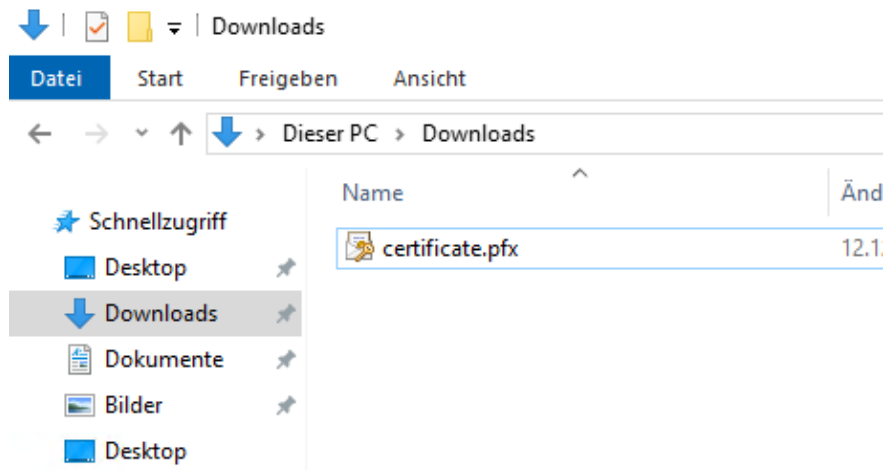
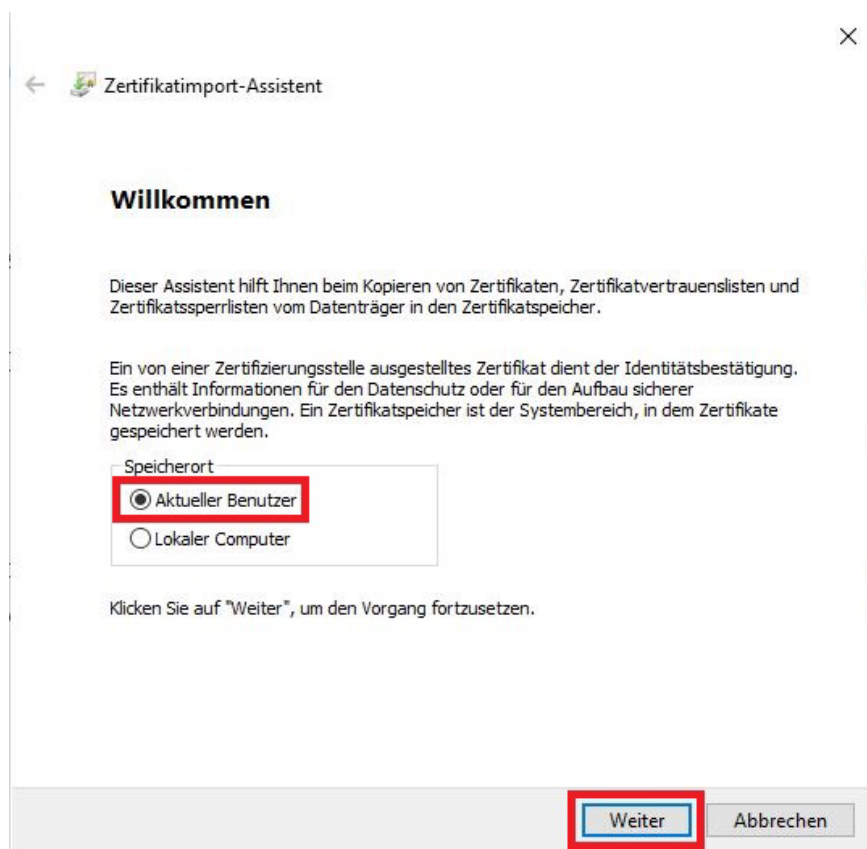


Persönliches Nutzerzertifikat installieren- Windows


1. Das Zertifikat wird standardmäßig im Download-Verzeichnis gespeichert. Öffnen Sie die .pfx-Datei mit einem Doppelklick.



2. Windows erkennt die Zertifikatsdatei und öffnet den Zertifikatimport-Assistent. Wählen Sie als Speicherort „Aktueller Benutzer“. Klicken Sie auf „Weiter“.



3. Dann wiederum Klick auf „Weiter“.

 Zertifikatimport-Assistent

Zu importierende Datei

Geben Sie die Datei an, die importiert werden soll.

Dateiname:

C:\Users\m.mustermann\Downloads\certificate.pfx

Durchsuchen...

Hinweis: Mehrere Zertifikate können in einer Datei in folgenden Formaten gespeichert werden:

Privater Informationsaustausch - PKCS #12 (.PFX, .P12)

Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)

Microsoft Serieller Zertifikatspeicher (.SST)

Weiter

Abbrechen

4. Sie müssen nun noch einmal das Passwort eingeben, mit dem Sie die „.pfx-Zertifikatsdatei“ geschützt haben und Angaben zu den „Importoptionen“ machen. Klicken Sie nach der Auswahl auf „Weiter“.

Für die „Importoptionen“ empfehlen wir die folgenden Einstellungen:

- „Privaten Schlüssel mit virtualisierungsbasierter Sicherheit schützen (nicht exportierbar)“
- „Alle erweiterten Eigenschaften mit einbeziehen“

Zur Erläuterung:

- Wählt man in den Optionen „Hohe Sicherheit“ aus, muss man bei jedem Versenden einer signierten E-Mail das Kennwort eingeben.
- Das Anhängen von „Privaten Schlüssel mit virtualisierungsbasierter Sicherheit schützen ...“ ist die sicherste Einstellung, hat aber zur Folge, dass der private Schlüssel später nicht aus dem Zertifikatspeicher exportiert werden kann. Man muss stattdessen auf die originale Zertifikatsdatei zurückgreifen.

Speichern Sie also die Zertifikatsdatei „Dateiname.pfx“ an einem sicheren Ort (auch Ausfallsicherheit beachten) z.B. auf Ihrem persönlichen H: Laufwerk und sorgen Sie zusätzlich dafür, dass Sie auf das vergebene Kennwort im Bedarfsfall immer zugreifen können.

Achtung: Wenn sie verschlüsselte E-Mails empfangen, sollten Sie auch ältere Nutzerzertifikate aufbewahren, um auch später immer noch die entsprechenden E-Mails lesen zu können.

← Zertifikatimport-Assistent

Schutz für den privaten Schlüssel

Der private Schlüssel wurde mit einem Kennwort geschützt, um die Sicherheit zu gewährleisten.

Geben Sie das Kennwort für den privaten Schlüssel ein.

Kennwort:

.....

Kennwort anzeigen

Importoptionen:

Hohe Sicherheit für den privaten Schlüssel aktivieren. Wenn Sie diese Option aktivieren, werden Sie immer dann, wenn der private Schlüssel von einer Anwendung verwendet wird, zur Kennworteingabe aufgefordert.

Schlüssel als exportierbar markieren. Dadurch können Sie Ihre Schlüssel zu einem späteren Zeitpunkt sichern bzw. überführen.

Privaten Schlüssel mit virtualisierungsbasierter Sicherheit schützen (nicht exportierbar)

Alle erweiterten Eigenschaften mit einbeziehen

Weiter Abbrechen

5. Bei der Angabe zum Speicherort für die Zertifikate belassen Sie die empfohlene Einstellung. Klicken Sie auf „Weiter“ und dann auf „Fertig stellen“. Im Anschluss wird Ihnen der erfolgreiche Import bestätigt.

