

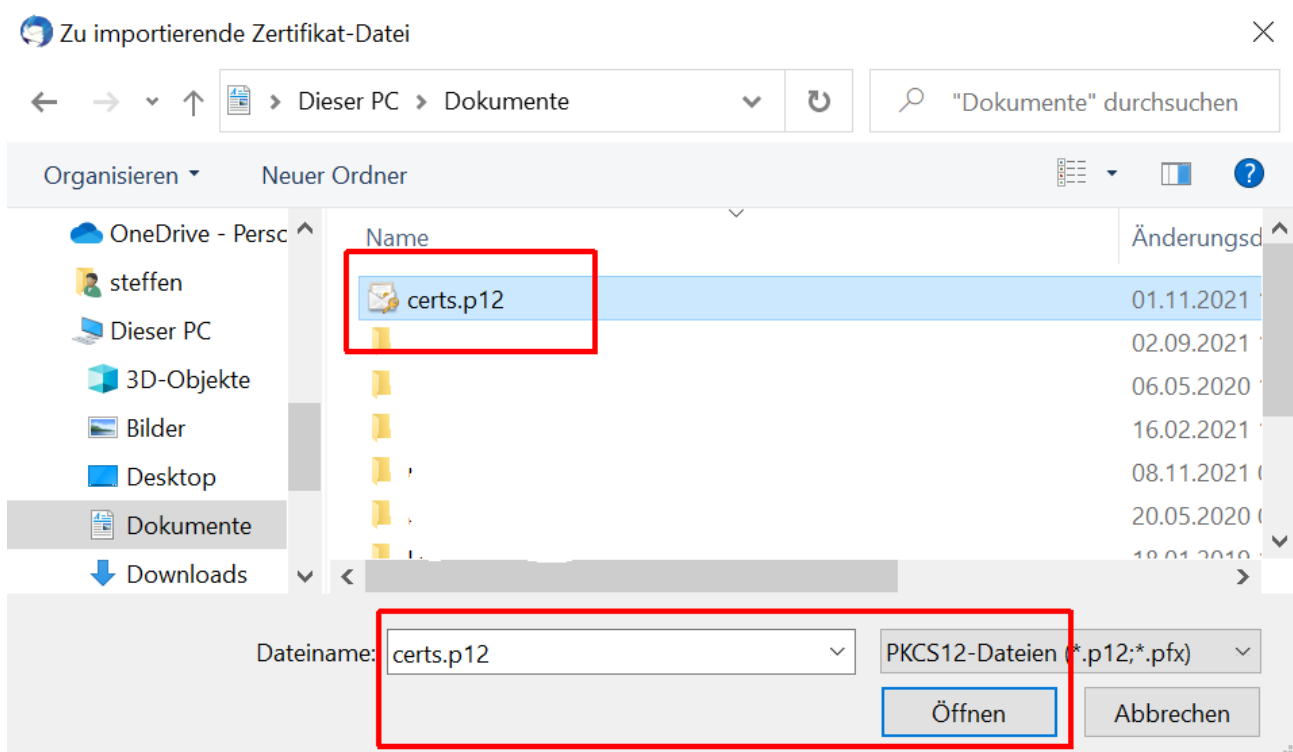
The screenshot shows the 'Konten-Einstellungen' window in Thunderbird. The left sidebar shows the account 'steffen.platzer@cms.hu-berlin.de' with various settings. The 'Ende-zu-Ende-Verschlüsselung' option is highlighted in blue. The main content area shows the 'Ende-zu-Ende-Verschlüsselung' settings. Under 'OpenPGP', it states that Thunderbird does not have a personal OpenPGP key for the account. There are buttons for 'Schlüssel hinzufügen...' and 'OpenPGP-Schlüssel verwalten'. Under 'S/MIME', there are input fields for 'Persönliches Zertifikat für digitale Unterschrift' and 'Persönliches Zertifikat für Verschlüsselung', each with 'Auswählen...' and 'Leeren' buttons. Below these are buttons for 'S/MIME-Zertifikate verwalten' and 'S/MIME-Kryptographie-Module verwalten'. At the bottom, there are settings for 'Senden von Nachrichten - Standardeinstellungen'.

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

klicken Sie auf *Importieren*

The screenshot shows the 'Zertifikatsverwaltung' window. The 'Ihre Zertifikate' tab is selected and highlighted with a red box. Other tabs include 'Authentifizierungs-Entscheidungen', 'Personen', 'Server', and 'Zertifizierungsstellen'. Below the tabs, it says 'Sie haben Zertifikate dieser Organisationen, die Sie identifizieren:'. A table with columns 'Zertifikatsname', 'Kryptographie-M...', and 'Gültig bis' is shown, but it is mostly obscured by a large greyed-out area. At the bottom, there are buttons for 'Ansehen...', 'Sichern...', 'Alle sichern...', 'Importieren...' (highlighted with a red box), and 'Löschen...'. An 'OK' button is in the bottom right corner.

ein Fenster zum Importieren des persönlichen Nutzerzertifikates öffnet sich



Wechseln Sie in das Verzeichnis wo Sie Ihr persönliches Nutzerzertifikat während der Erstellung gespeichert haben z.B. "\\Eigene Dateien\" oder "\\Dokumente\""

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 dieses immer, wenn Sie E-Mails signieren, verschlüsseln oder entschlüsseln wollen.

Beachten Sie auch die Hinweise zum Masterpasswort am Ende der Beschreibung

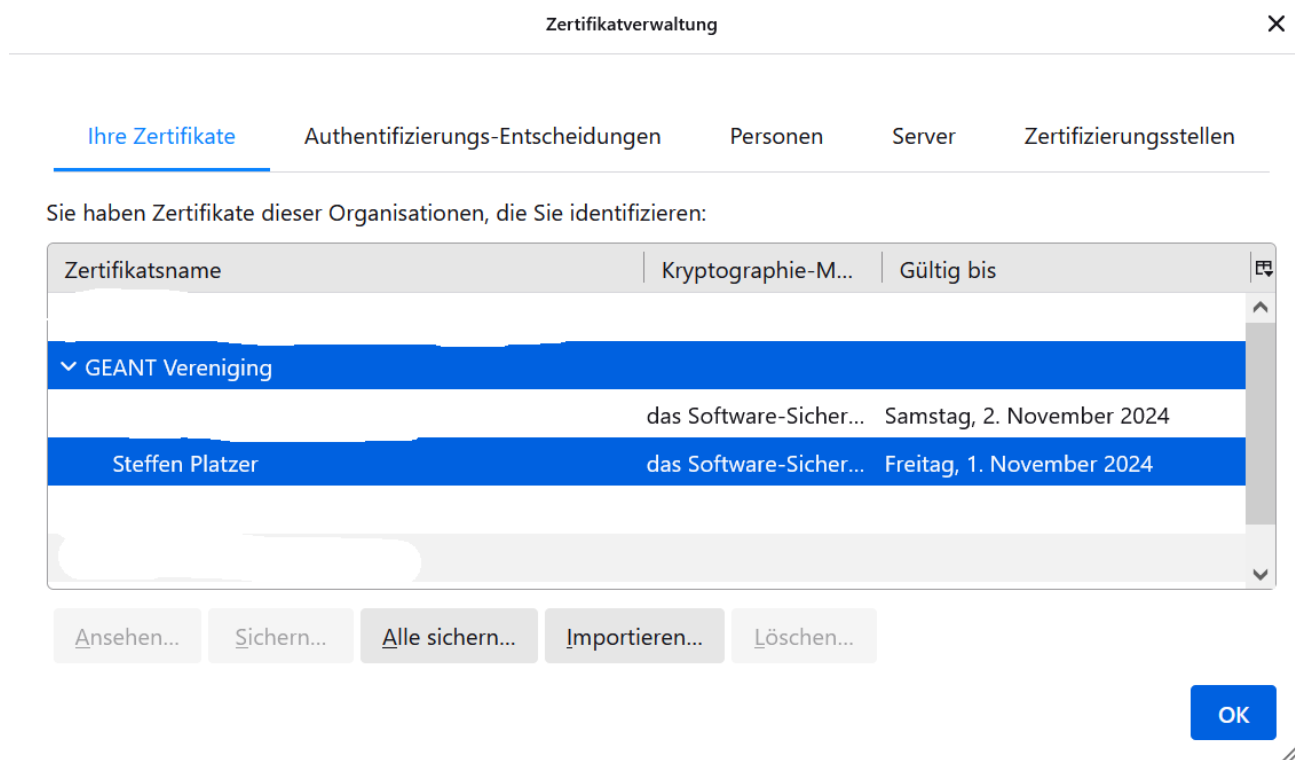
danach werden Sie aufgefordert Ihre Passwort einzugeben welches sie beim Erstellen ihrer Zertifikatsdatei vergeben haben



Nach korrekter Eingabe erscheint folgende Meldung.



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



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.

[Mehr über Verschlüsselung und Standard-Einstellungen erfahren](#)

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]**

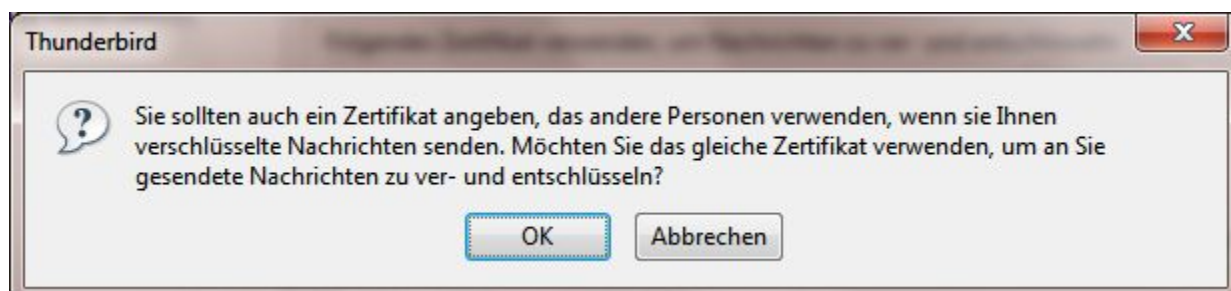
Details des ausgewählten Zertifikats:

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 ihre Empfänger und diese können es direkt für die verschlüsselte Kommunikation mit ihnen benutzen.

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

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

[Hinweise zum Haupt-/Masterpasswort](#)

[Zertifikat Backup anlegen](#)