



Installation und Verwendung Ihres persönlichen Nutzerzertifikates in 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 über die Ihnen zugesandte URL als Download gespeichert, z.B. "\\Eigene Dateien\single.p12")

Sie haben die PIN (Sicherungs-PIN / Passwort, das zur Verschlüsselung dieses Zertifikatbackups verwendet wurde) für den Import Ihres persönlichen Softzertifikates während des Videoidentverfahrens bekommen.

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' (Account Settings) window in Thunderbird. The left sidebar is expanded to show the 'Ende-zu-Ende-Verschlüsselung' (End-to-End Encryption) settings for the account 'steffen.platzer@cms.hu-berlin.de'. The main content area is titled 'Ende-zu-Ende-Verschlüsselung' and contains the following text:

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"

The screenshot shows the 'Zertifikatsverwaltung' (Certificate Management) window. The 'Ihre Zertifikate' (My Certificates) tab is selected and highlighted with a red box. The window title is 'Zertifikatsverwaltung' and it has a close button (X) in the top right corner.

The tabs are: **Ihre Zertifikate**, Authentifizierungs-Entscheidungen, Personen, Server, Zertifizierungsstellen.

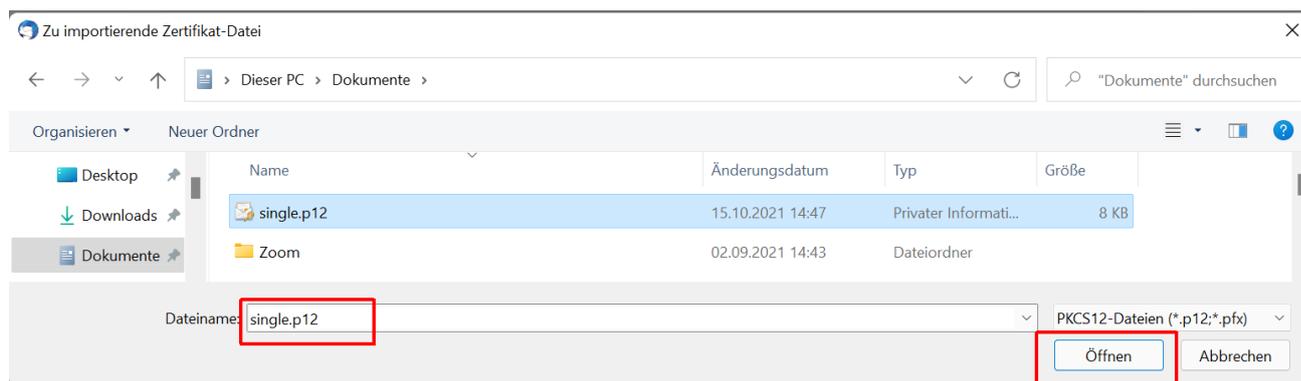
Sie haben Zertifikate dieser Organisationen, die Sie identifizieren:

| Zertifikatsname | Kryptographie-M... | Gültig bis |
|-----------------|--------------------|------------|
| [Redacted] | [Redacted] | [Redacted] |
| [Redacted] | [Redacted] | [Redacted] |

Buttons at the bottom: [Ansehen...](#) [Sichern...](#) [Alle sichern...](#) [Importieren...](#) [Löschen...](#)

[OK](#)

ein Fenster zum Importieren des persönlichen Nutzerzertifikates öffnet sich



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.

| Zertifikatsname | Kryptographie-... | Gültig bis |
|--|-------------------|------------|
| <ul style="list-style-type: none"> <ul style="list-style-type: none"> Steffen Platzer das Software-Sich... Montag, 2. Dezember 2024 Steffen Platzer das Software-Sich... Samstag, 8. Juni 2024 Steffen Platzer das Software-Sich... Montag, 16. Januar 2023 Steffen Platzer das Software-Sich... Sonntag, 18. Dezember 2022 Steffen Platzer das Software-Sich... Samstag, 4. Januar 2020 | | |

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](#)

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

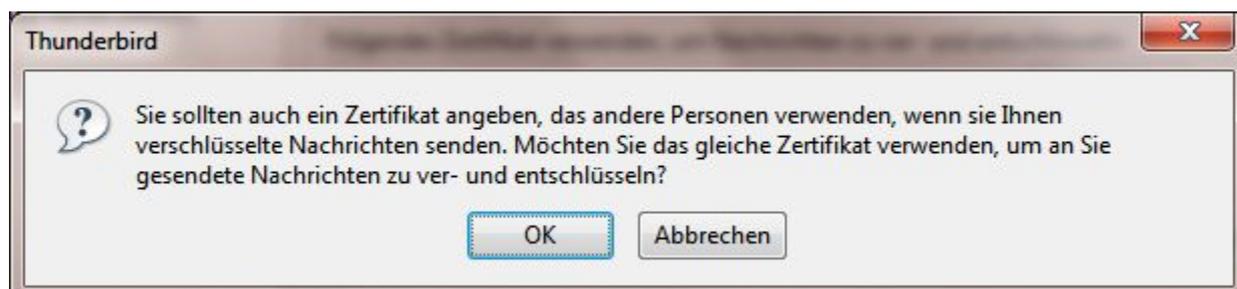
E-Mail: steffen.platzer@cms.hu-berlin.de

Ausgestellt von: CN=GEANT Personal CA 4,O=GEANT Vereniging,C=NL

Gespeichert in: das Software-Sicherheitsmodul

OK

Abbrechen



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. Die ausgestellten Zertifikate werden nicht mehr über das HU-Adressbuch (ldap.hu-berlin.de) für ihre Kommunikationspartner zur Verfügung gestellt. 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](#)