Kraftfahrt-
Bundesamt

Anleitung für den Import von TLS-Clientzertifikaten

Stand: Januar 2022

Anleitung für den Import von TLS-Clientzertifikaten

Inhaltsverzeichnis:

1 Einleitung

Das Kraftfahrt-Bundesamt stellt über den Server portal.kba.doi-de.net das **Ze**ntrale **V**erkehrs-**I**nformations-**S**ystem (ZEVIS) bereit, mit dem Abfragen der Register des Amtes durchgeführt und Mitteilungen an die Register gesendet werden können.

Für den Zugriff über das NdB-VN (vormals DOI-Netz) werden TLS-Clientzertifikate genutzt.
Diese werden bei dem Zugriff auf die Dialoganwendungen des Kraftfahrt-Bundesamtes auf dem PC installiert.
Beim Zugriff von Verfahrenssoftware auf die Webservices des Amtes wird diese i. d. R. auf Application Servern installiert.

Die folgende Anleitung beschreibt die notwendigen Schritte zum Import der TLS-Client-Zertifikate in verschiedene Browser unter Windows 10 und 11 für den Zugriff auf die Dialoganwendungen von ZEVIS. Unter Windows 7 und 8 kann der Import geringfügig abweichen.

Nicht beschrieben ist der Import der TLS-Clientzertifikate in Application Server und Verfahrenssoftware. Diesbezügliche Informationen erhalten Sie aus der Dokumentation oder direkt beim Hersteller Ihrer Verfahrenssoftware.

Der Import der Client-Zertifikate auf LINUX-Systeme ist ebenfalls nicht beschrieben.
Der Import in den Browser Firefox ist nach aktueller Kenntnis auf einem LINUX-Derivat vergleichbar mit dem beschriebenen Import bei Firefox unter Windows.

Vor dem Import der Datei müssen die P12-Datei und das Passwort für den Import vorliegen.

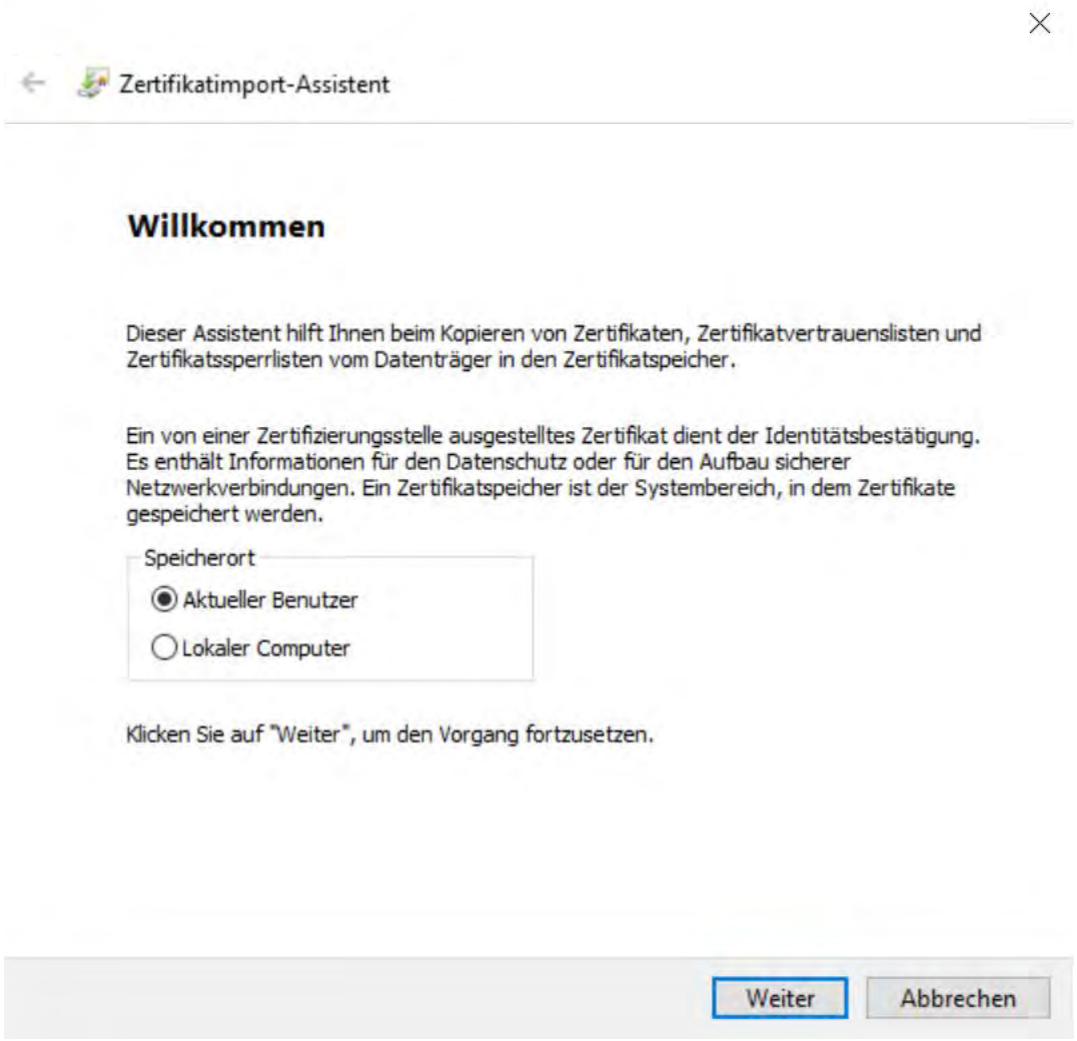
2 Import der TLS-Zertifikate in den Windows Zertifikatsspeicher -schnellere Variante ohne Überprüfung (für die Browser Chrome und Opera)

Die Browser Google Chrome und Opera nutzen für die Speicherung der Zertifikate den Windows-Zertifikatsspeicher. Daher ist das Vorgehen bei diesen Browsern gleich.

2.1 Doppelklick auf die übermittelte P12-Datei

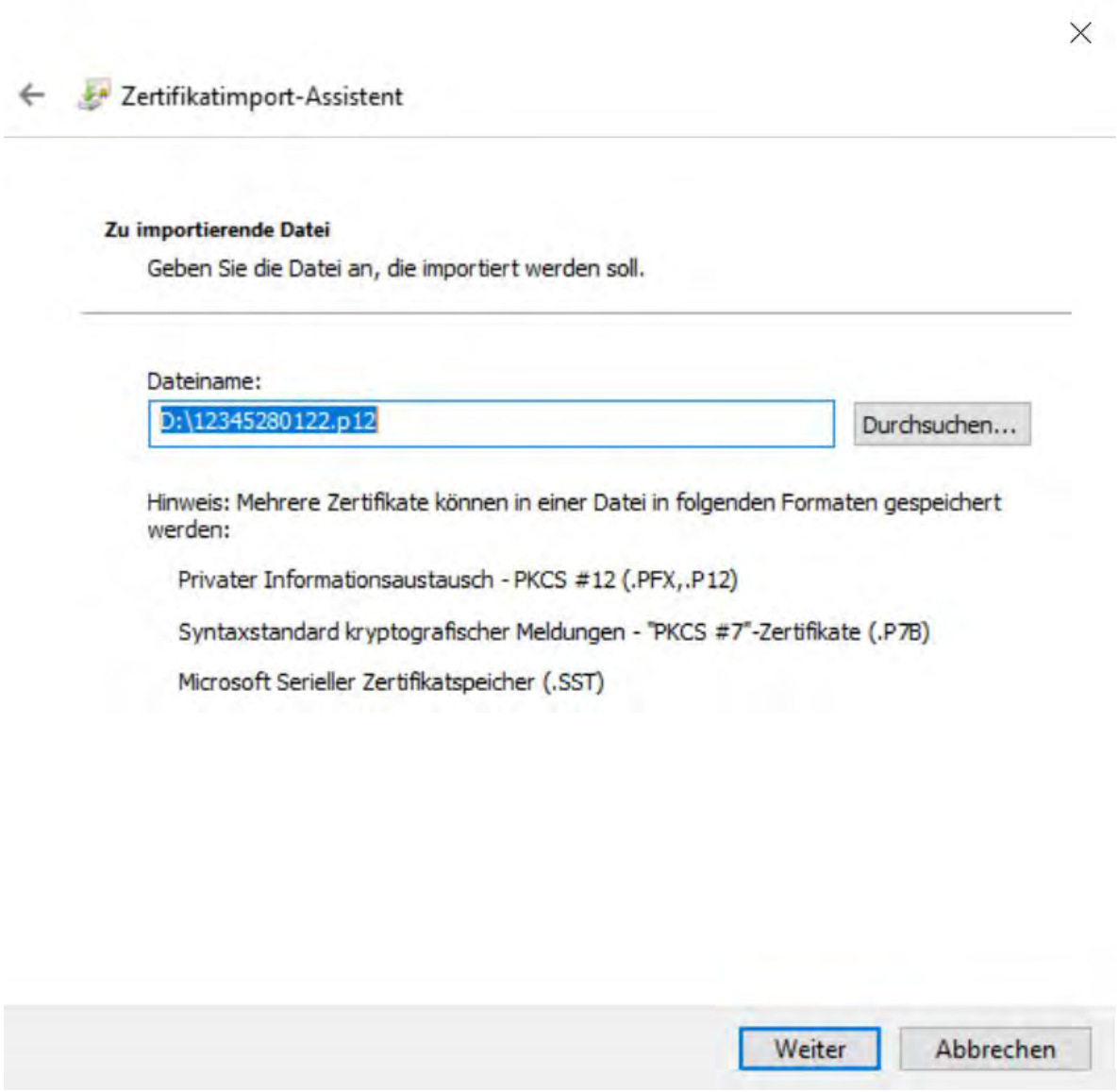
Bitte führen Sie einen Doppelklick auf die vom KBA übermittelte P12-Datei aus.

Im folgenden Fenster belassen Sie bitte die Auswahl auf „Aktueller Benutzer“ und klicken Sie auf „Weiter“.

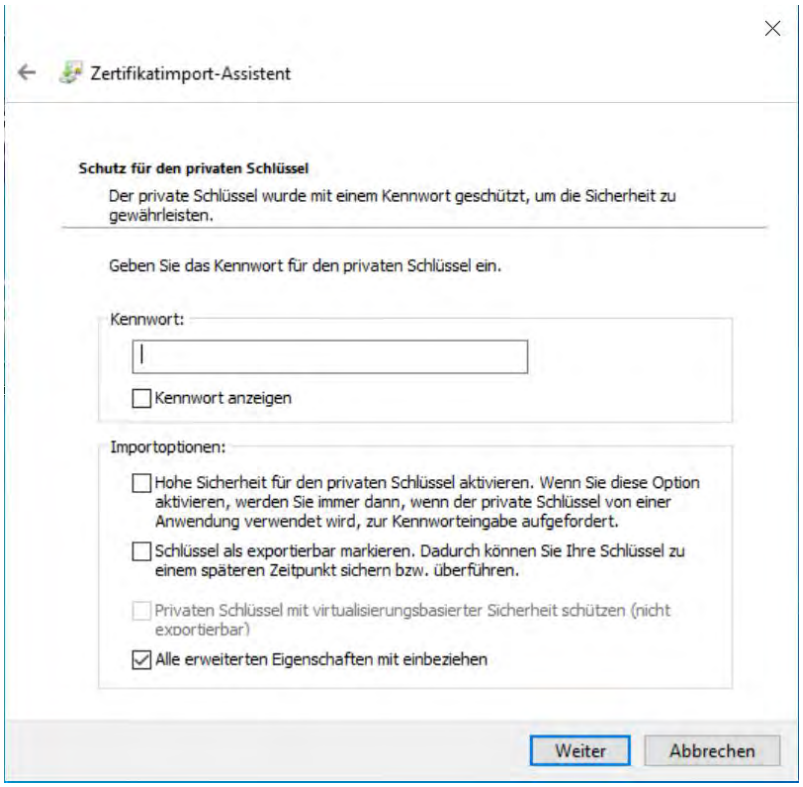


2.2 Doppelklick auf die übermittelte P12-Datei

Beim nächsten Fenster klicken Sie bitte auf „Weiter“.



2.3 Eingabe des Passworts



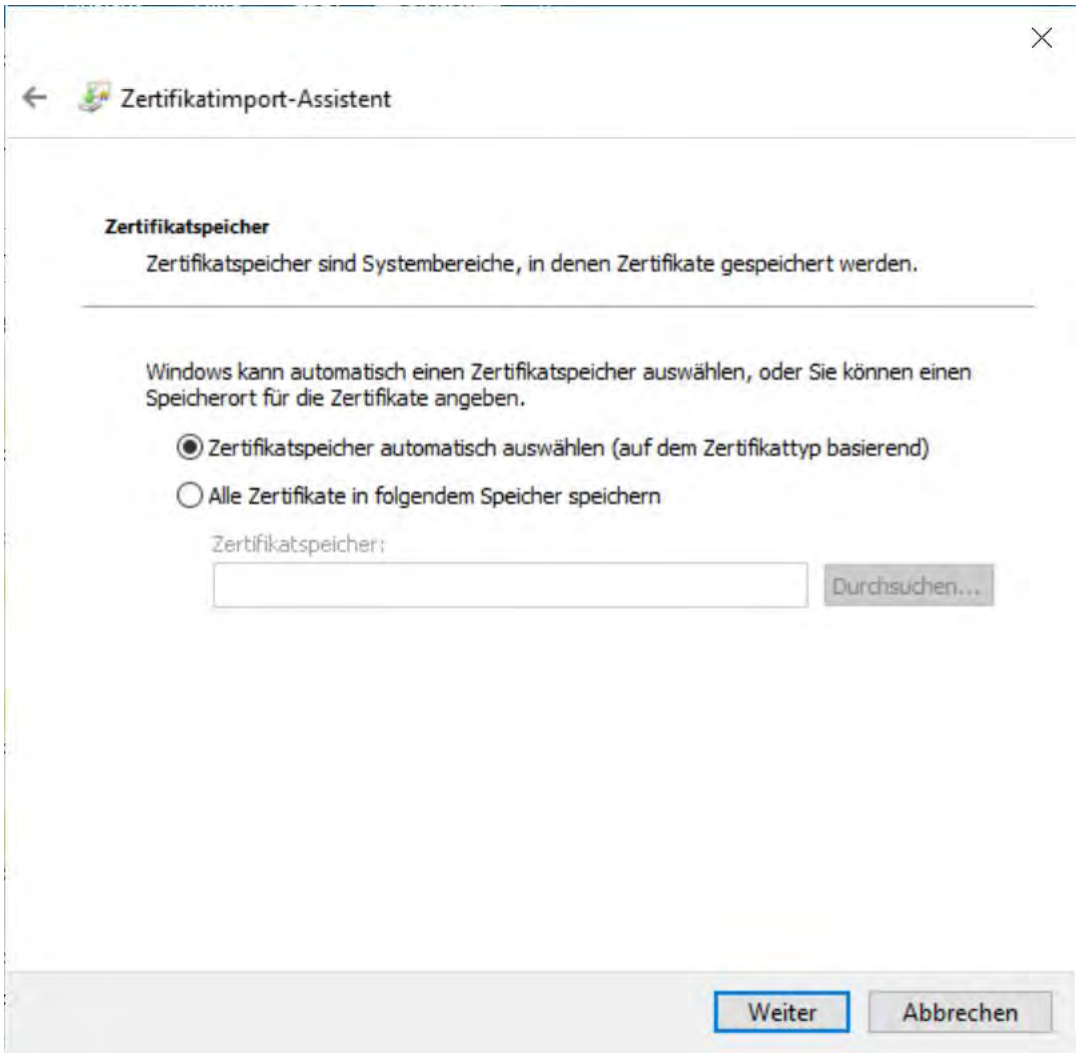
Das Passwort für den Import wird in der Regel per Briefpost an den Leiter der IT der beantragenden Behörde versandt. Dieses Passwort wird beim Kraftfahrt-Bundesamt nicht gespeichert, daher verwahren Sie den Passwortbrief sorgfältig.
Ist das Import-Passwort verloren gegangen, wenden Sie sich bitte an die Anwenderbetreuung des Kraftfahrt-Bundesamtes.

Die Option „Schlüssel als exportierbar markieren“ sollte aus Sicherheitsgründen nicht ausgewählt werden.

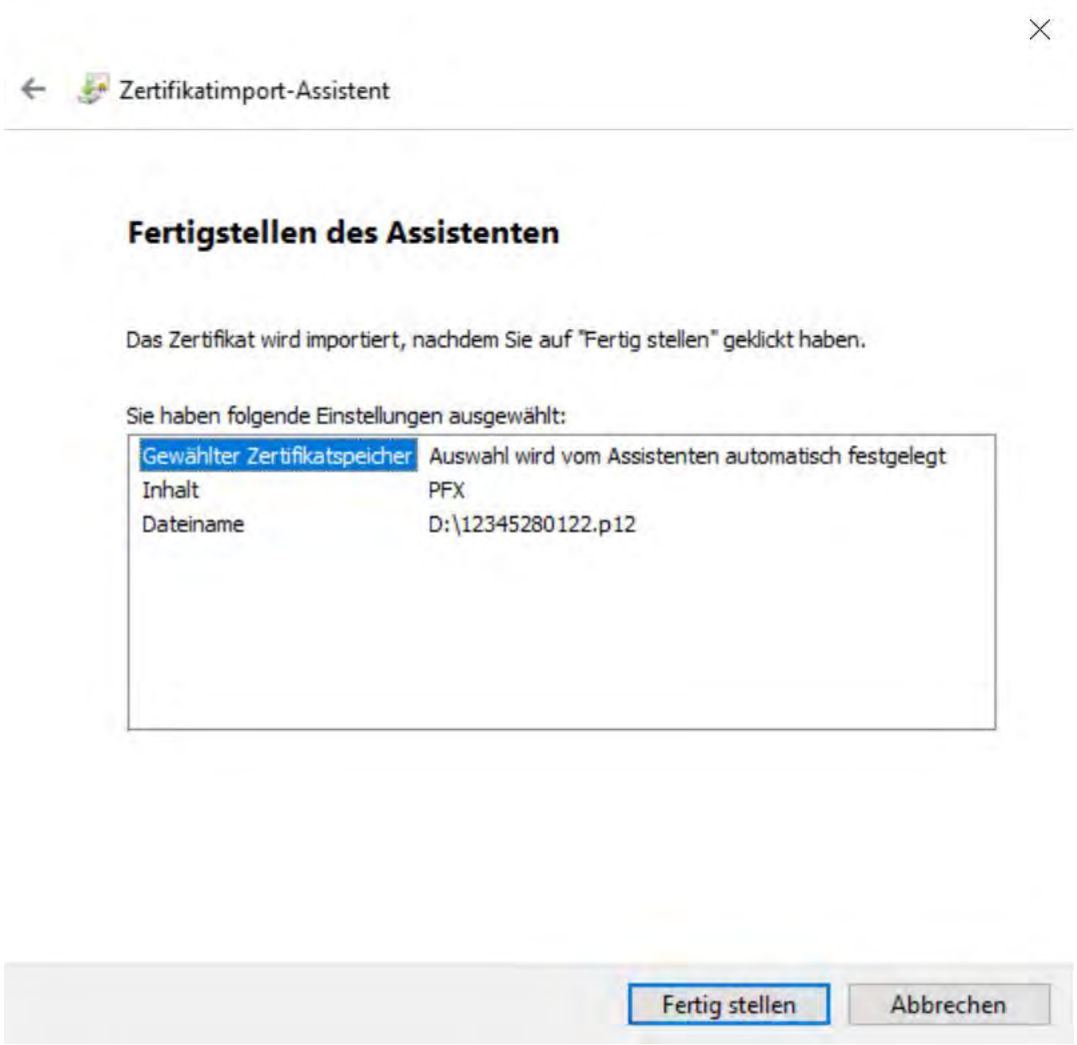
Die Option „Hohe Sicherheit für den privaten Schlüssel aktivieren“ sollte ebenfalls nicht aktiviert werden, da in diesem Fall bei jedem Zugriff das Importpasswort erneut eingegeben werden muss.

2.4 Zertifikatsspeicher auswählen.

Beim nächsten Fenster belassen Sie die Auswahl bitte auf „Zertifikatsspeicher automatisch auswählen“ und klicken Sie bitte auf „Weiter“.



2.5 … und Fertigstellen



2.6 Bestätigen des Imports des Root-Zertifikats

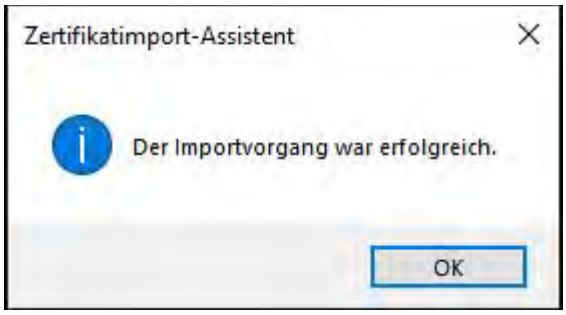
Bei dem Import des Root-Zertifikats werden Sie zur Sicherheit zusätzlich aufgefordert, den Fingerprint des Root-Zertifikats zu überprüfen.
Der Fingerprint des Root-Zertifikats ist

```
0d85 600b 7706 70ce 4e1f 486e fcf4 9b97 b5c3 0d6b
```

Bitte prüfen sie den Fingerprint und drücken Sie bei Übereinstimmung auf „JA“

Haben Sie bei der Auswahl des Zertifikatsspeichers nicht „automatisch auswählen“ gewählt, erfolgt diese Abfrage nicht. In diesen Fällen werden die Zertifikate „ca-kba“ und „SSL-Client2016“ in den Zertifikatsspeicher „Eigene Zertifikate“ importiert. Das Zertifikat „ca-kba“ muss in diesem Fall anschließend per Drag and Drop in den Bereich „Vertrauenswürdige Stammzertifizierungsstellen/Zertifikate“ und das Zertifikat „SSL-Client2016“ in den Bereich „Zwischenzertifizierungsstellen“ verschoben werden.

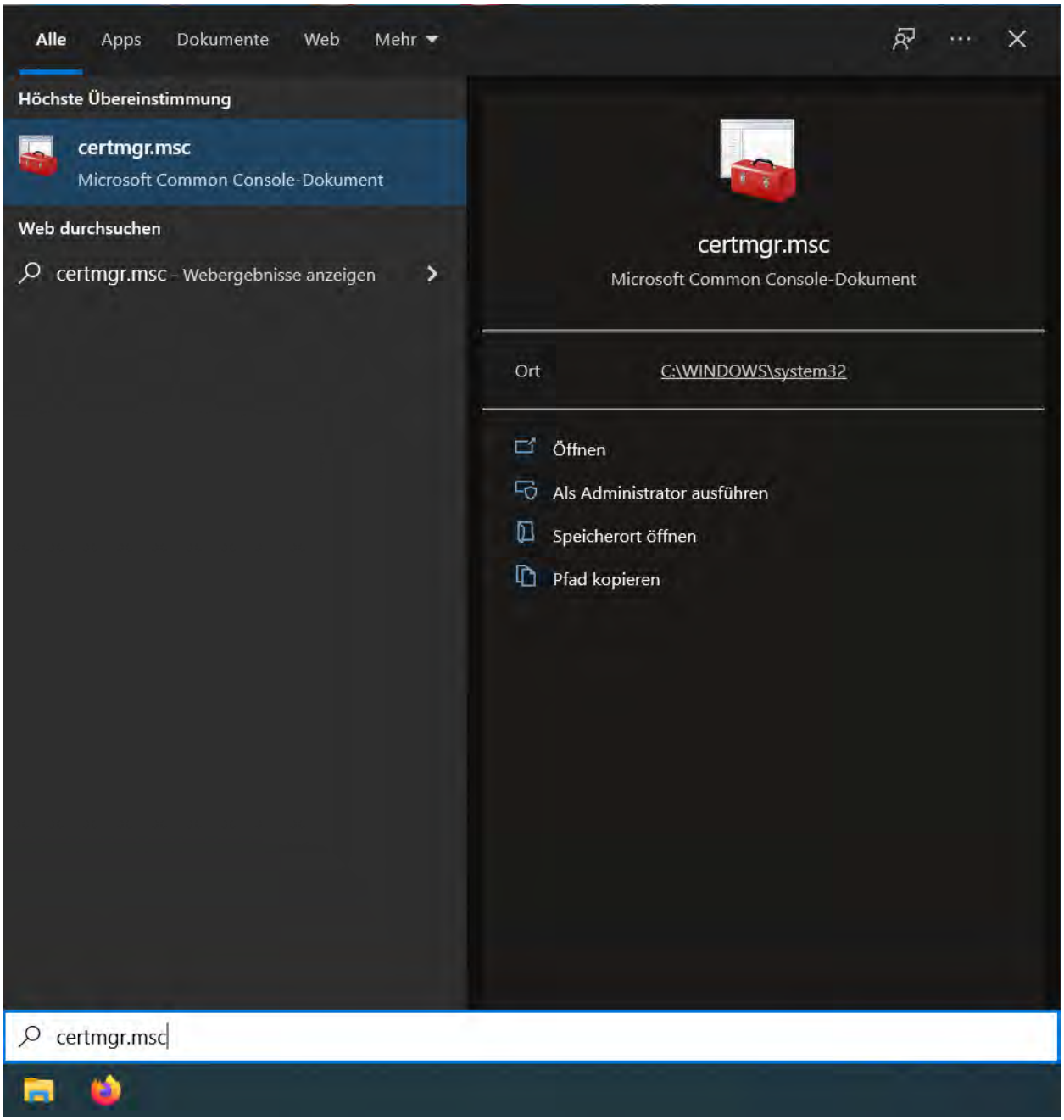
2.7 Bestätigen der Bestätigungsmeldung.

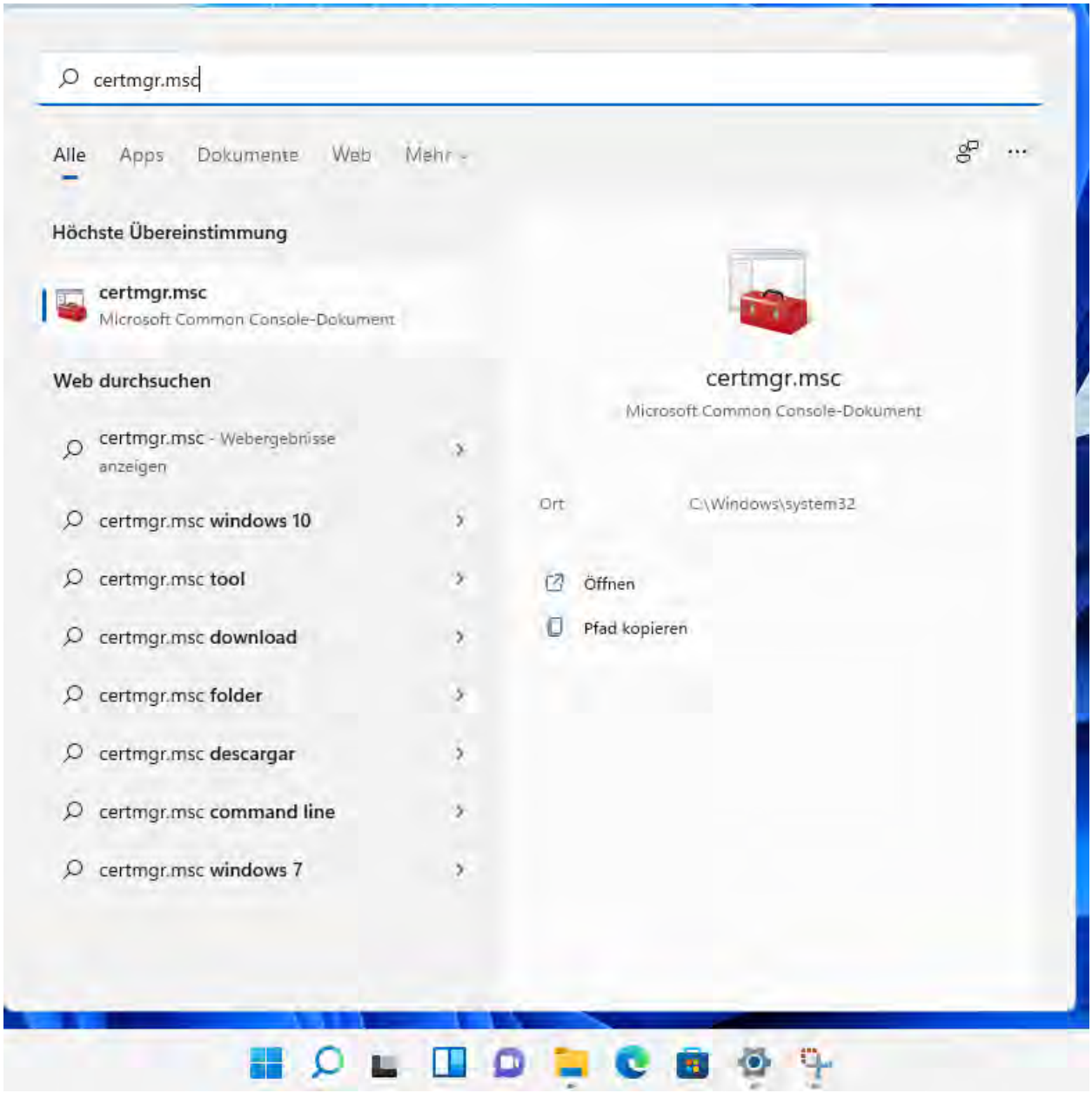


3 Import der TLS-Zertifikate in den Windows Zertifikatsspeicher -Variante mit Überprüfungsmöglichkeit (für die Browser Chrome und Opera)

Die Browser Google Chrome und Opera nutzen für die Speicherung der Zertifikate den Windows-Zertifikatsspeicher. Daher ist das Vorgehen bei beiden Browsern gleich.

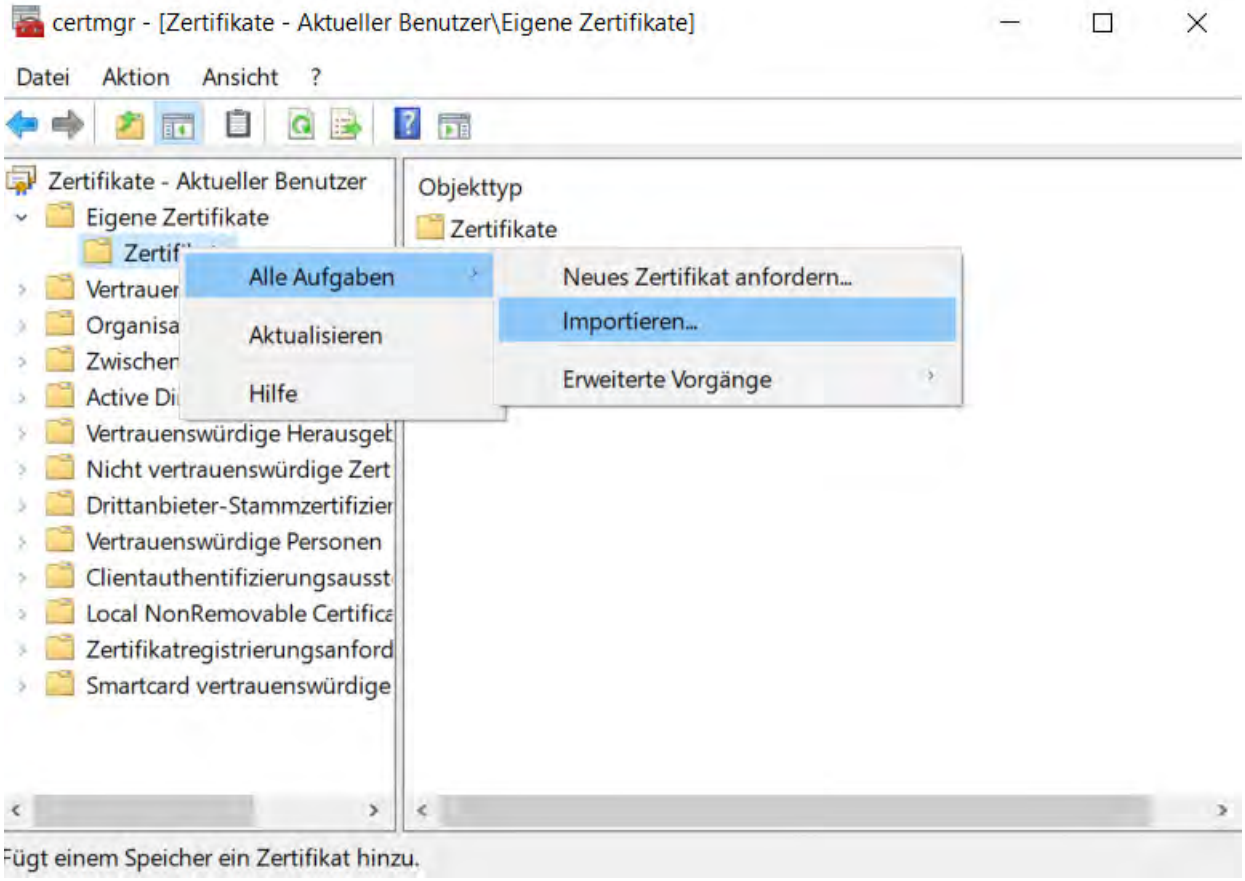
3.1 Öffnen des Zertifikatsmanagers durch Drücken der Windows-Taste und Eingabe der Zeichenfolge „certmgr.msc“



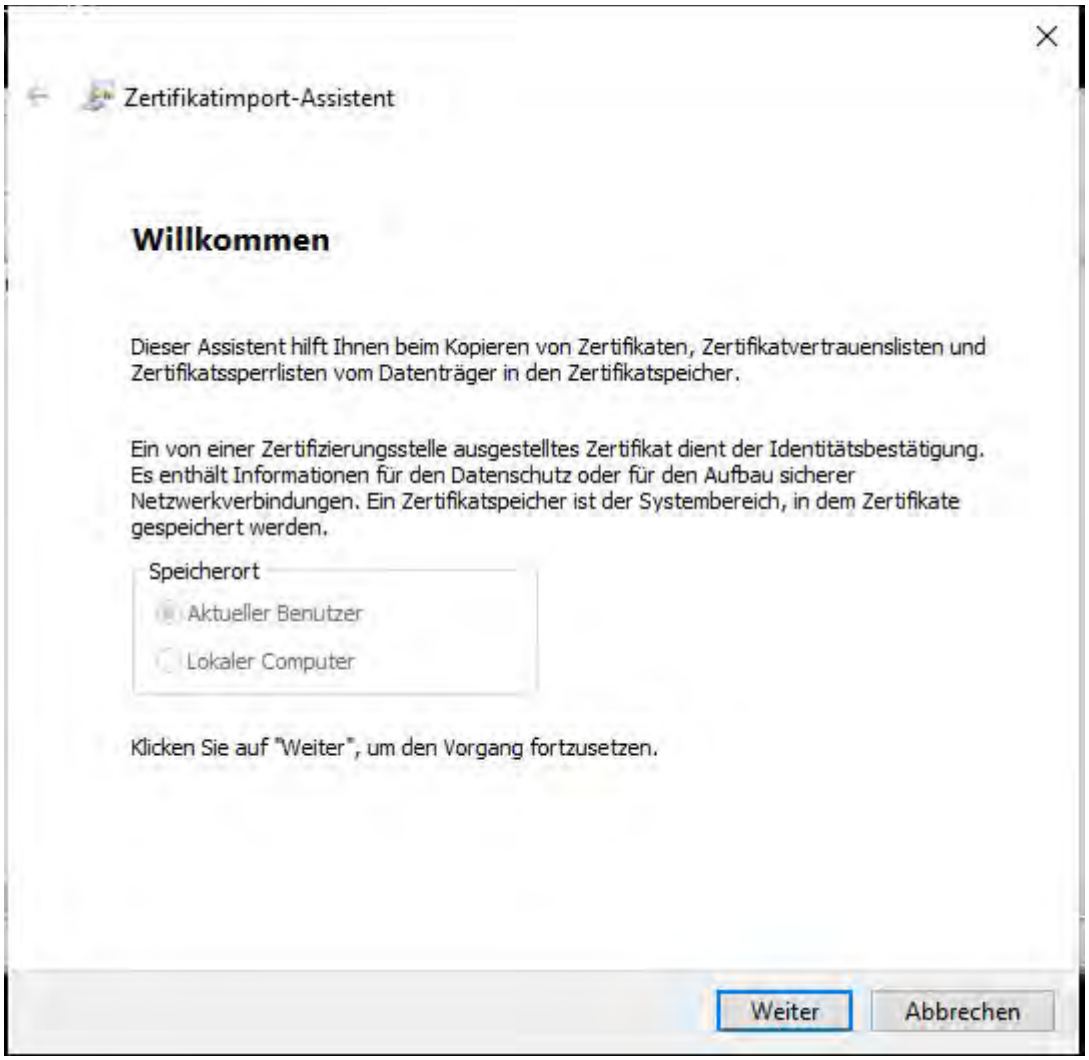

certmgr.msc
Alle
Apps
Dokumente
Web
Mehr
Höchste Übereinstimmung
certmgr.msc
Microsoft Common Console-Dokument
Web durchsuchen
certmgr.msc - Webergebnisse anzeigen
certmgr.msc windows 10
certmgr.msc tool
certmgr.msc download
certmgr.msc folder
certmgr.msc descargar
certmgr.msc command line
certmgr.msc windows 7
certmgr.msc
Microsoft Common Console-Dokument
Ort
C:\Windows\system32
Öffnen
Pfad kopieren

3.2 Starten des Import-Assistenten

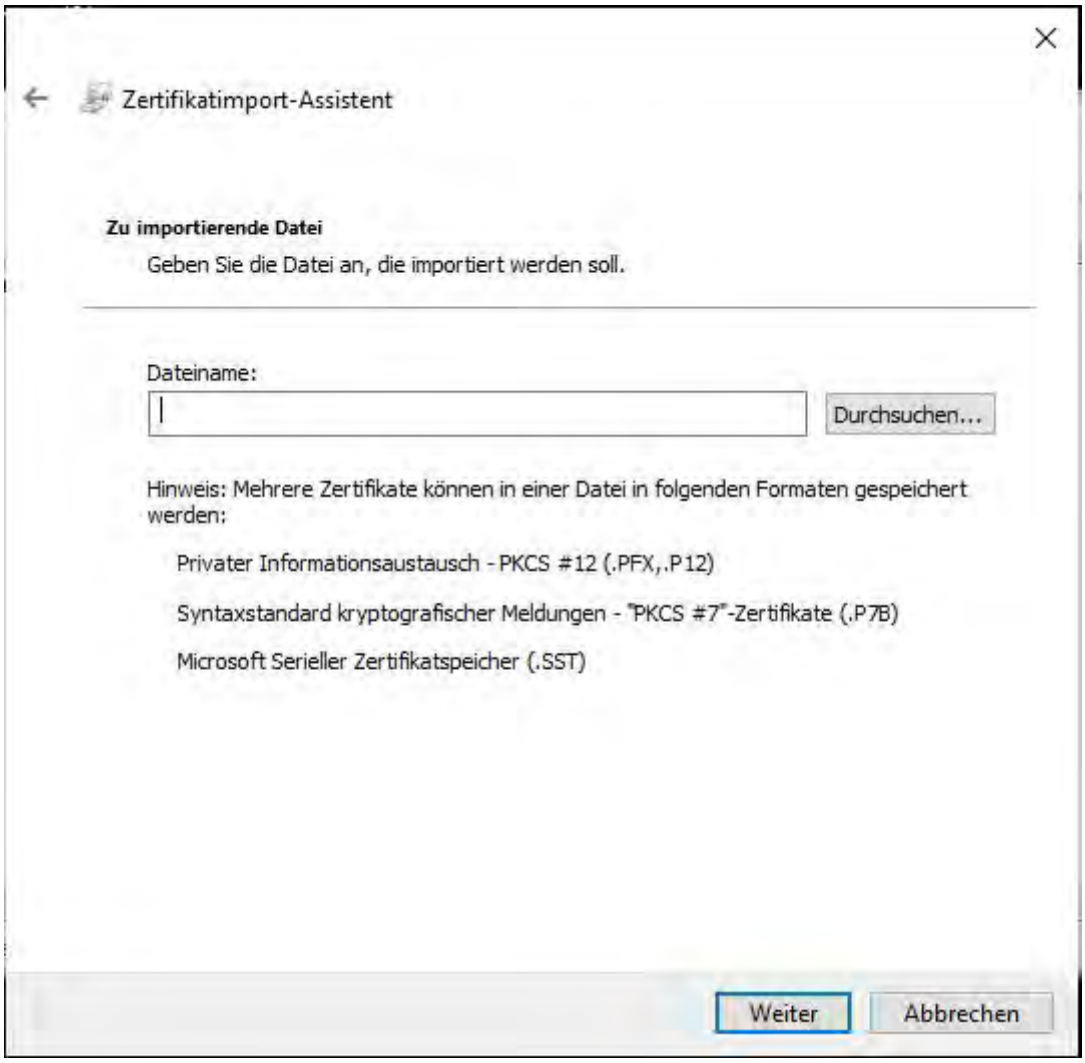
Sie können den Import-Assistenten über einen Rechtsklick auf „Eigene Zertifikate“ – „Alle Aufgaben“ – „Importieren“ oder nach einem Klick auf „Eigene Zertifikate“ – „Aktion“ – „Alle Aufgaben“ – „Importieren“ starten.



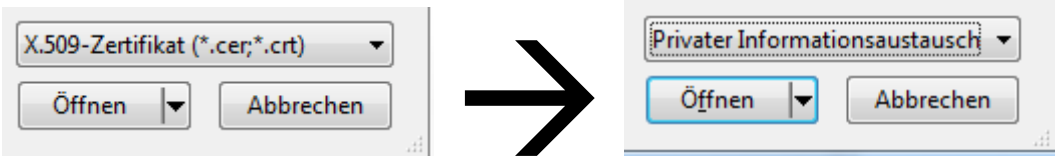
3.3 Startbildschirm



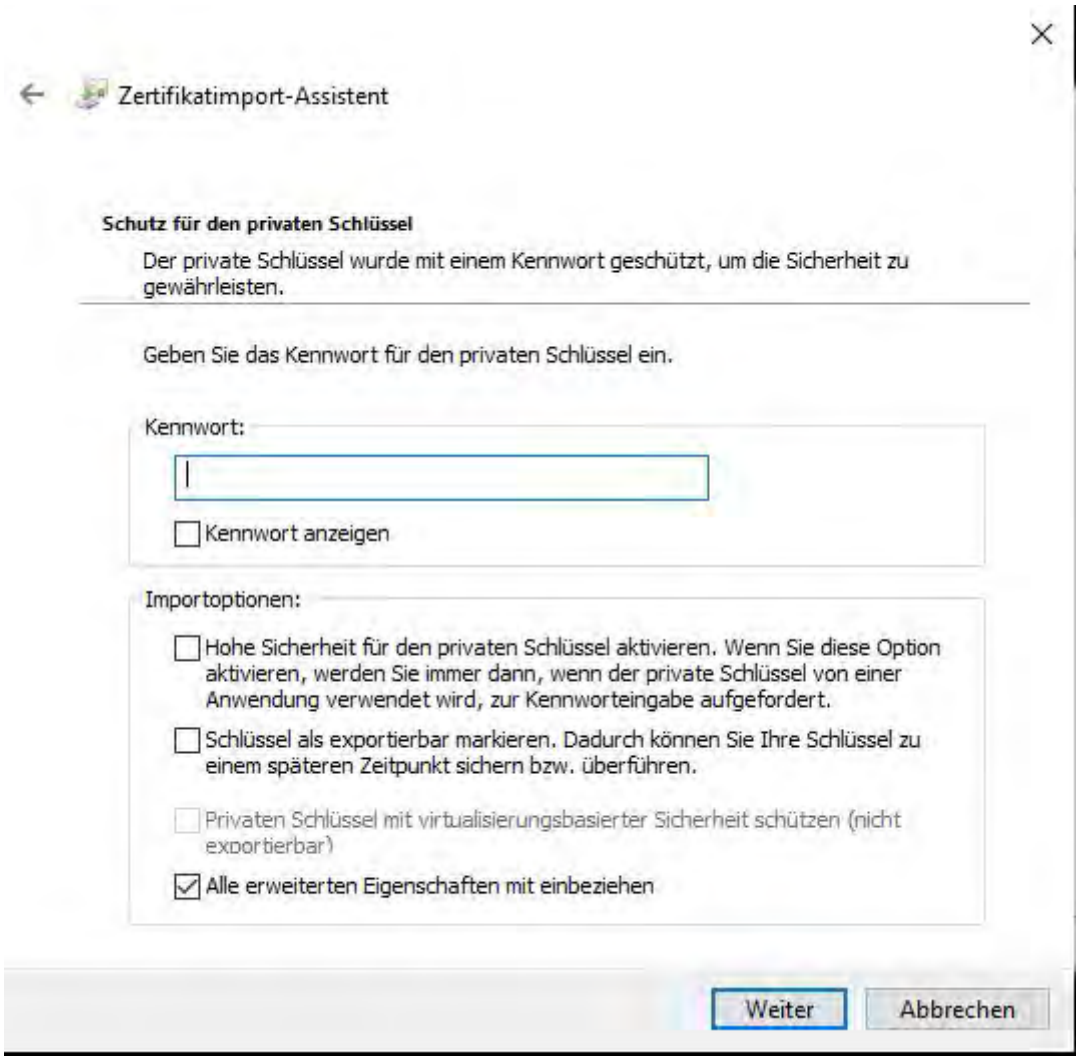
3.4 Im nächsten Dialogfeld ist die vom KBA übersandte P12-Datei auszuwählen.



Ggf. werden bei einem Klick auf Durchsuchen nur Zertifikate (*.cer, *.crt) angezeigt. In diesem Fall muss zunächst das Feld über „Öffnen“ auf „Privater Informations-austausch (PFX / P12)“ umgestellt werden.



3.5 Eingabe des Passworts für den Import



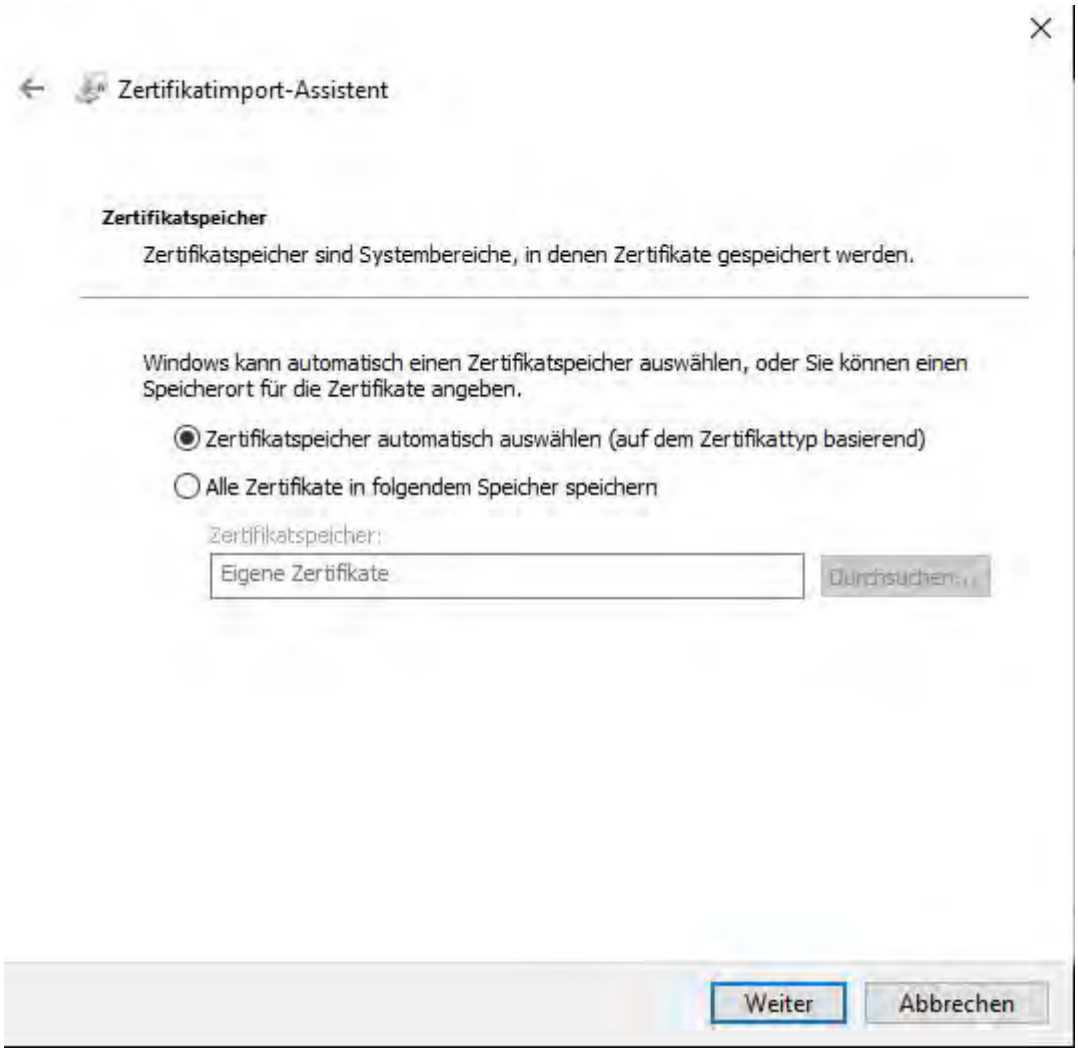
Das Passwort für den Import wird in der Regel per Briefpost an den Leiter der IT der beantragenden Behörde versandt.

Dieses Passwort wird beim Kraftfahrt-Bundesamt nicht gespeichert, daher verwahren Sie den Passwortbrief sorgfältig.
Ist das Import-Passwort verloren gegangen, wenden Sie sich bitte an die Anwenderbetreuung des Kraftfahrt-Bundesamtes.

Die Option „Schlüssel als exportierbar markieren“ sollte aus Sicherheitsgründen nicht ausgewählt werden.

Die Option „Hohe Sicherheit für den privaten Schlüssel aktivieren“ sollte ebenfalls nicht aktiviert werden, da in diesem Fall bei jedem Zugriff das Importpasswort erneut eingegeben werden muss.

3.6 Zertifikatsspeicher auswählen.



Der Zertifikatsspeicher kann i. d. R. automatisch ausgewählt werden.

Sollte das Zertifikat allerdings anschließend nicht unter „Eigene Zertifikate“ – „Zertifikate“ angezeigt werden, sollte bei diesem Schritt als Zertifikatsspeicher „Eigene Zertifikate“ ausgewählt werden.

3.7 Einstellungen überprüfen und Fertig stellen.

3.8 Bestätigen des Imports des Root-Zertifikats

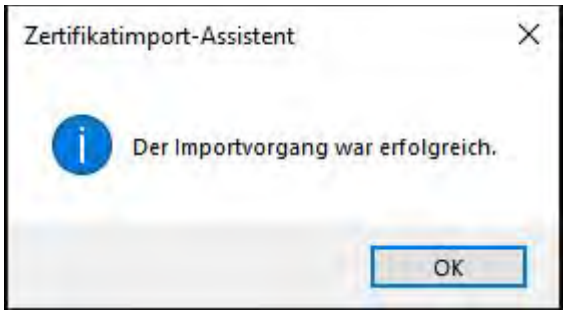
Bei dem Import des Root-Zertifikats werden Sie zur Sicherheit zusätzlich aufgefordert, den Fingerprint des Root-Zertifikats zu überprüfen.
Der Fingerprint des Root-Zertifikats ist

```
0d85 600b 7706 70ce 4e1f 486e fcf4 9b97 b5c3 0d6b
```

Bitte prüfen sie den Fingerprint und drücken Sie bei Übereinstimmung auf „JA“

Haben Sie bei der Auswahl des Zertifikatsspeichers nicht „automatisch auswählen“ gewählt, erfolgt diese Abfrage nicht. In diesen Fällen werden die Zertifikate „ca-kba“ und „SSL-Client2016“ in den Zertifikatsspeicher „Eigene Zertifikate“ importiert. Das Zertifikat „ca-kba“ muss in diesem Fall anschließend per Drag and Drop in den Bereich „Vertrauenswürdige Stammzertifizierungsstellen/Zertifikate“ und das Zertifikat „SSL-Client2016“ in den Bereich „Zwischenzertifizierungsstellen“ verschoben werden.

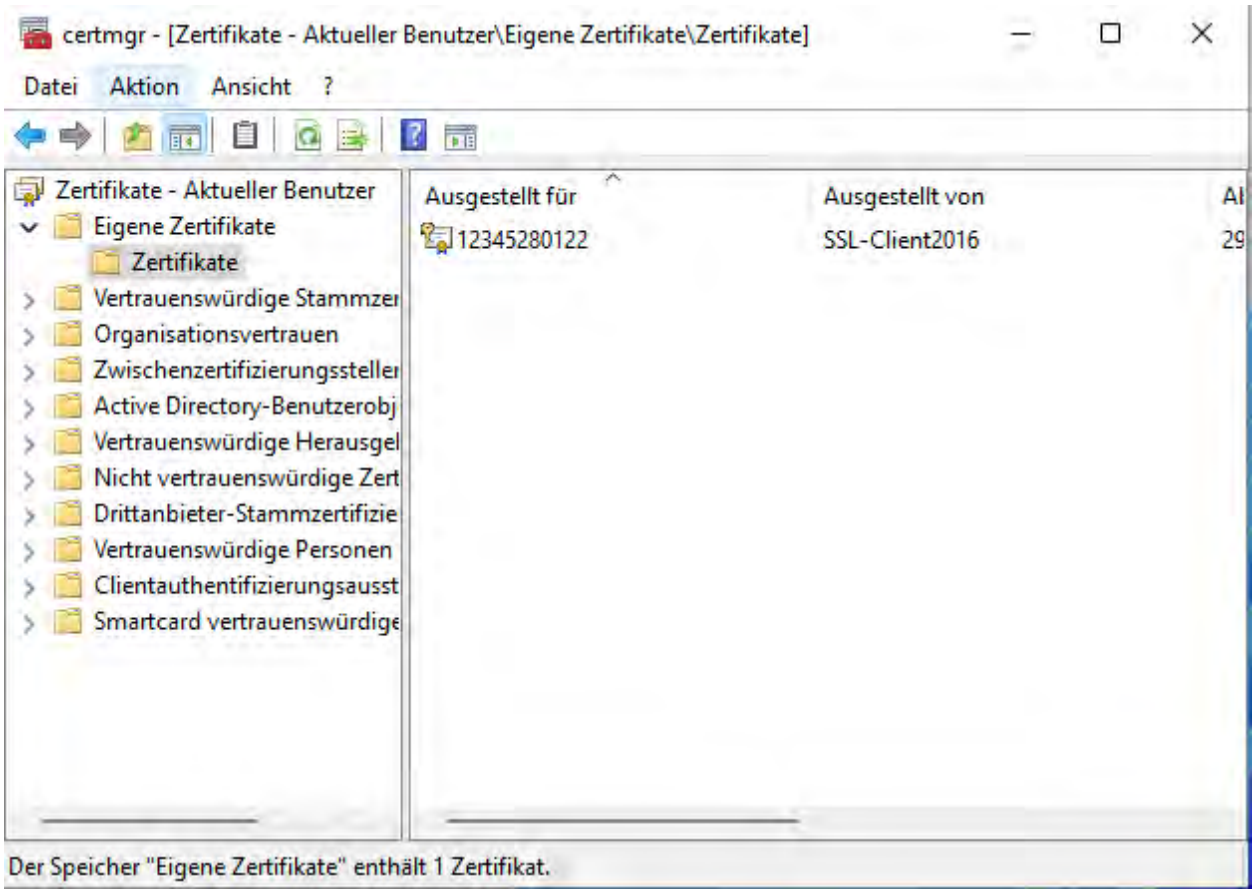
3.9 Bestätigen der Bestätigungsmeldung.



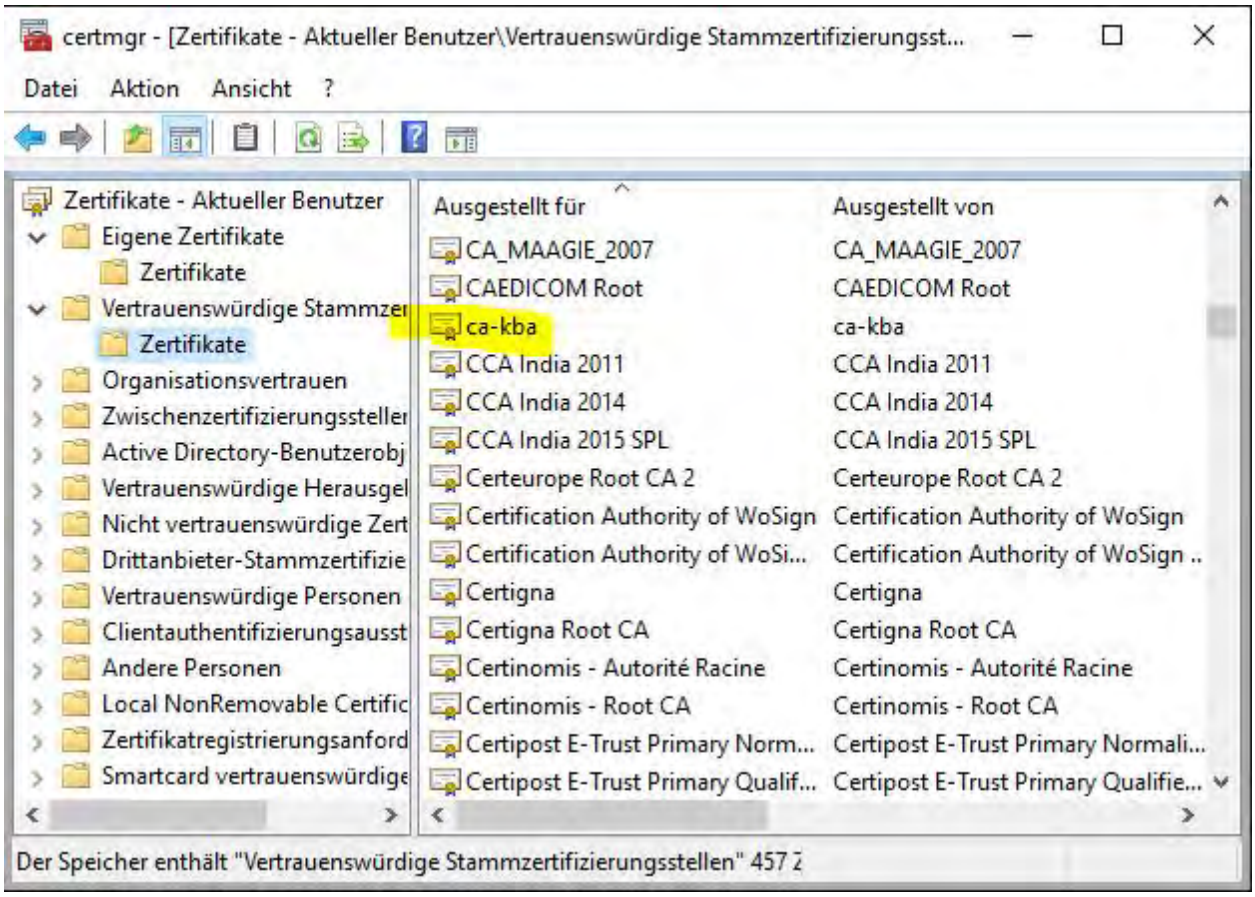
3.10 Überprüfen

Bitte schließen Sie nach dem Import den Zertifikatsmanager und starten Sie ihn erneut.

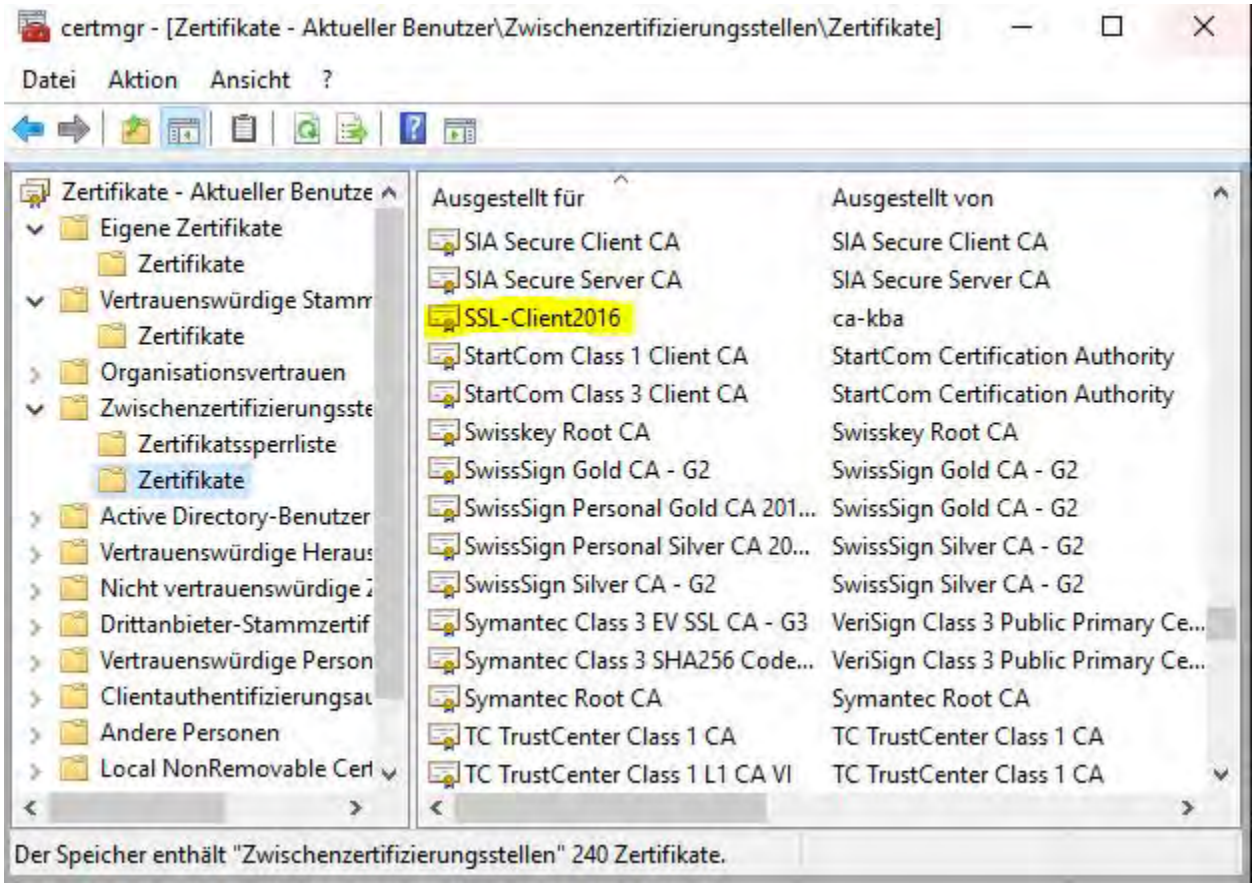
Unter „Eigene Zertifikate“ – „Zertifikate“ sollte nun das importierte Zertifikat aufgeführt werden.



Unter „Vertrauenswürdige Stammzertifizierungsstellen“ – „Zertifikate“ sollte nun das Zertifikat „ca-kba“ aufgeführt werden.

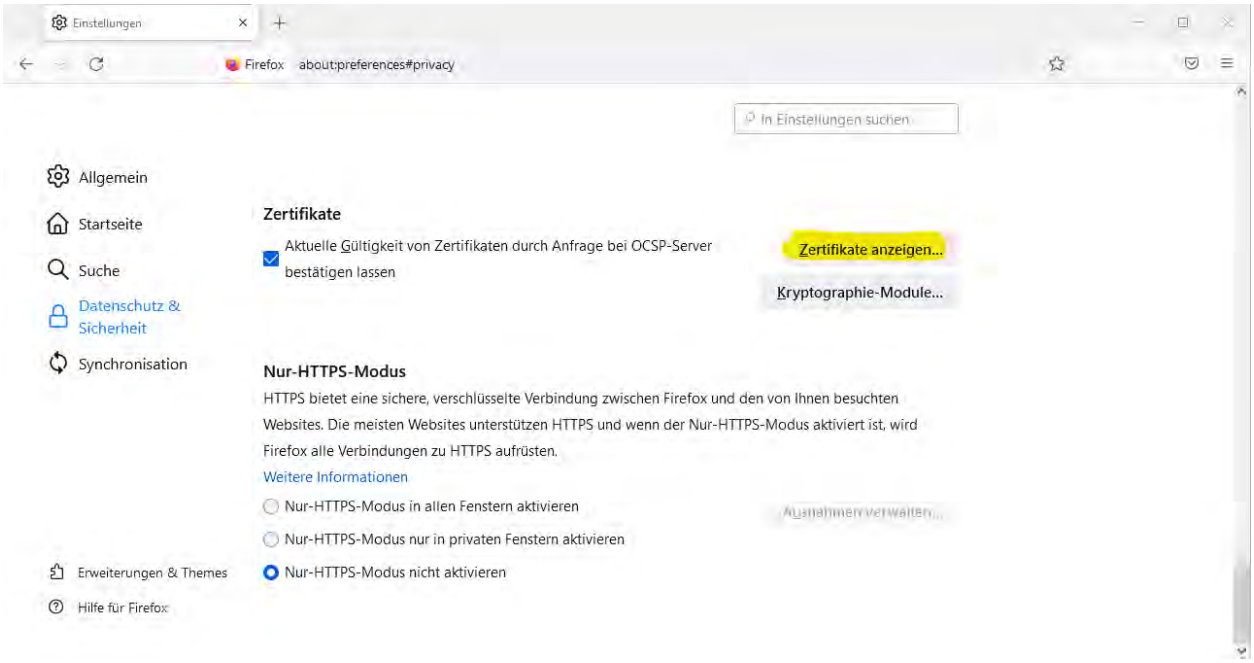


Unter „Zwischenzertifizierungsstellen“ – „Zertifikate“ sollte nun das Zertifikat „SSL-Client2016“ oder „SSL-Client2022“ aufgeführt werden.

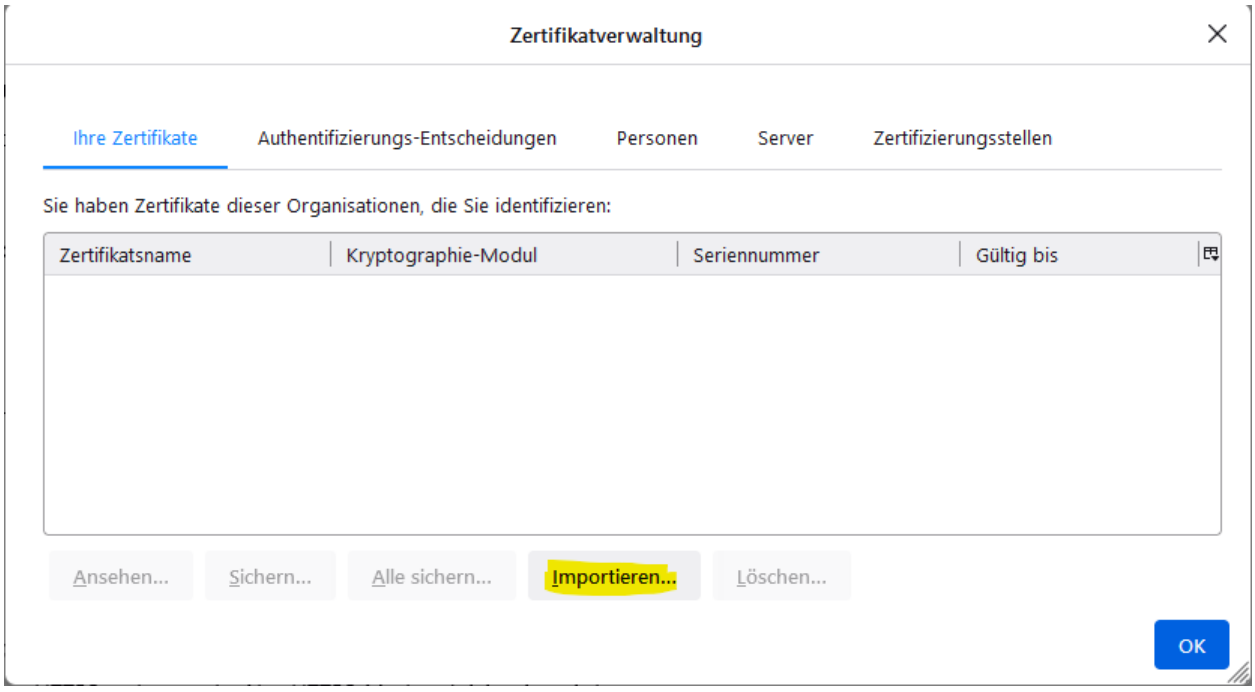


4 Import der Clientzertifikate in Mozilla Firefox

4.1 Starten der Firefox-Zertifikatsverwaltung unter „Einstellungen“ – „Datenschutz und Sicherheit“ – „Zertifikate“ – „Zertifikate anzeigen“

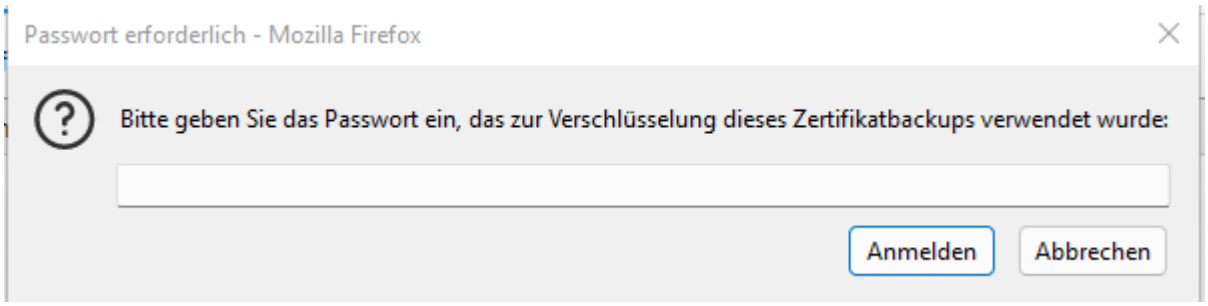


4.2 In der Firefox Zertifikatsverwaltung wählen Sie die Registerkarte „Ihre Zertifikate“ aus und klicken Sie auf „Importieren“.



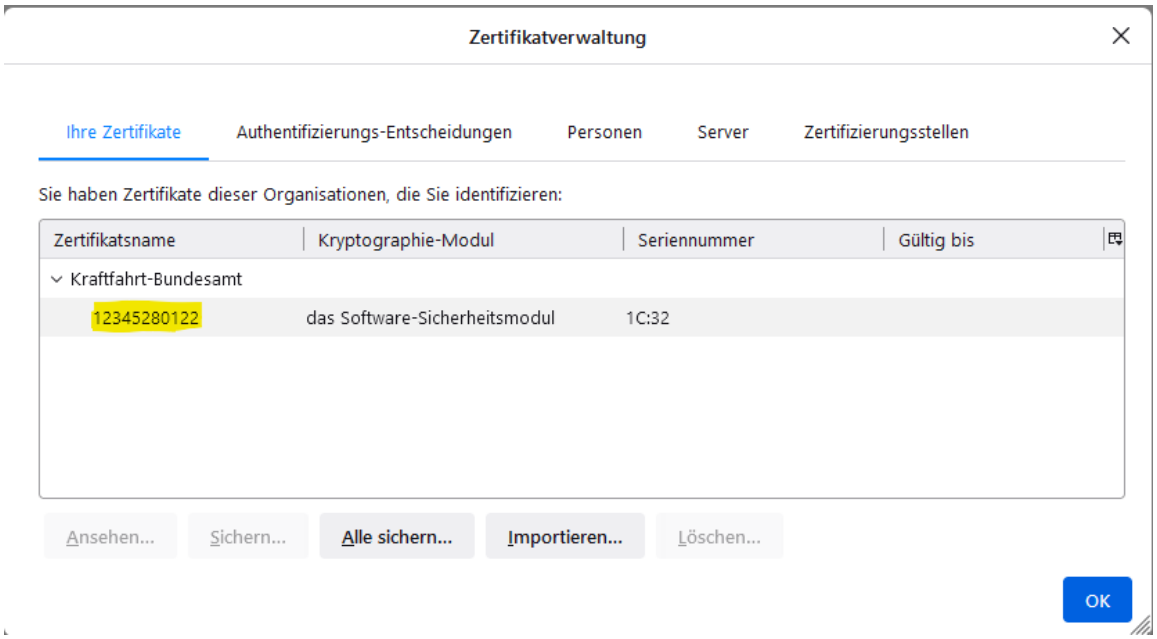
4.3 Wählen Sie die vom KBA übersandte P12-Datei aus

4.4 Geben Sie das vom KBA übermittelte Passwort ein.



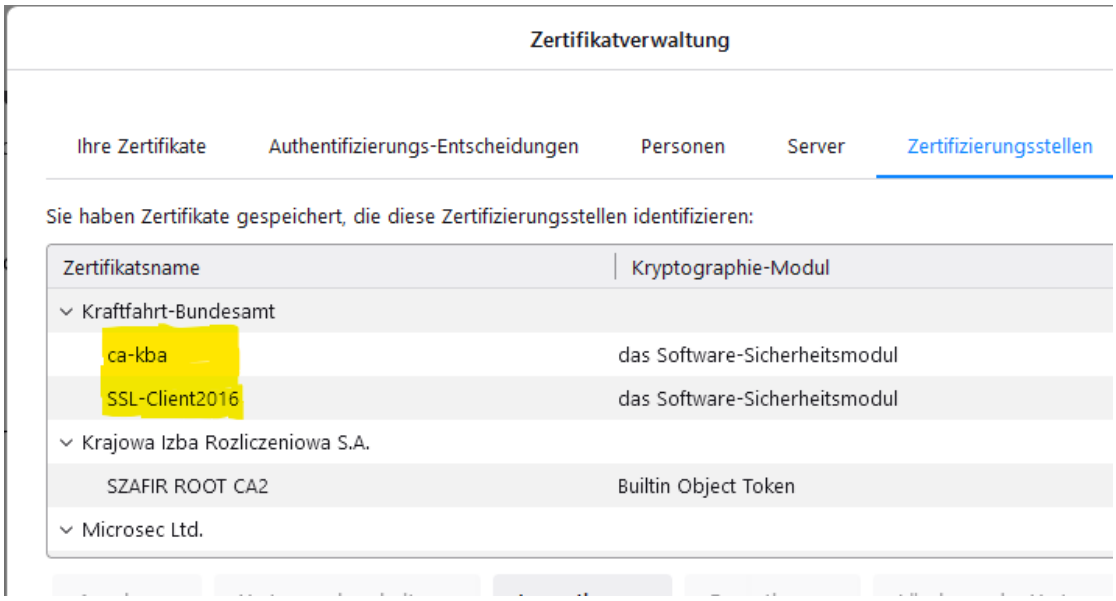
Das Passwort für den Import wird in der Regel per Briefpost an den Leiter der IT der beantragenden Behörde versandt.

4.5 Überprüfen Sie unter „Ihre Zertifikate“, ob das Zertifikat importiert wurde.



Der Name des Zertifikats entspricht dabei im Regelfall dem Dateinamen der importierten Datei und ist ebenfalls auf dem Passwortbrief zu finden.

4.6 Überprüfen Sie unter „Zertifizierungsstellen“, ob die Zertifikate „ca-kba“ und „SSL-Client2016“ oder „SSL-Client2022“ importiert wurden.



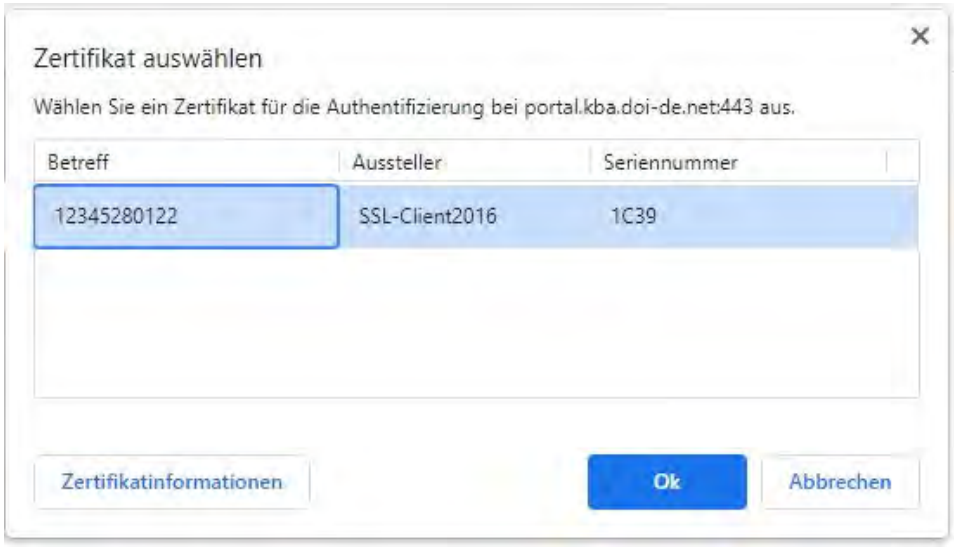
5 Zugriff

Nach der Installation der Client-Zertifikate kann ein Testzugriff auf das ZEVIS-Portal stattfinden.

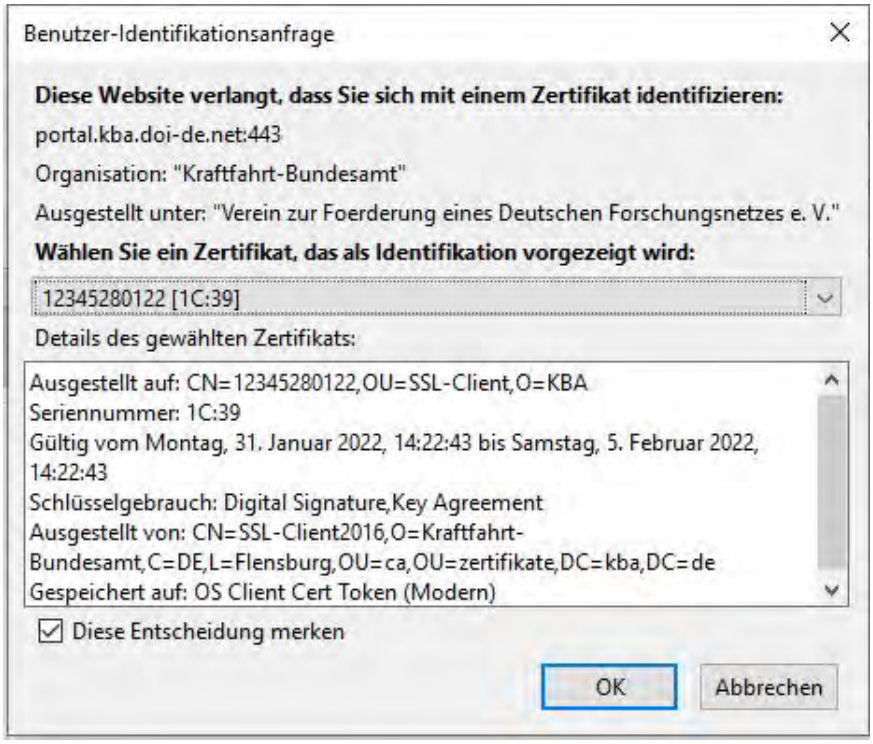
Bitte rufen Sie dafür im Browser https://portal.kba.doi-de.net/ auf.

Sie werden daraufhin aufgefordert, das entsprechende Client-Zertifikat auszuwählen und zu bestätigen.

z. B. in Google Chrome und Opera



z. B. im Mozilla Firefox



6 Probleme

Schlägt der Zugriff fehl, führen Sie bitte zunächst ein Update ihres Browsers durch.
Ältere Browser bieten noch keine Unterstützung für TLS 1.2 und sind daher nicht in der Lage die geforderte Verschlüsselung anzuwenden.

Symptome	Mögliche Ursache
• Beim Aufruf der Seite erscheint unmittelbar die Fehlermeldung „Gesicherte Verbindung fehlgeschlagen“	• Veraltete Browser-Version • Das Client Zertifikat wurde nicht erfolgreich importiert. • (eher unwahrscheinlich) Das Client-Zertifikat wurde gesperrt / zurückgezogen
• Beim Aufruf der Seite erscheint nach der Bestätigung des Client-Zertifikats die Fehlermeldung „Gesicherte Verbindung fehlgeschlagen“	• Ggf. Veraltete Browser-Version • Falls Sie eine lokale Antiviren-Software mit Web-Antivirus nutzen, sollten Sie https://portal.kba.doi-de.net als Vertrauenswürdige Website eintragen. • Falls der Zugriff über einen Webproxy erfolgt, auf dem SSL-Inspection aktiviert ist, muss für den Zugriff auf https://portal.kba.doi-de.net die SSL-Inspection deaktiviert werden. • Ihr Client-Zertifikat wurde gesperrt / zurückgezogen *Im Falle einer notwendigen Sperrung eines Zertifikats wird der Antragsteller von der Anwenderbetreuung des Kraftfahrt-Bundesamtes informiert.* *Bitte wenden Sie sich an den Benutzerservice des Kraftfahrt-Bundesamtes.*

• Beim Aufruf der Seite erhalten Sie die Fehlermeldung „Seite nicht gefunden“
• Sie haben **keinen** Proxy-Server im Browser konfiguriert.
• Bei dem Absetzen des Kommandos
`nslookup portal.kba.doi-de.net`
in der Eingabeaufforderung erscheint die Fehlermeldung:
`*** portal.kba.doi-de.net wurde nicht gefunden: Non-existent domain.`
	• Kein DNS-Server konfiguriert oder fehlende Weiterleitung von DNS-Anfragen an doi-de.net an die DNS-Server des NdB-Verbindungsnetzes.
	Bitte stellen Sie sicher, dass der DNS-Server ihrer Behörde Anfragen zu der Zone „doi-de.net“ an den DNS-Server ihres Landesverwaltungsnetz-Anbieters weiterleitet.

• Beim Aufruf der Seite erhalten Sie die Fehlermeldung „Seite nicht gefunden“
• Sie haben **keinen** Proxy-Server im Browser konfiguriert.
• Bei dem Absetzen des Kommandos
`telnet portal.kba.doi-de.net 443`
in der Eingabeaufforderung erscheint die Fehlermeldung:
`Verbindungsaufbau zu portal.kba.doi-de.net...`
`Es konnte keine Verbindung mit dem Host hergestellt werden, auf Port443: Verbindungsfehler`
	• Fehlerhaftes Routing
	• Fehlende Anbindung an das NdB-Verbindungsnetz (DOI-Netz) über das Landesverwaltungsnetz
	• Fehlende Firewall-Freischaltung für den Zugriff auf das ZEVIS-Portal
	- innerhalb der Behörde,
	- im Landesrechenzentrum
	Bitte prüfen Sie die Verbindung zusammen mit Ihrem Landesrechenzentrum.

• Beim Aufruf der Seite erhalten Sie die Fehlermeldung „Seite nicht gefunden“ • Sie haben **einen** Proxy-Server im Browser konfiguriert.	• Fehlerhaftes Routing • Konfigurationsfehler auf dem Proxy-Server • Der Proxy-Server hat keine Anbindung an das NdB-VN (DOI-Netz) über das Landesverwaltungsnetz • Fehlende Firewall-Freischaltung für den Zugriff auf das ZEVIS-Portal - innerhalb der Behörde, - im Landesrechenzentrum Bitte prüfen Sie die Verbindung zusammen mit Ihrem Landesrechenzentrum.

Ansprechpartner beim Kraftfahrt-Bundesamt

Technische Informationen bezüglich der Netzanbindung und der Sicherheitsmaßnahmen erhalten Sie über:

Technischer Support
Tel.: (0461) 316-1400
Fax.: (0461) 316-2818
E-Mail: KBA-ServiceDesk@kba.de

Informationen zur Beantragung sowie Antragsunterlagen erhalten Sie über:

Anwenderbetreuung
Tel.: (0461) 316-1717
Fax.: (0461) 316-2942
E-Mail: Anwenderbetreuung@kba.de

Kraftfahrt-Bundesamt
24932 Flensburg
Internet: www.kba.de

Impressum

Herausgabe:
Kraftfahrt-Bundesamt
24932 Flensburg

Internet: www.kba.de

Fachliche Auskünfte und Beratung:

Telefon: 0461 316-1717
Telefax: 0461 316-2942
E-Mail: Anwenderbetreuung@kba.de

Erschienen im Dezember 2015
Stand: Januar 2022

Druck: Druckzentrum KBA

Bildquelle: www.shutterstock.de