Zertifikatsbearbeitung

STAATSBETRIEB SÄCHSISCHE INFORMATIK DIENSTE | Freistaat SACHSEN

Anleitung zum Stand - 21.02.2024

erstellt durch den

Staatsbetrieb Sächsische Informatik Dienste

Import, Export und Löschung von Zertifikaten mit dem Windows Zertifikatsspeicher

Arbeitsgruppe		**DVDV-pflegende Stelle Sachsen**	
Version		1.0 vom 21.02.2024	
Autor	Ohle, Maik	**Telefonnummer**	**0351 3264-7399**
		E-Mail	saxdvdv@sid.sachsen.de
geändert durch		**Telefonnummer**	
		E-Mail	

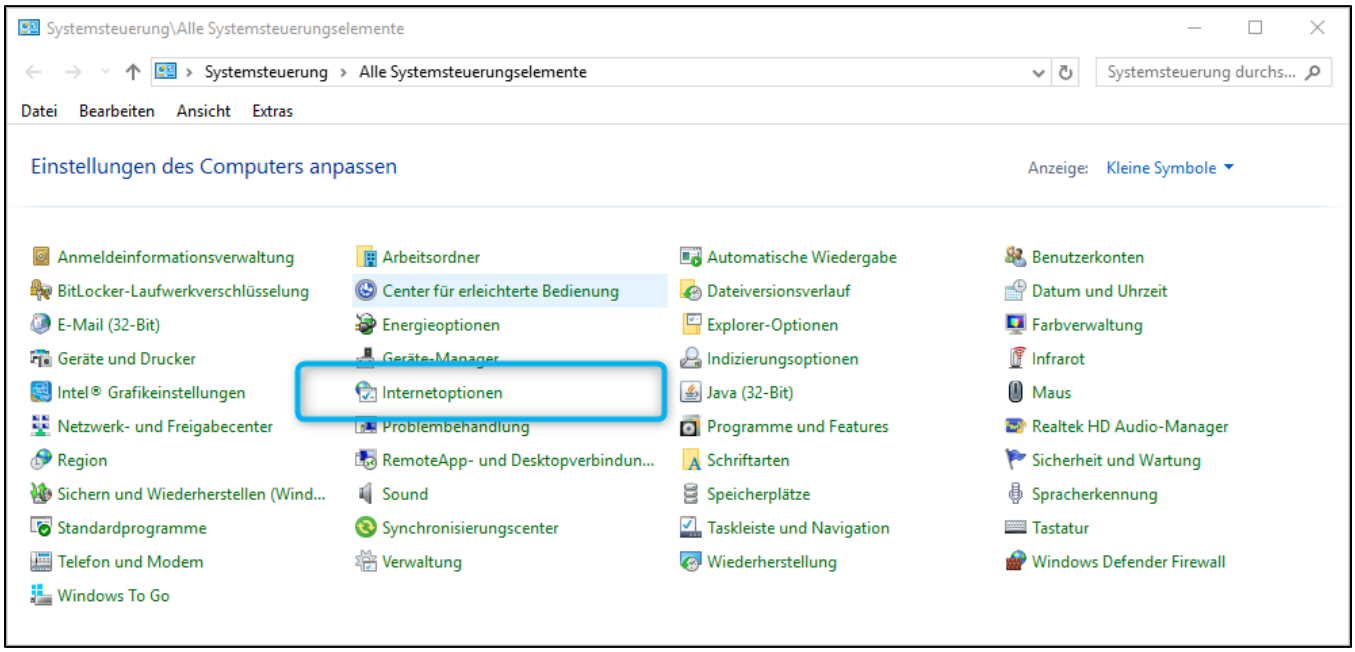
Inhaltsverzeichnis

1 Windows-Zertifikatsspeicher öffnen

Nachdem das Zertifikat heruntergeladen wurde, kann das Zertifikat in den globalen Windows-Zertifikatsspeicher einfügt werden.

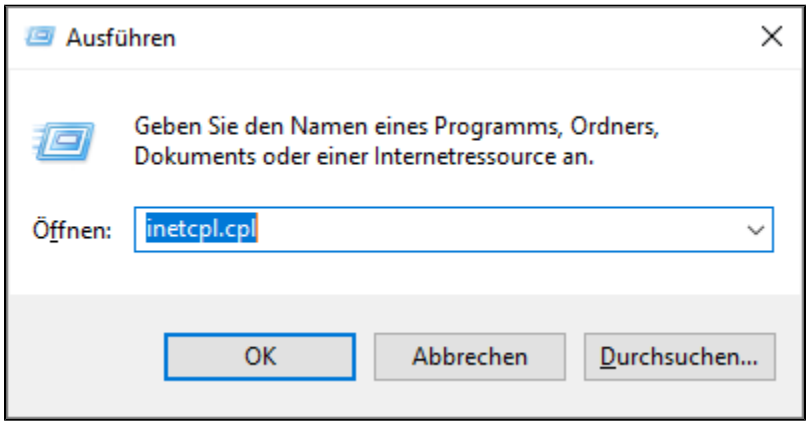
Der Windows-Zertifikatsspeicher kann über die Internetoptionen erreicht werden.

Die Internetoptionen können über die **Systemsteuerung\Internetoptionen** erreicht werden.

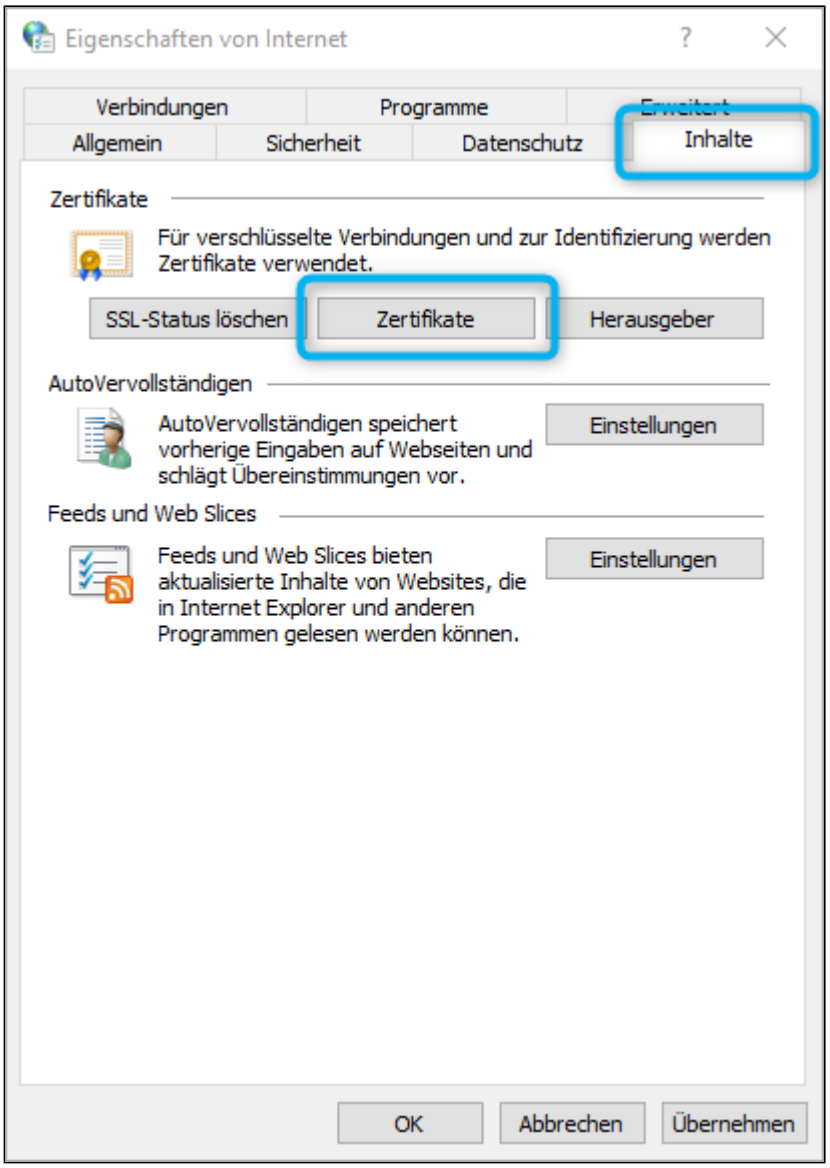


oder

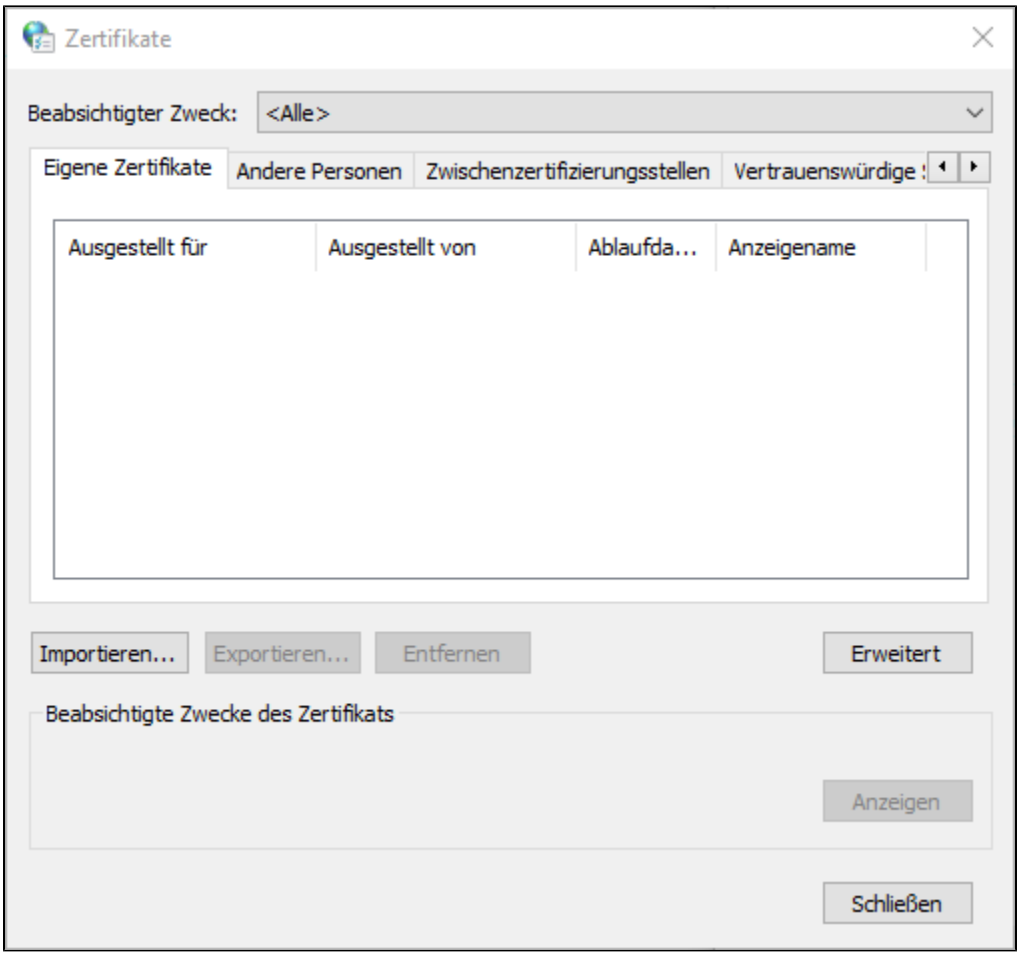
Starten Sie den "Ausführen Dialog" mit [**Windows +R**]. Geben Sie dazu den Befehl: **inetcpl.cpl** ein und schließen mit der [Taste Enter] oder '**OK**' ab.



Wechseln Sie auf die Registerkarte **Inhalte** und klicken Sie dann auf **Zertifikate**.

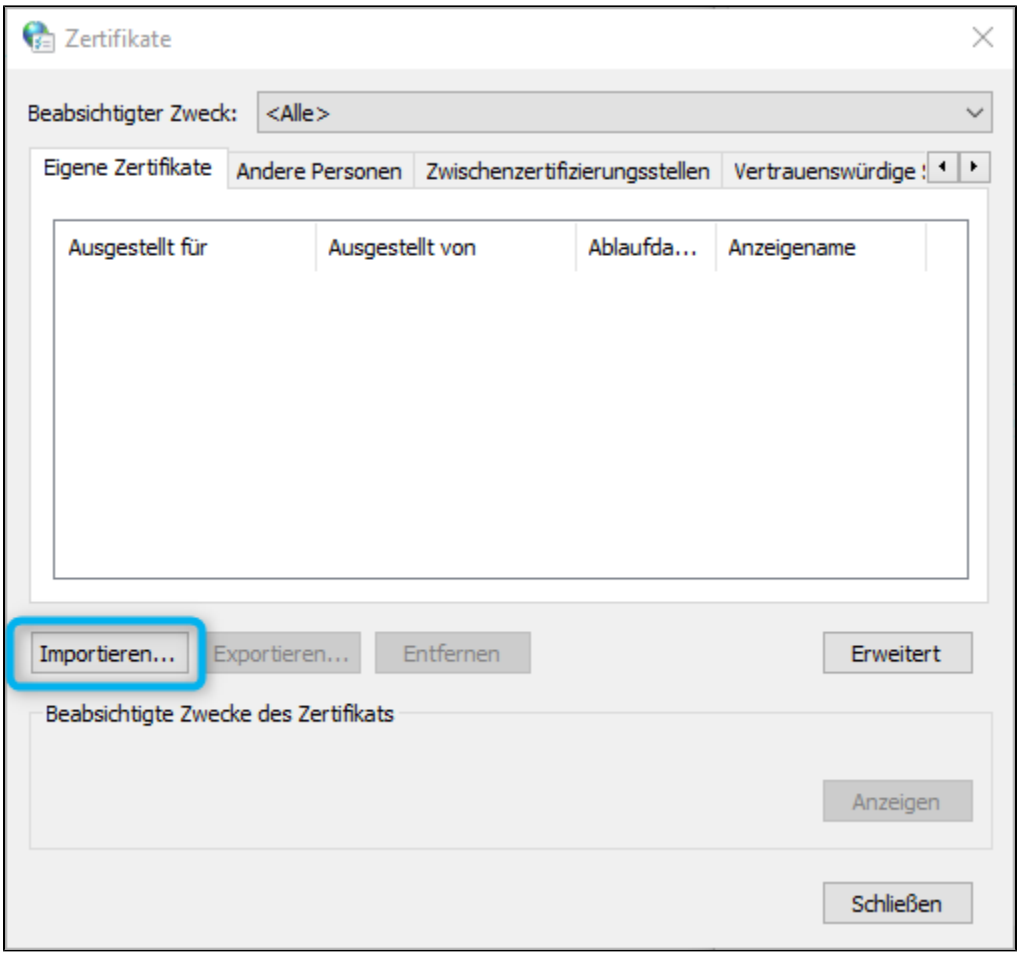


Daraufhin sehen Sie eine Übersicht der bereits installierten Zertifikate im Zertifikatsspeicher. Wenn noch keine eigenen Zertifikate installiert sind, existieren keine Einträge.

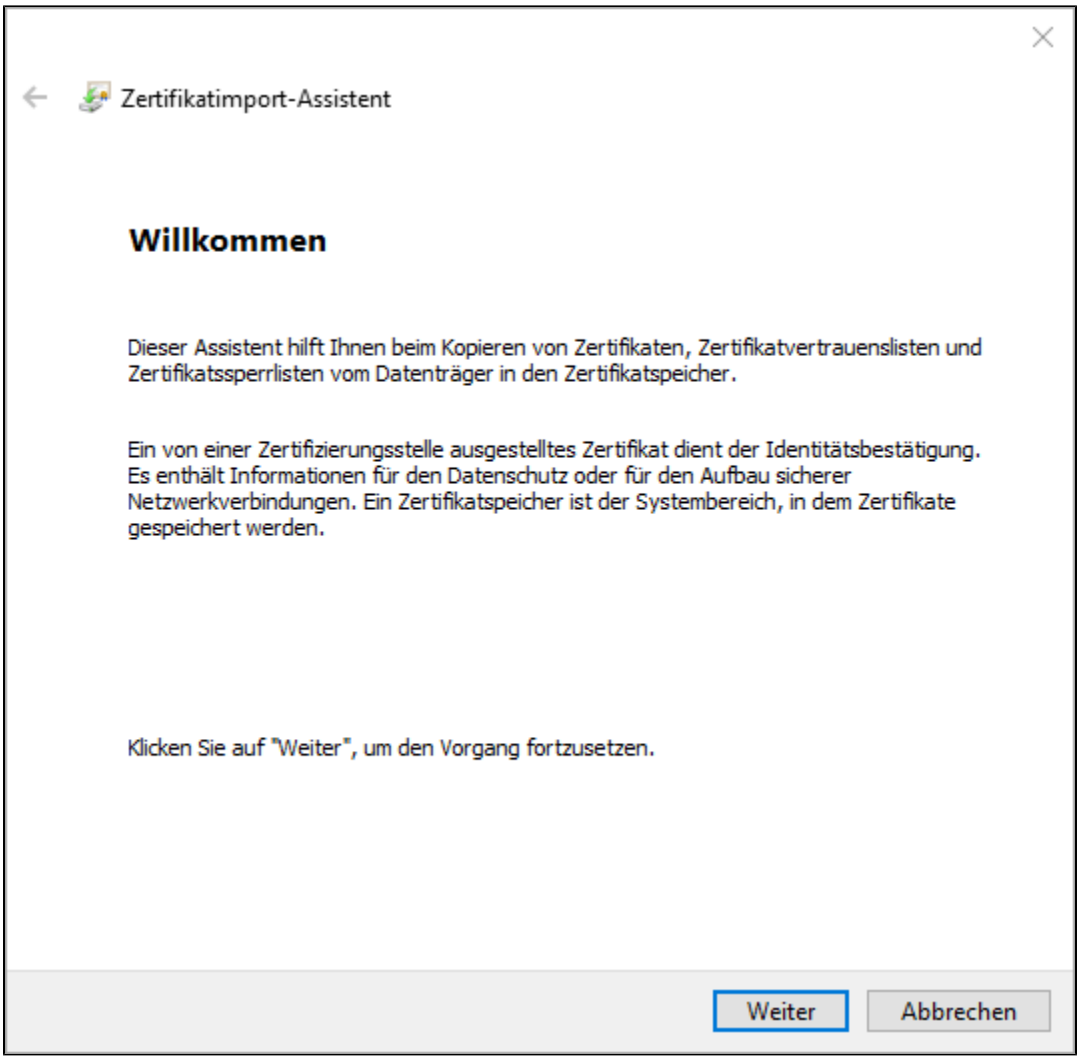


2 Zertifikat (*.p12) importieren

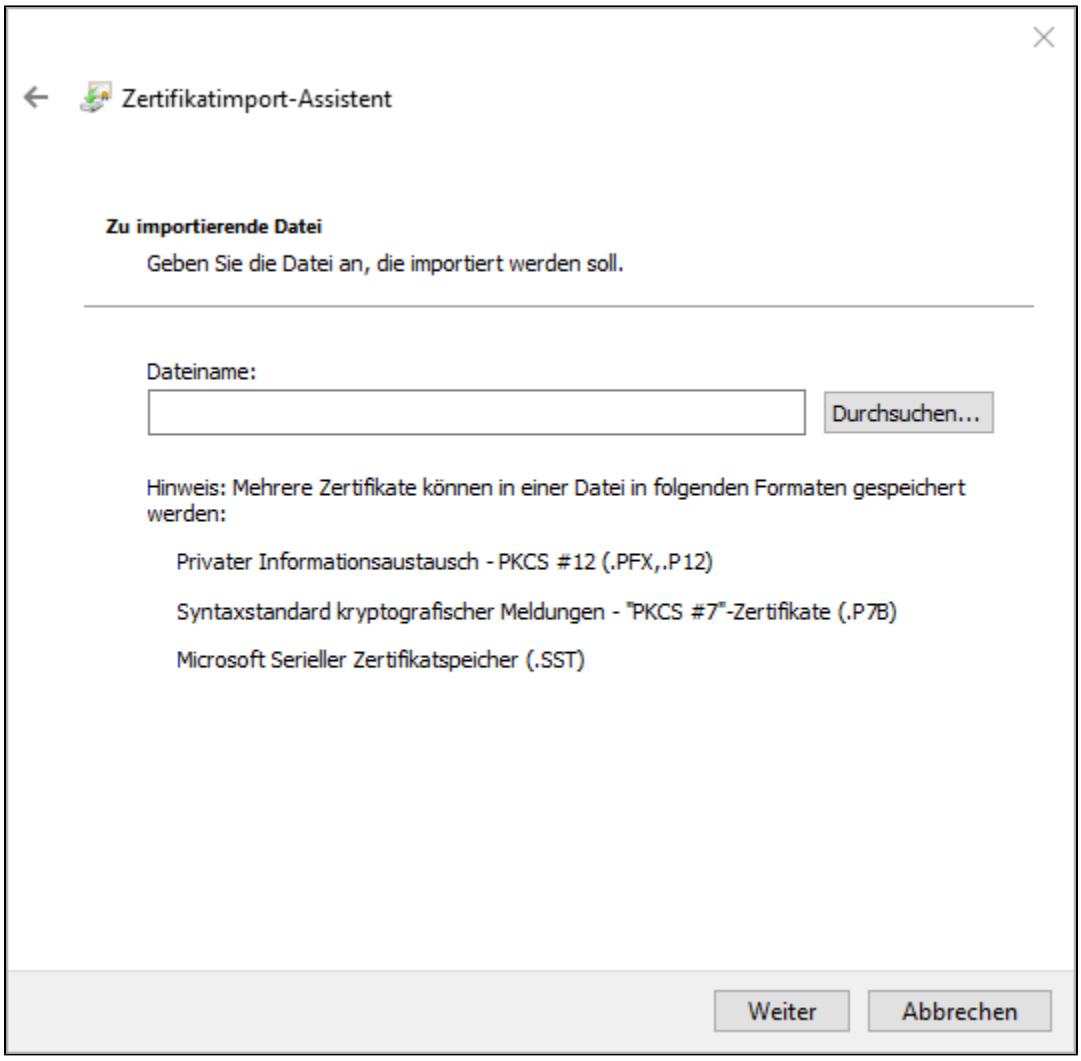
Klicken Sie nun auf **Importieren...**.



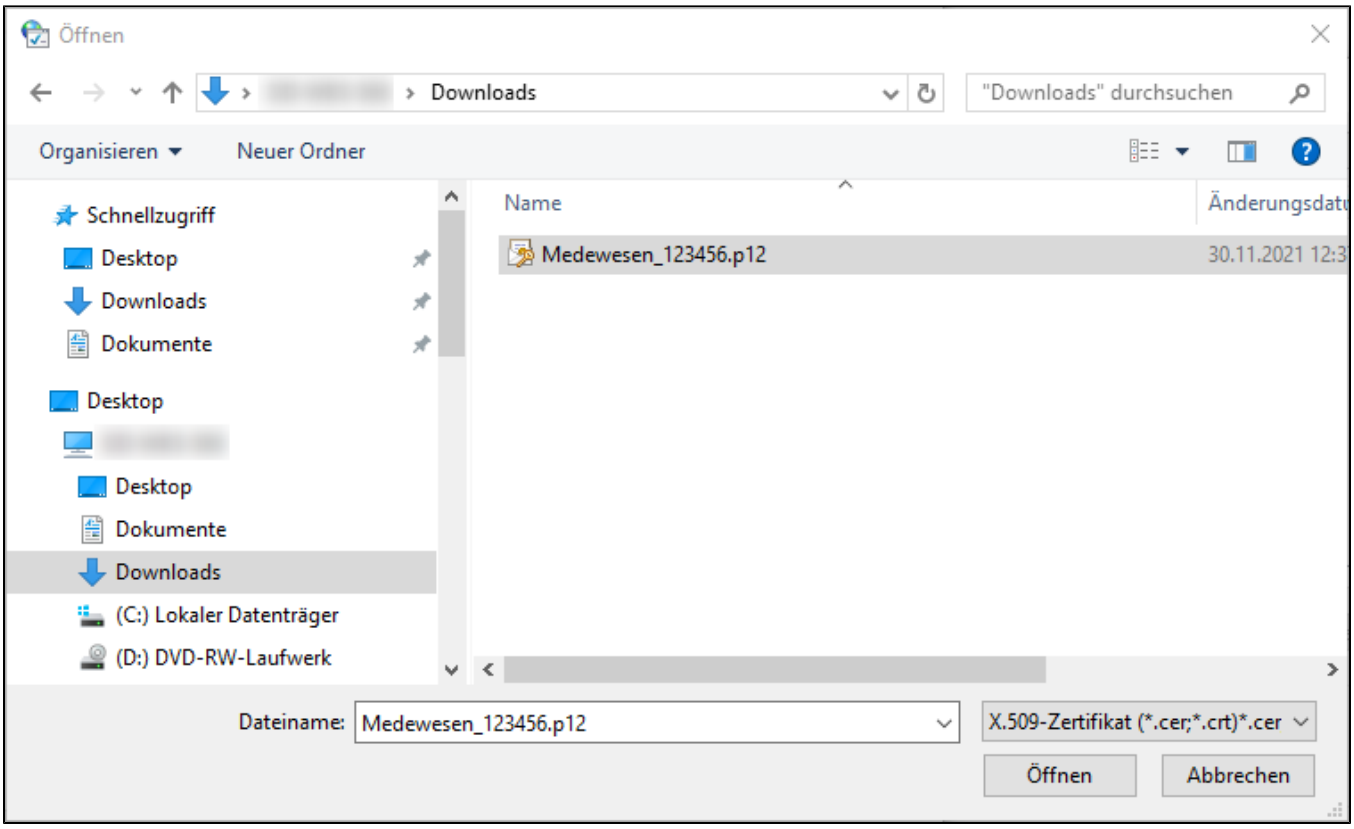
Es öffnet sich der Zertifikatsimport-Assistent für den Zertifikatsspeicher. Klicken Sie im Eingangsdialog auf **Weiter**.



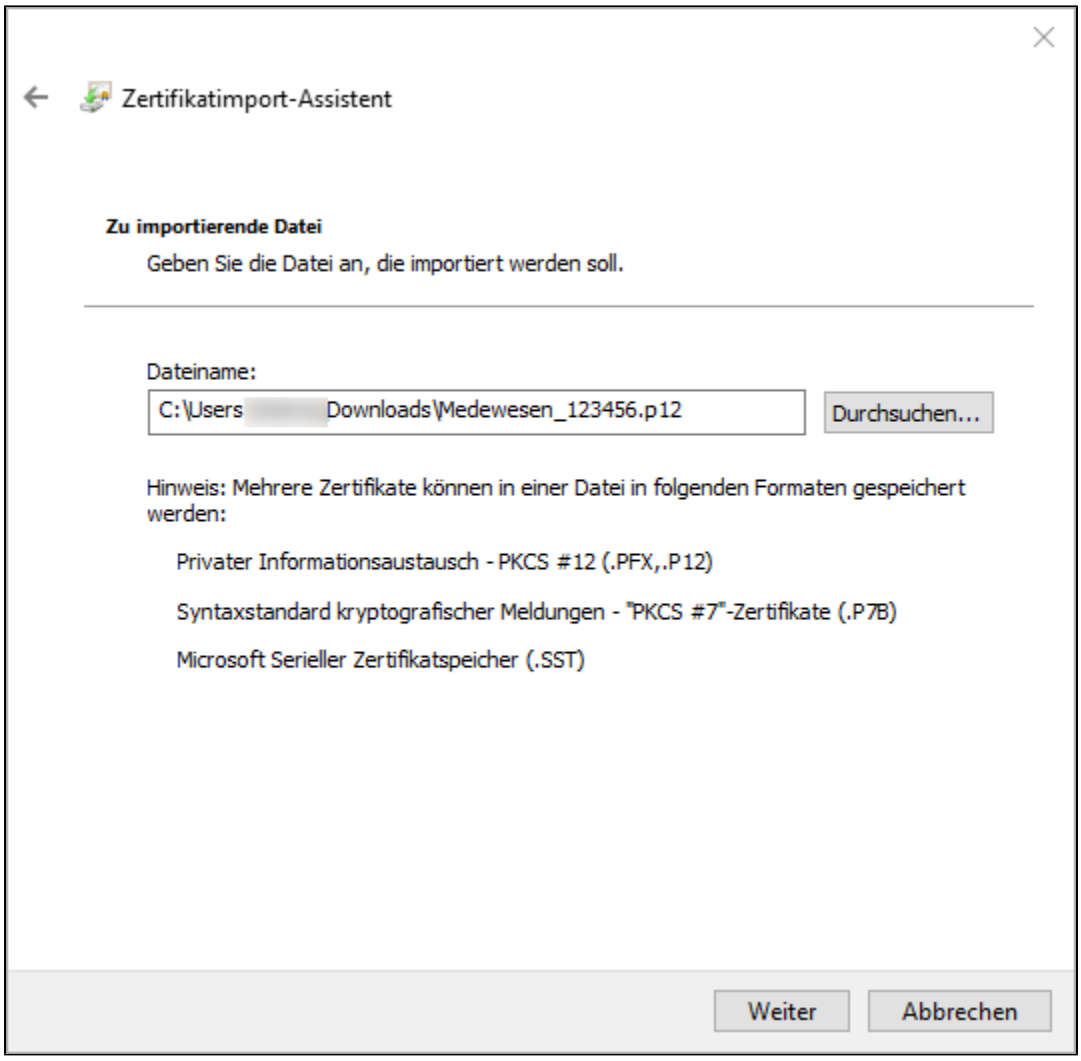
Der Zertifikatsimport-Assistent fordert Sie zur Auswahl der zu importierenden Zertifikatsdatei auf.
Sie können den kompletten Dateipfad direkt eingeben oder durch Klicken auf **Durchsuchen** die Dateiauswahlbox benutzen.



Wählen Sie den Datenträger aus und öffnen Sie dann ggf. das Verzeichnis, in dem das Zertifikat gespeichert ist. Wählen Sie dann das Zertifikat aus, dass Sie importieren möchten. Klicken Sie dann auf **Öffnen**.

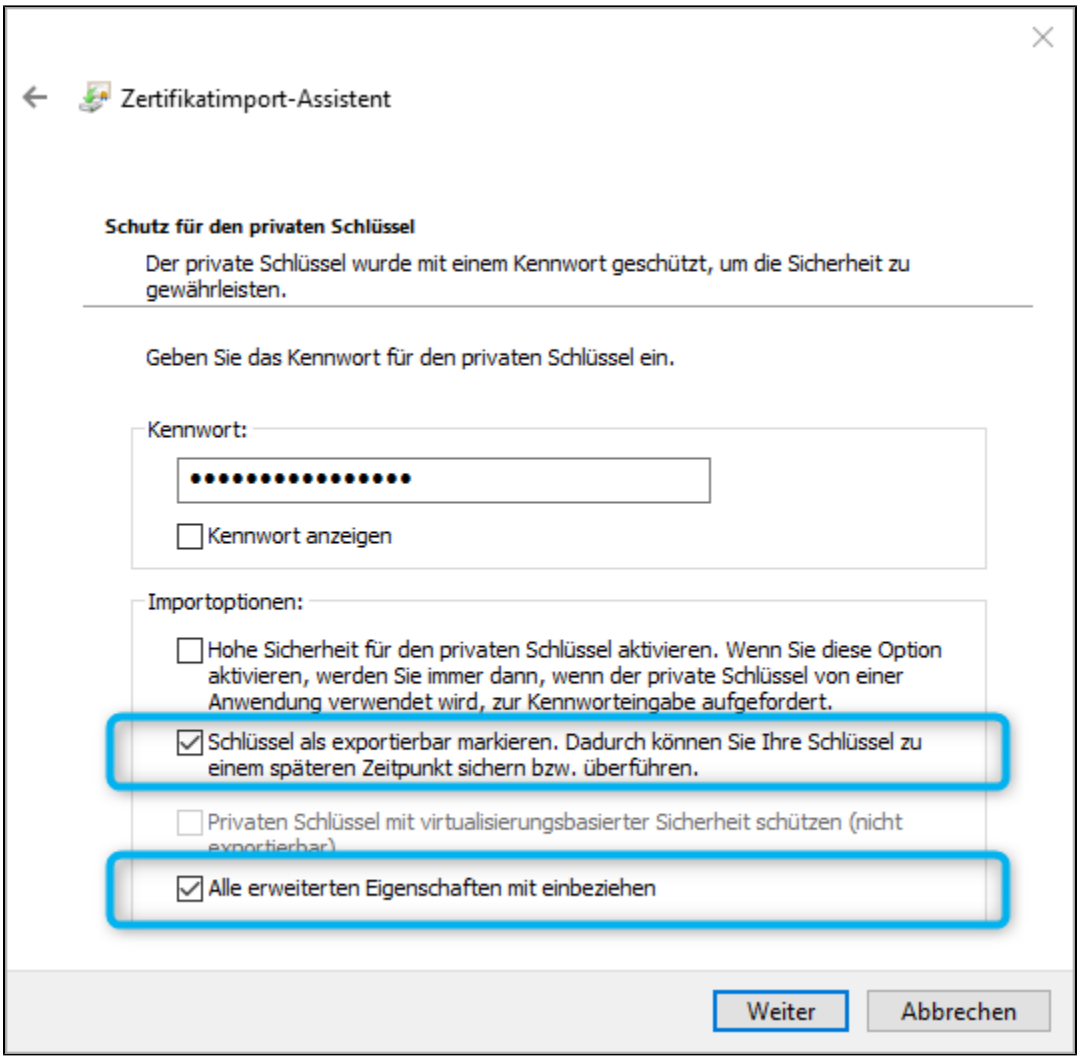


Die ausgewählte Datei wird jetzt im Zertifikatsimport-Assistent angezeigt. Klicken Sie auf **Weiter**.

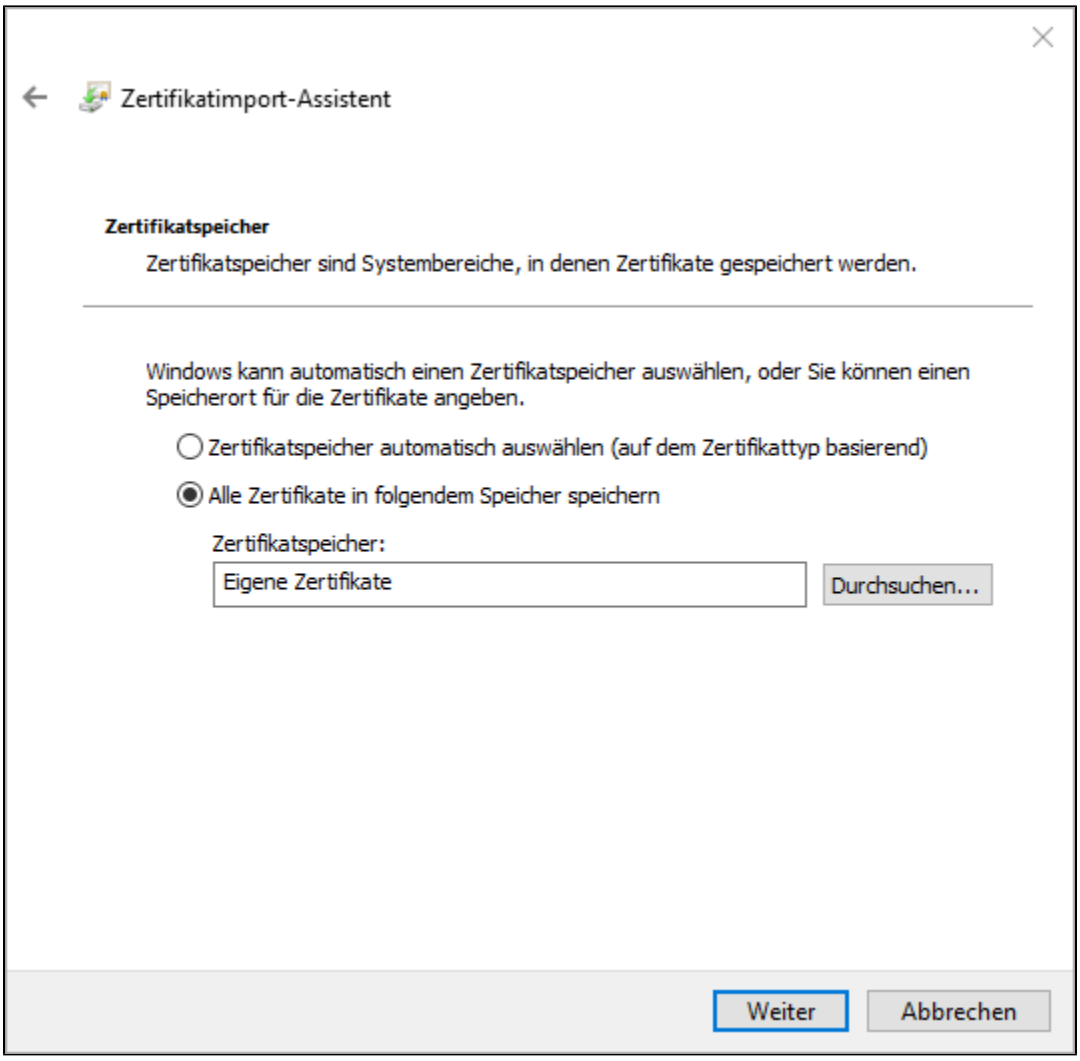


Sie werden jetzt aufgefordert, das Passwort für das Zertifikat einzugeben. Das PKCS #12-Kennwort für die Zertifikate finden Sie auf dem Zertifikatsantrag auf Blatt 3.

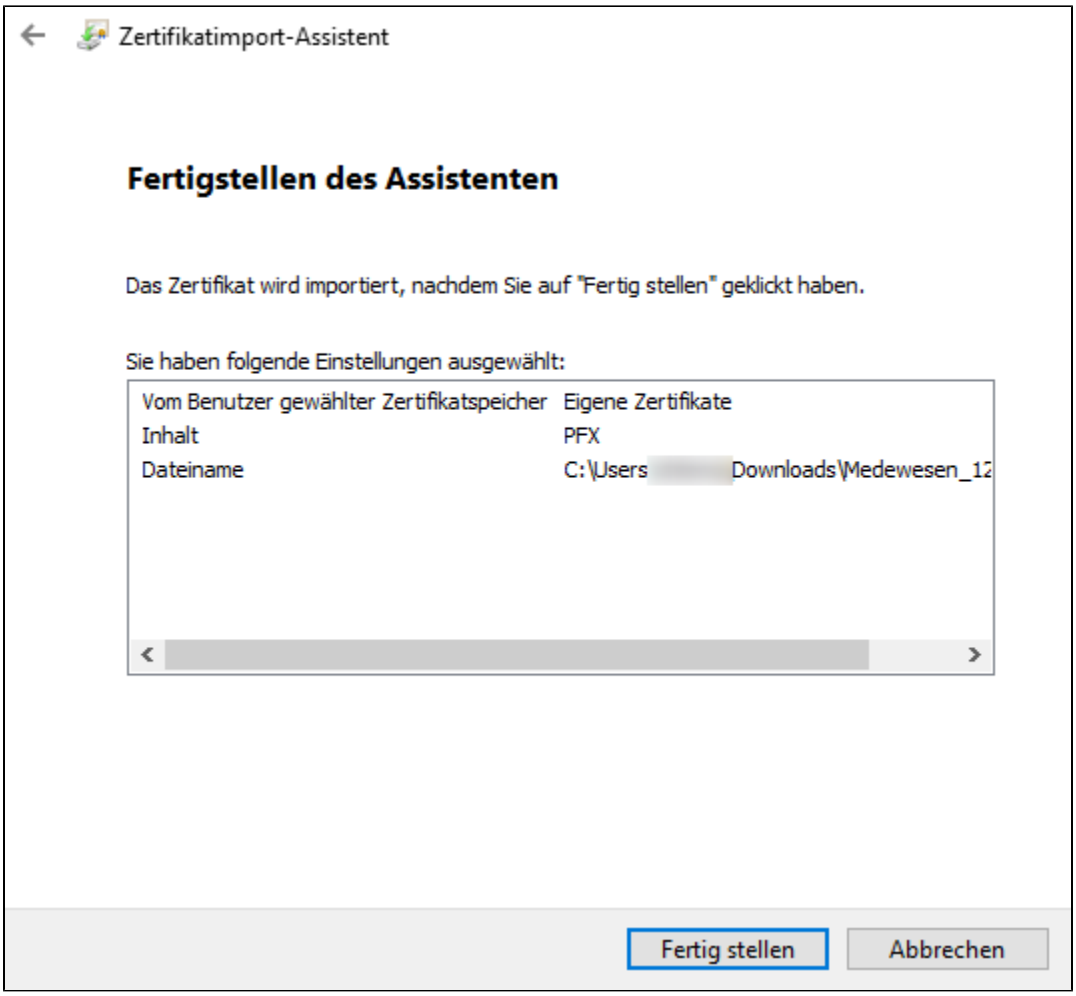
Möchten Sie dieses Zertifikat später wieder von diesem Rechner aus exportieren, setzen Sie das Häkchen bei Schlüssel als exportierbar markieren und klicken dann auf **Weiter**.



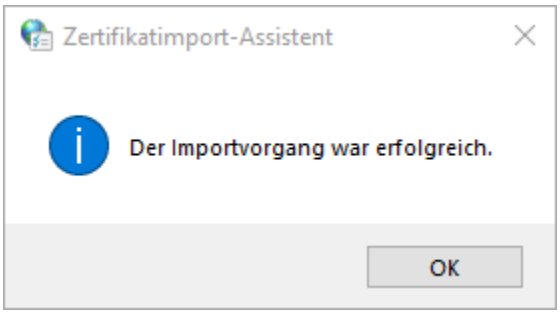
Anschließend können Sie noch den Zertifikatsspeicher auswählen. Für das hier beschriebene Zertifikat wählen Sie den Zertifikatsspeicher "Eigene Zertifikate". Klicken Sie dann auf **Weiter**.



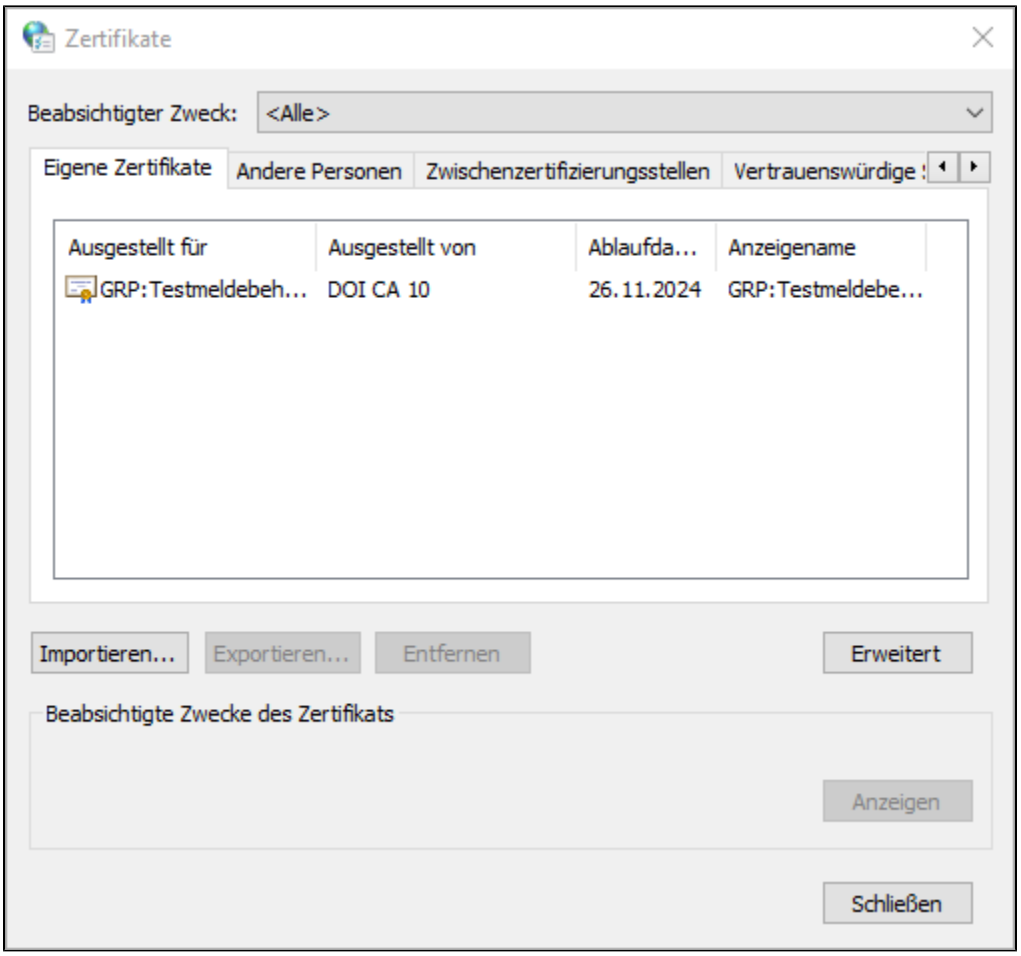
Die Installation wird abgeschlossen. Klicken Sie jetzt auf "**Fertig stellen"**.



Sie bekommen die Meldung angezeigt, dass der Importvorgang erfolgreich war. Klicken Sie dann auf **OK**.



Der Import ist abgeschlossen. Nach erfolgreicher Installation erscheint das Zertifikat als Eintrag im Reiter "Eigene Zertifikate" im Zertifikatsspeicher.



3 Zertifikat exportieren

Für die Verwendung in weiteren Anwendungen können Sie Ihr Zertifikat exportieren.

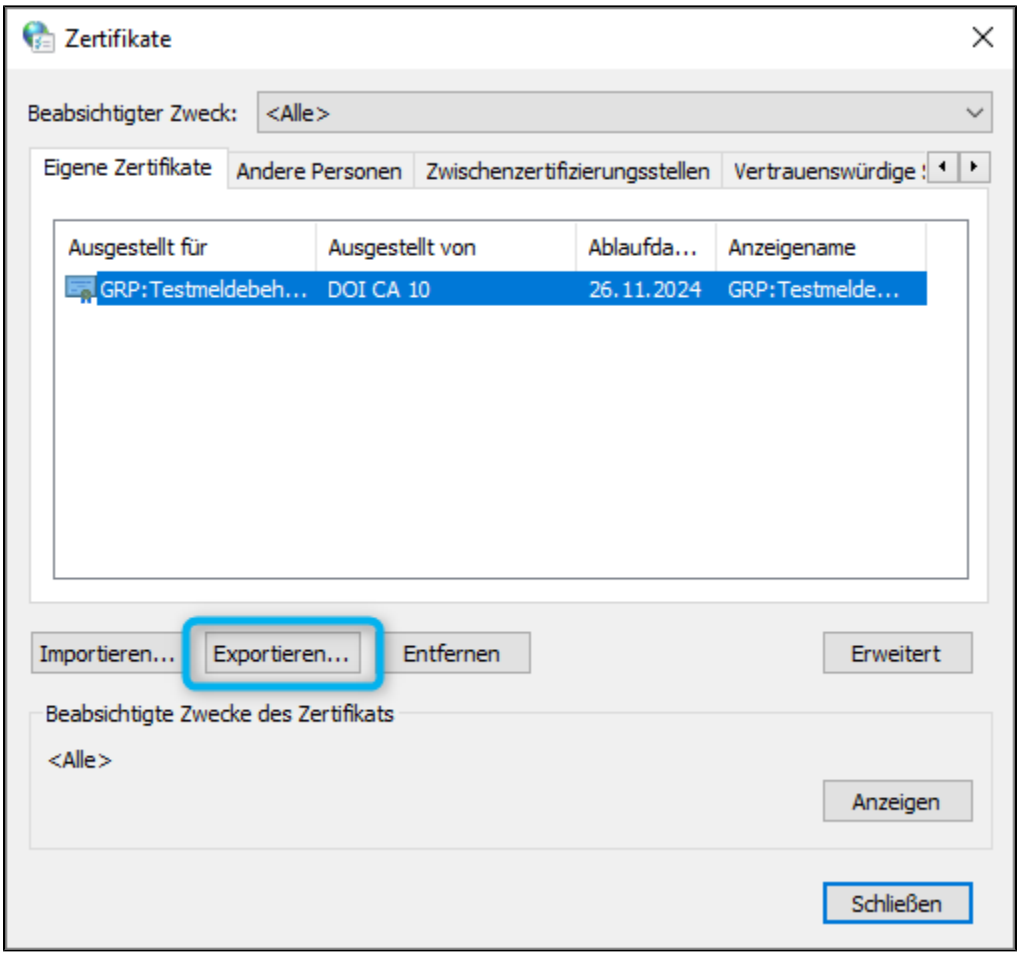
Um Ihr Zertifikat in weiteren Anwendungen aktiv verwenden zu können, müssen Sie Ihren privaten Schlüssel und alle Zertifikate im Zertifizierungspfad exportieren. Sie erhalten dabei eine Datei mit der Endung „pfx“ bzw. „p12“.

Möchten Sie Ihr Zertifikat nur für die Hinterlegung im DVDV exportieren, müssen Sie nur das öffentliche Zertifikat exportieren. Sie erhalten dabei eine Datei mit der Endung „crt“ oder „cer“.

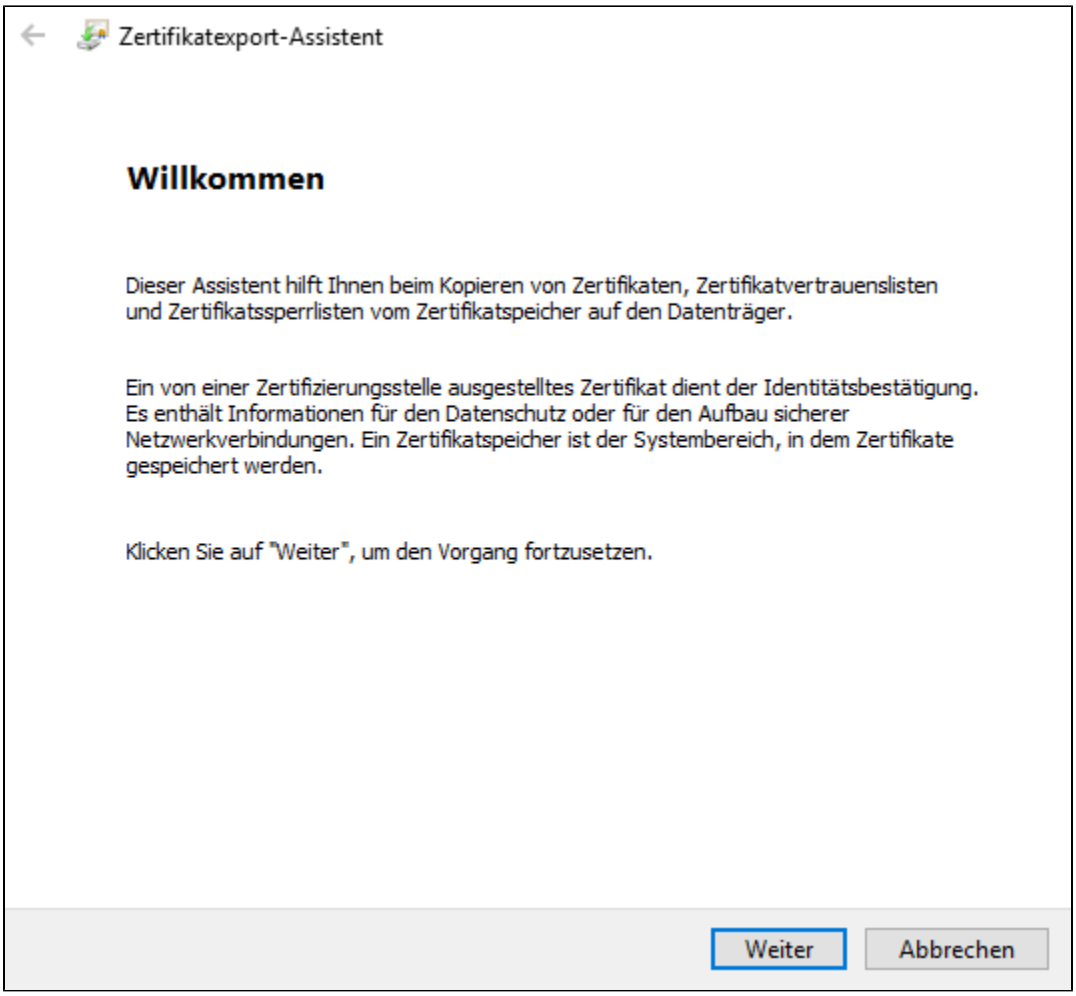
Bitte beachten Sie den Unterschied, damit Sie nicht aus Versehen Ihr privates Zertifikat weitergeben!

3.1 Export „privates Zertifikat“ aus dem Windows Zertifikatsspeicher

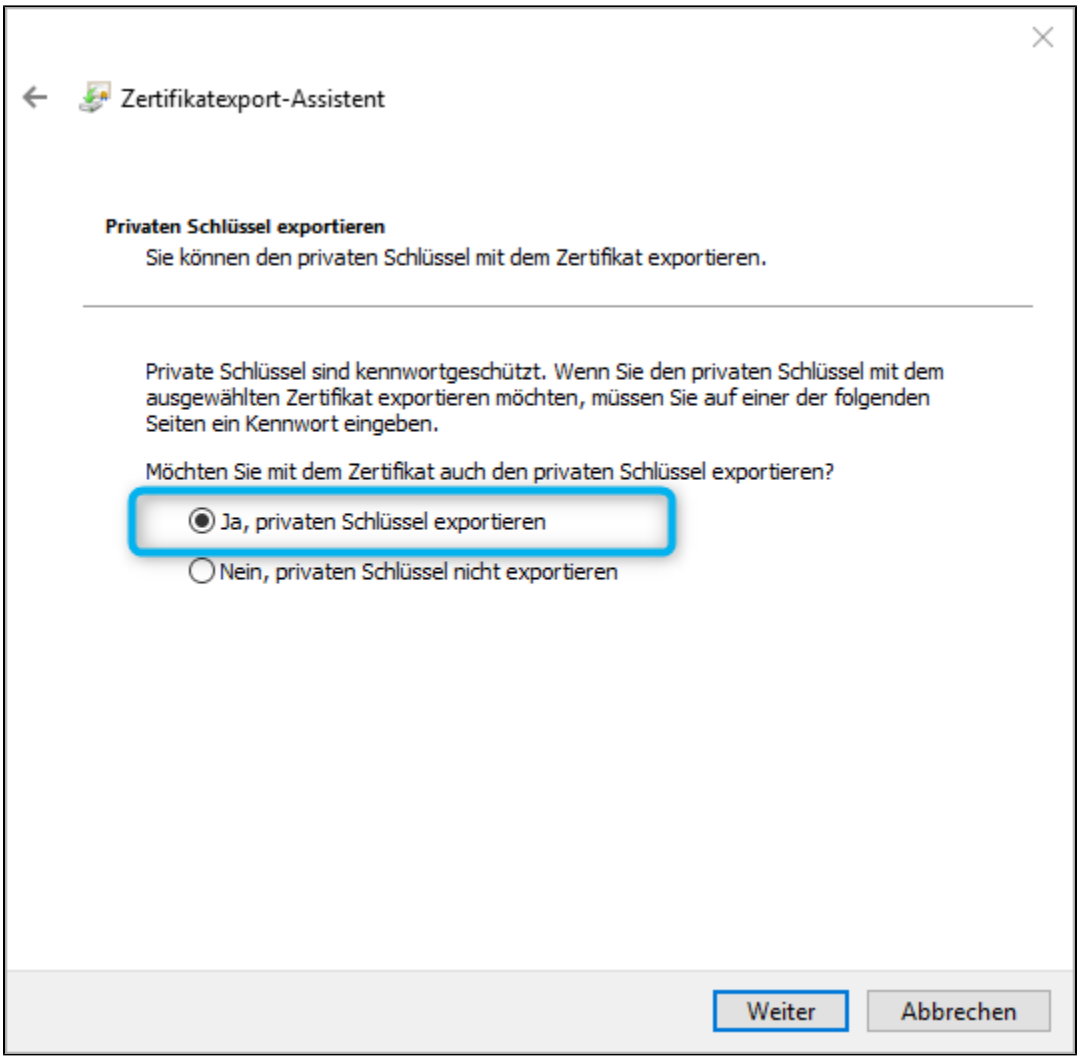
Klicken Sie zunächst mit der linken Maustaste auf das zu exportierende Zertifikat, sodass es farblich hinterlegt ist, und dann auf **Exportieren**.



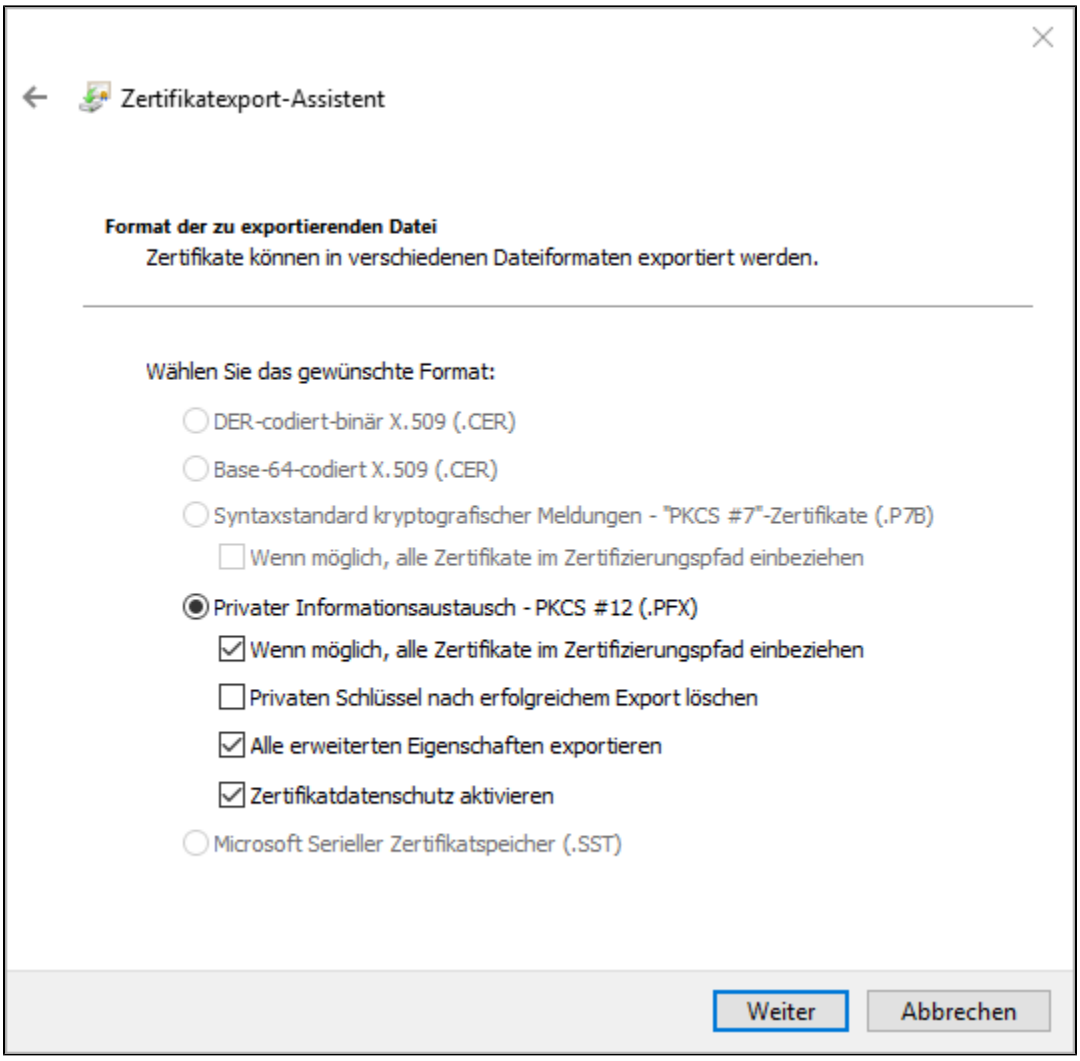
Sie gelangen zum Zertifikatsexport-Assistent. Klicken Sie im Eingangsdialog auf **Weiter**.



Setzen Sie im nächsten Fenster den Punkt bei Ja, privaten Schlüssel exportieren und klicken Sie auf **Weiter**.

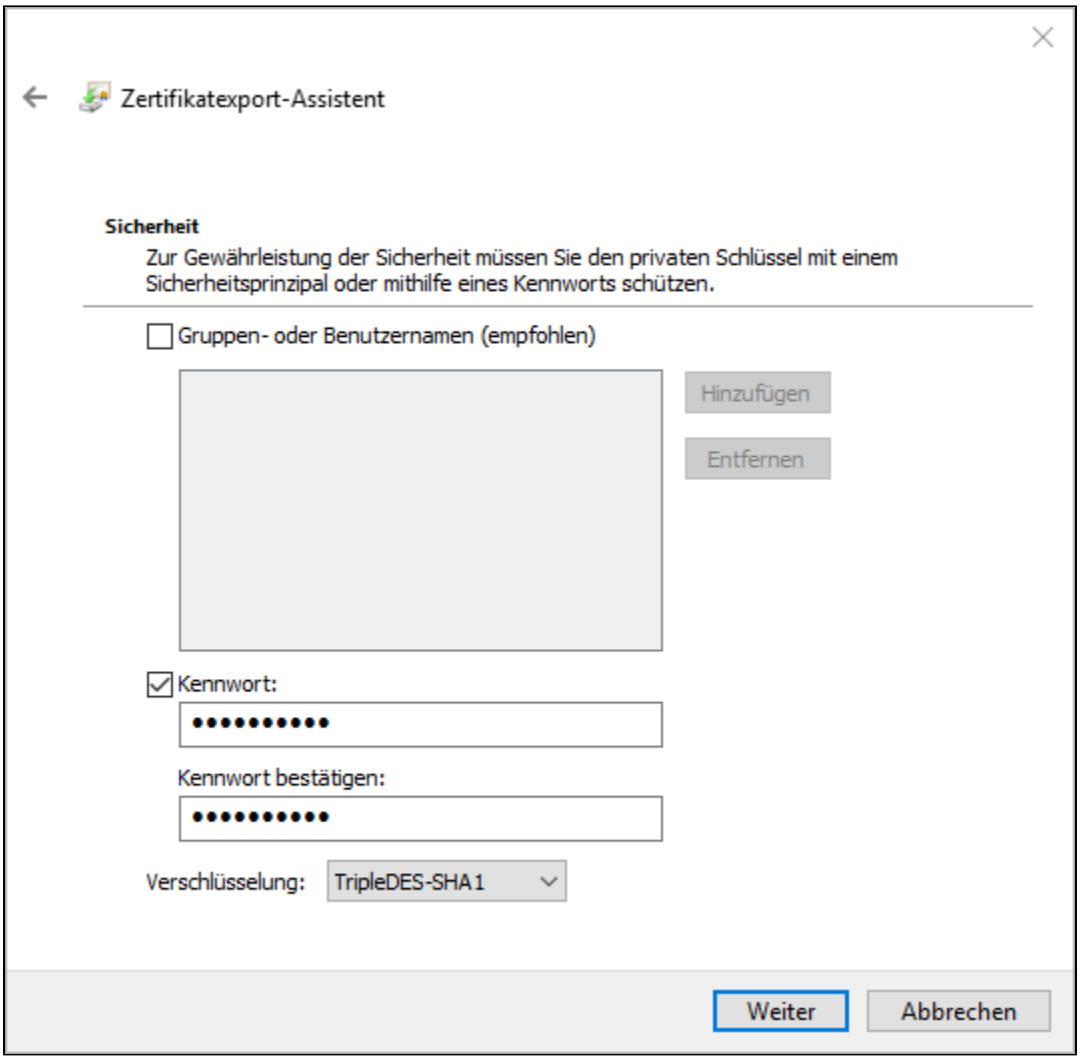


Nehmen Sie folgende Änderungen an der Einstellung vor, klicken Sie hier einfach auf **Weiter**.

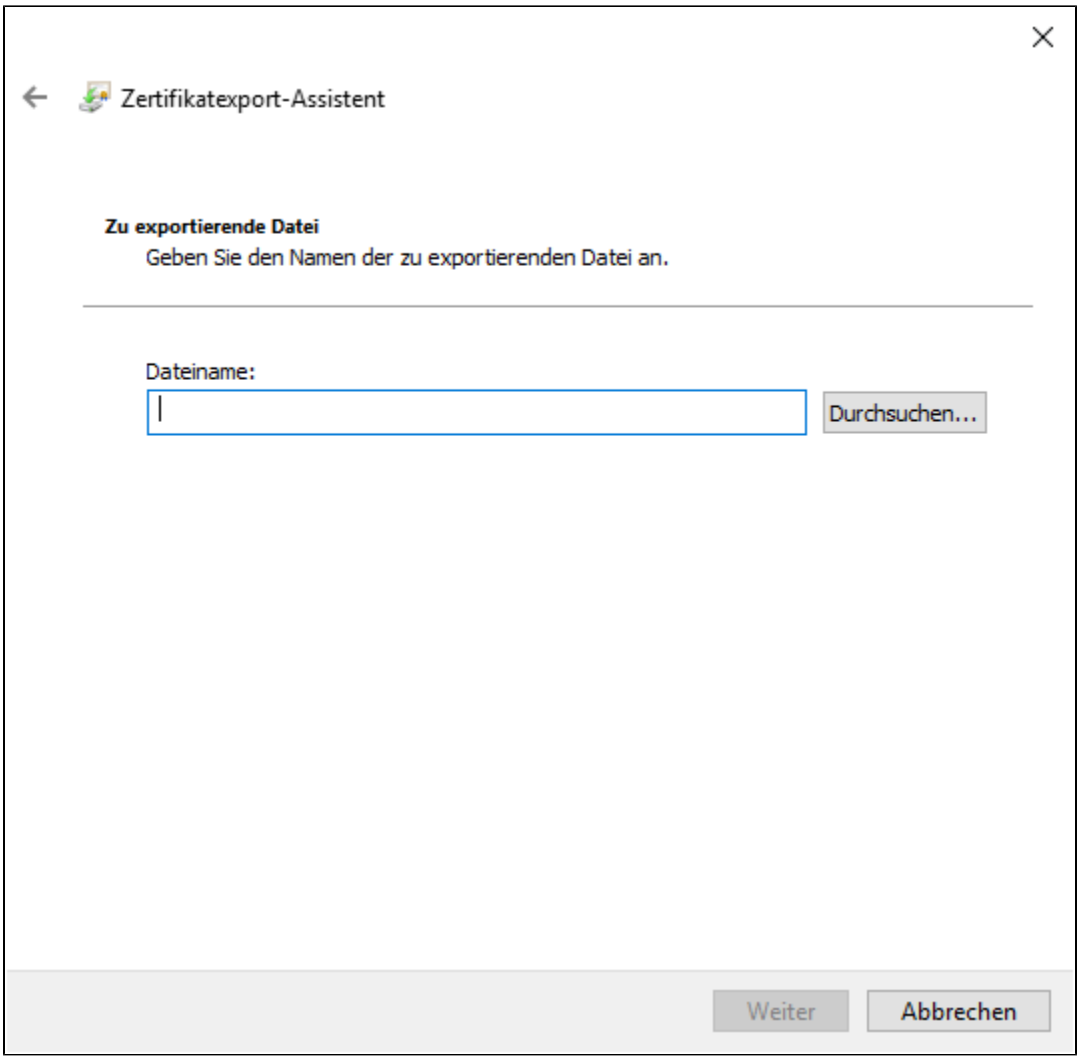


Vergeben Sie jetzt ein Kennwort, nur mit diesem Kennwort kann das Zertifikat wieder importiert werden.

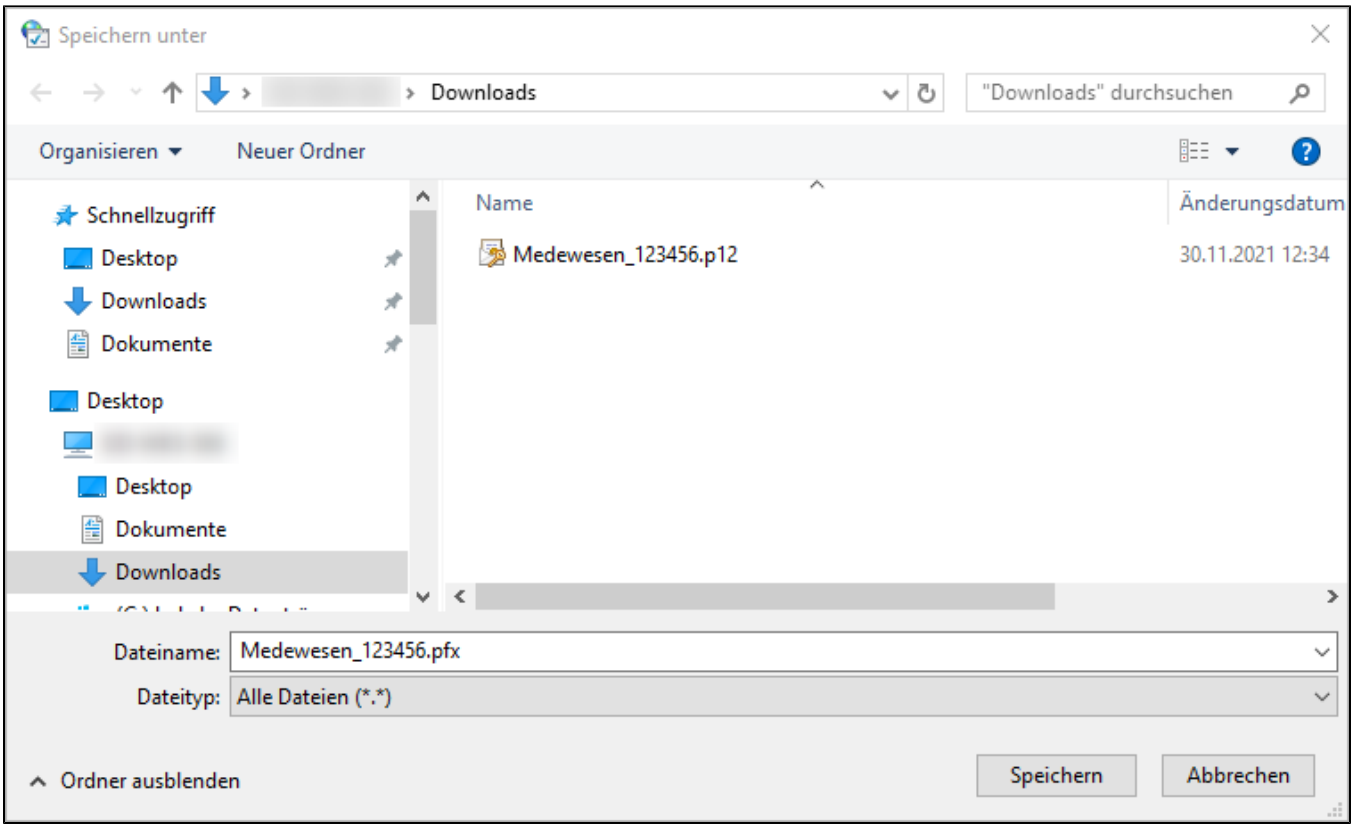
Bitte das Kennwort sorgfältig und für Dritte unzugänglich aufbewahren. Klicken Sie auf **Weiter**.



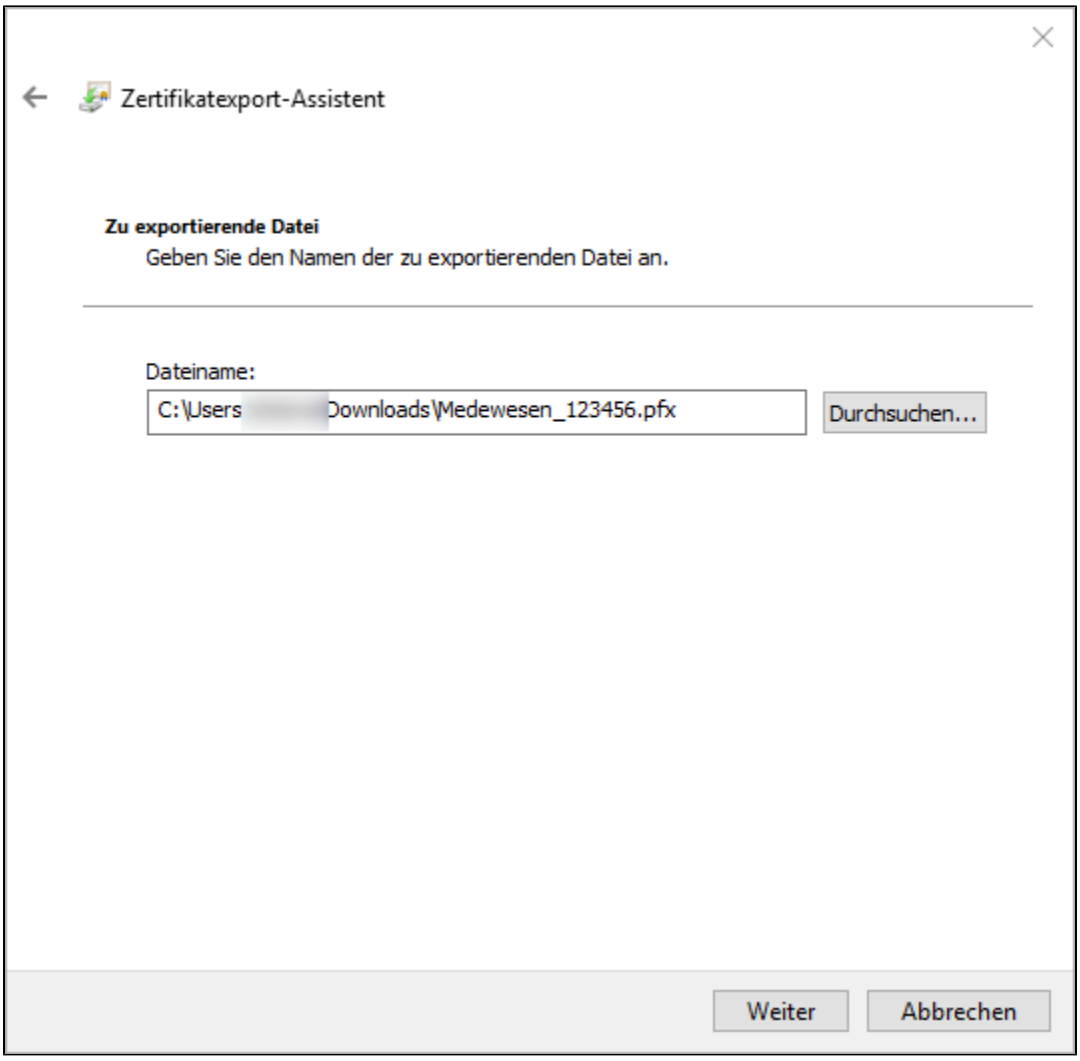
Klicken Sie auf **Durchsuchen**.



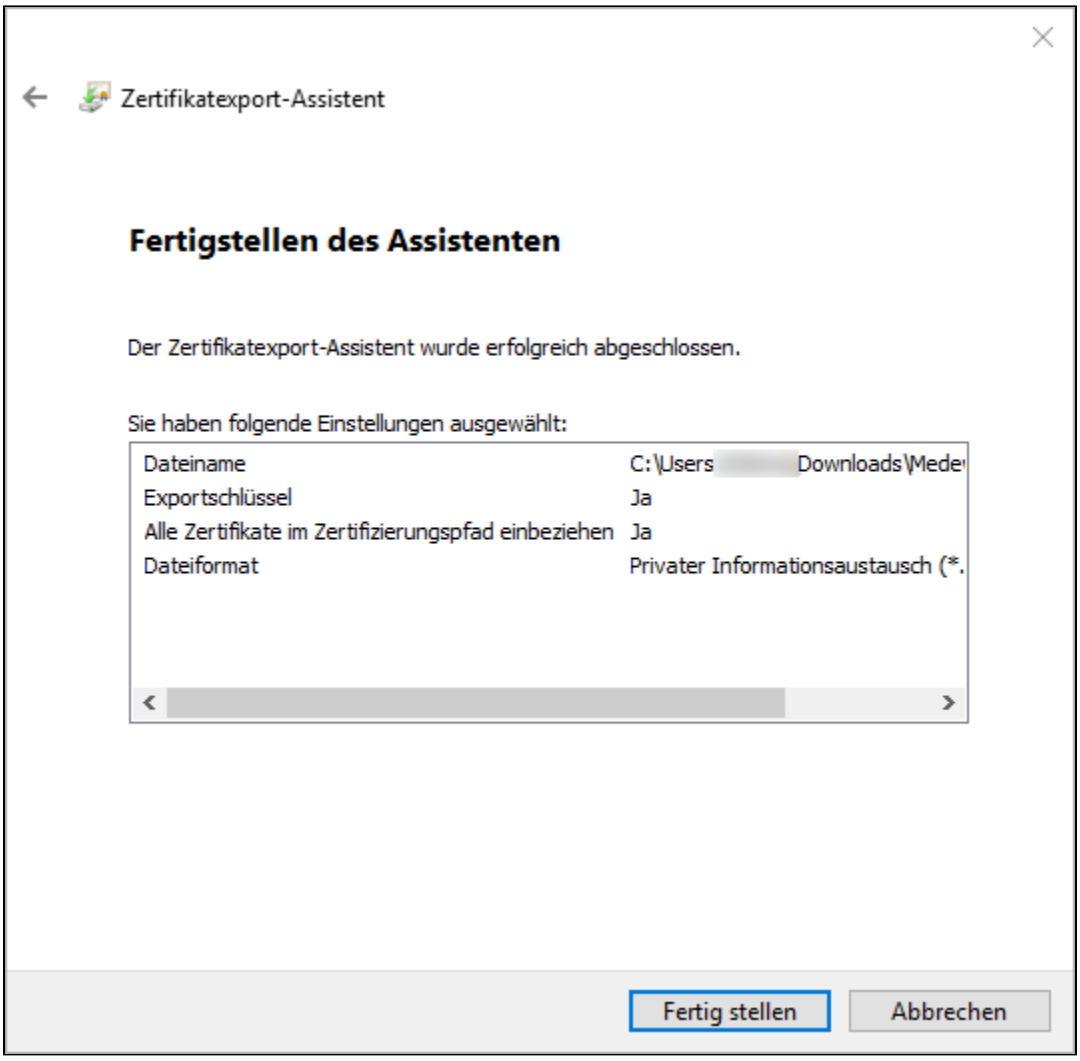
Wählen Sie hier den Speicherort aus, vergeben Sie den Dateinamen und klicken dann auf **Speichern**.



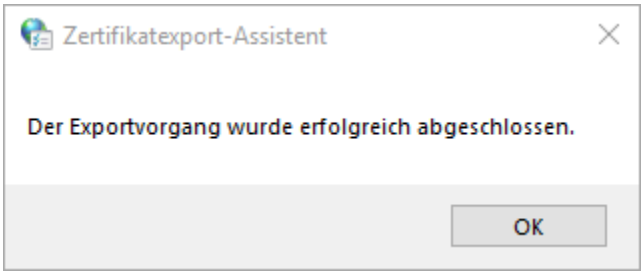
Klicken Sie auf **Weiter**.



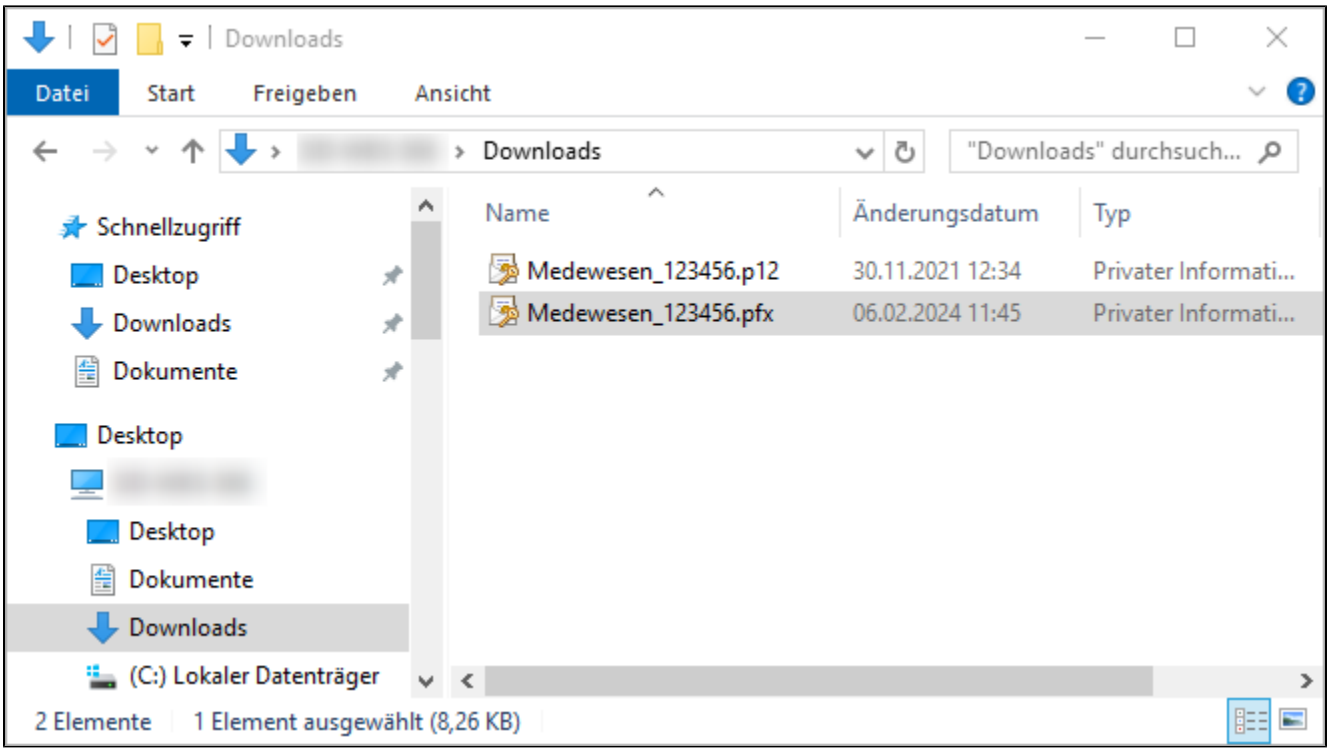
Es werden alle Eingaben eingeblendet. Nach dem Klicken auf "**Fertig stellen"** ist der Exportvorgang abgeschlossen



Der Exportvorgang wurde erfolgreich abgeschlossen. Klicken Sie auf **OK.**



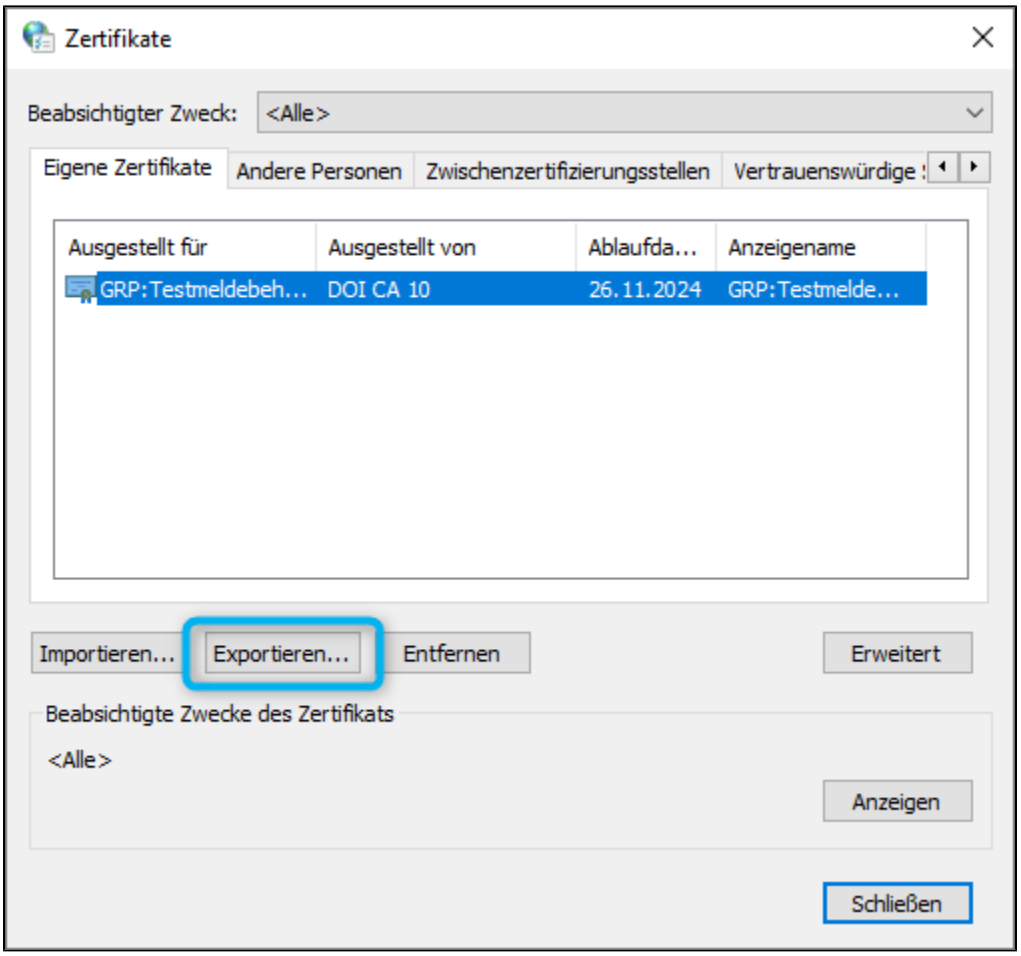
Das neue private Zertifikat "**Medewesen_123456.pfx**" wurde erstellt.



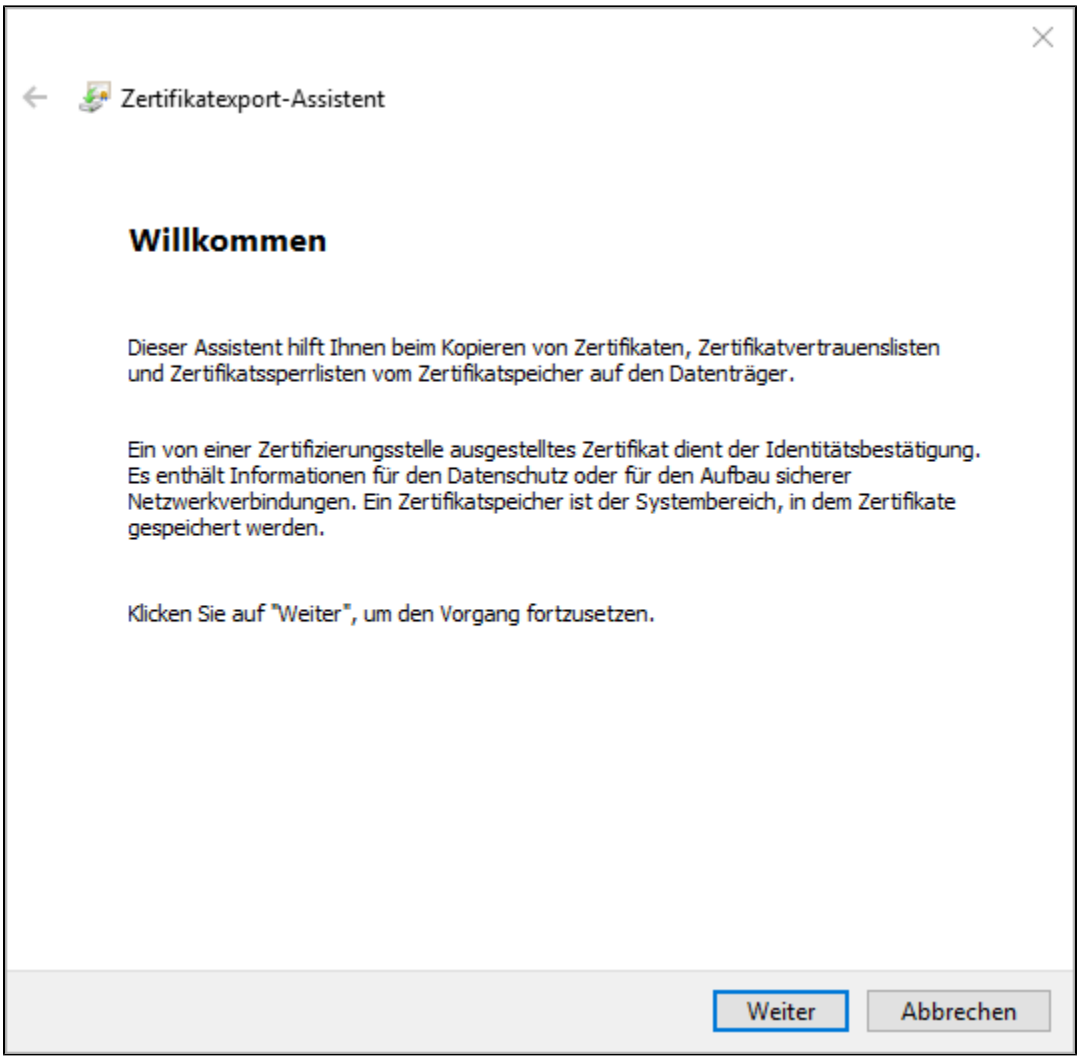
Jeder Person die Zugriff auf diese Dateien hat und das Kennwort kennt, kann im Namen Ihrer Behörde elektronische Unterschriften leisten!

Bitte Handhaben Sie das Zertifikat und die Zertifikatsdaten entsprechend sorgsam.

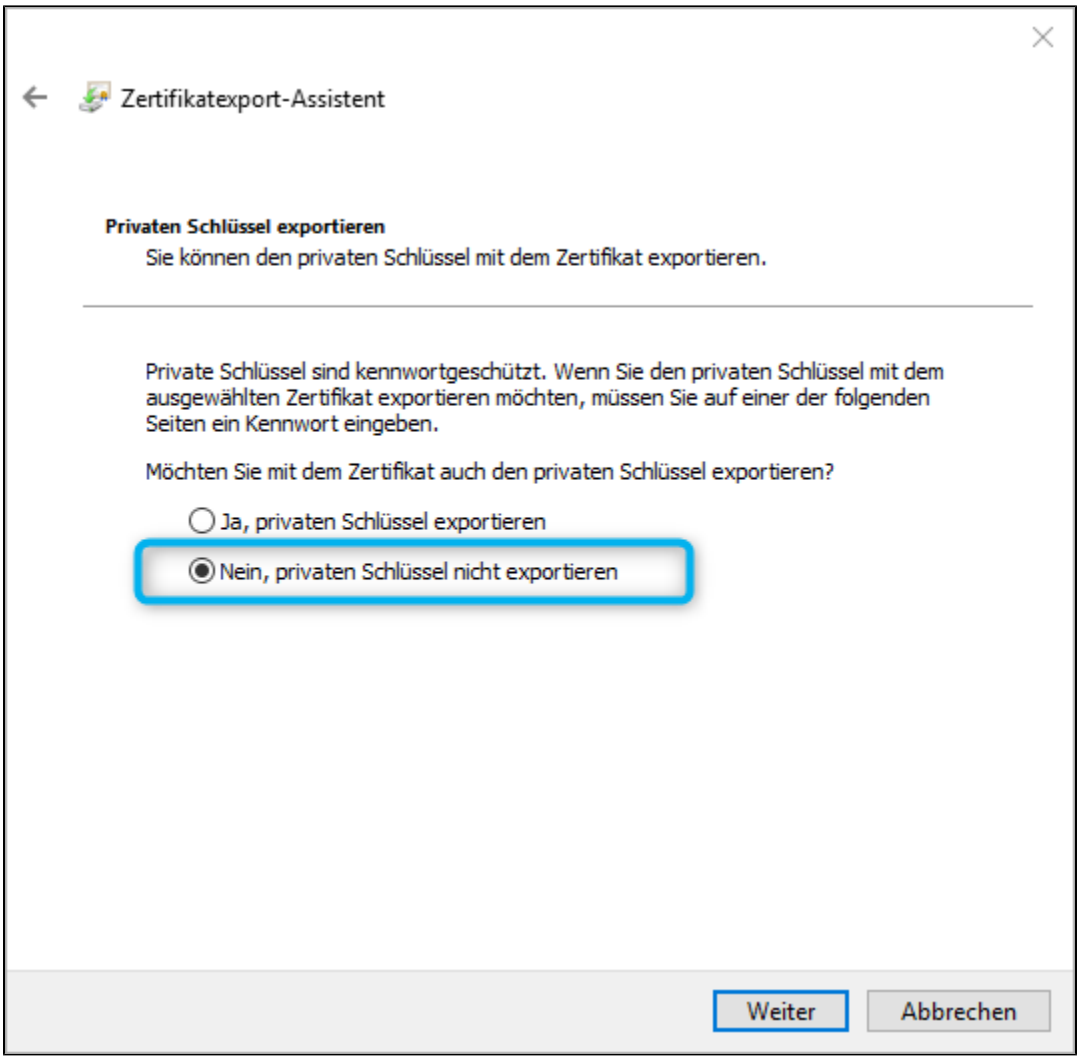
3.2 Export „öffentliches Zertifikat“ aus dem Windows Zertifikatsspeicher



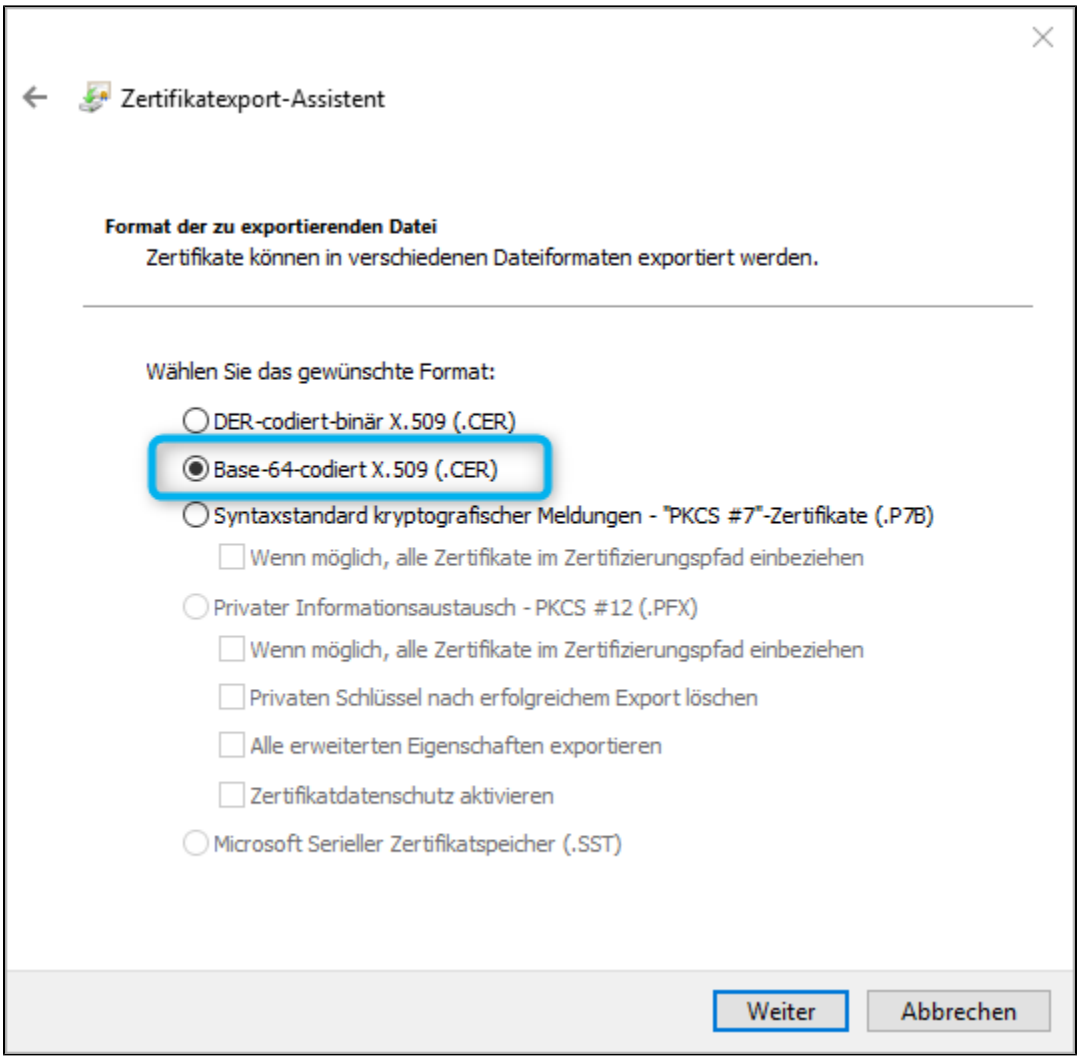
Sie gelangen zum Zertifikatsexport-Assistent. Klicken Sie im Eingangsdialog auf **Weiter**.



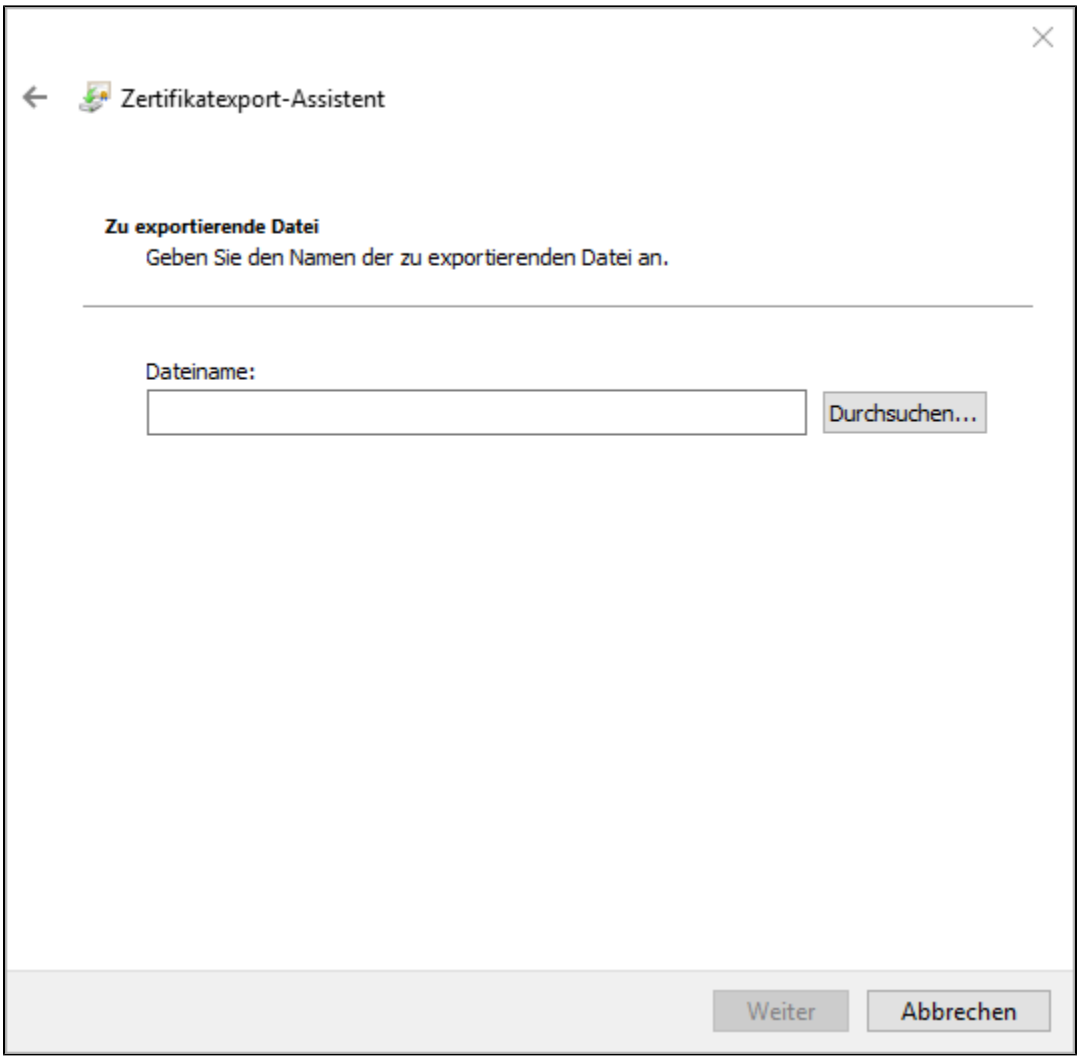
Aktivieren Sie '**Nein, privaten Schlüssel nicht exportieren'** und bestätigen Sie Ihre Auswahl mit **Weiter**.



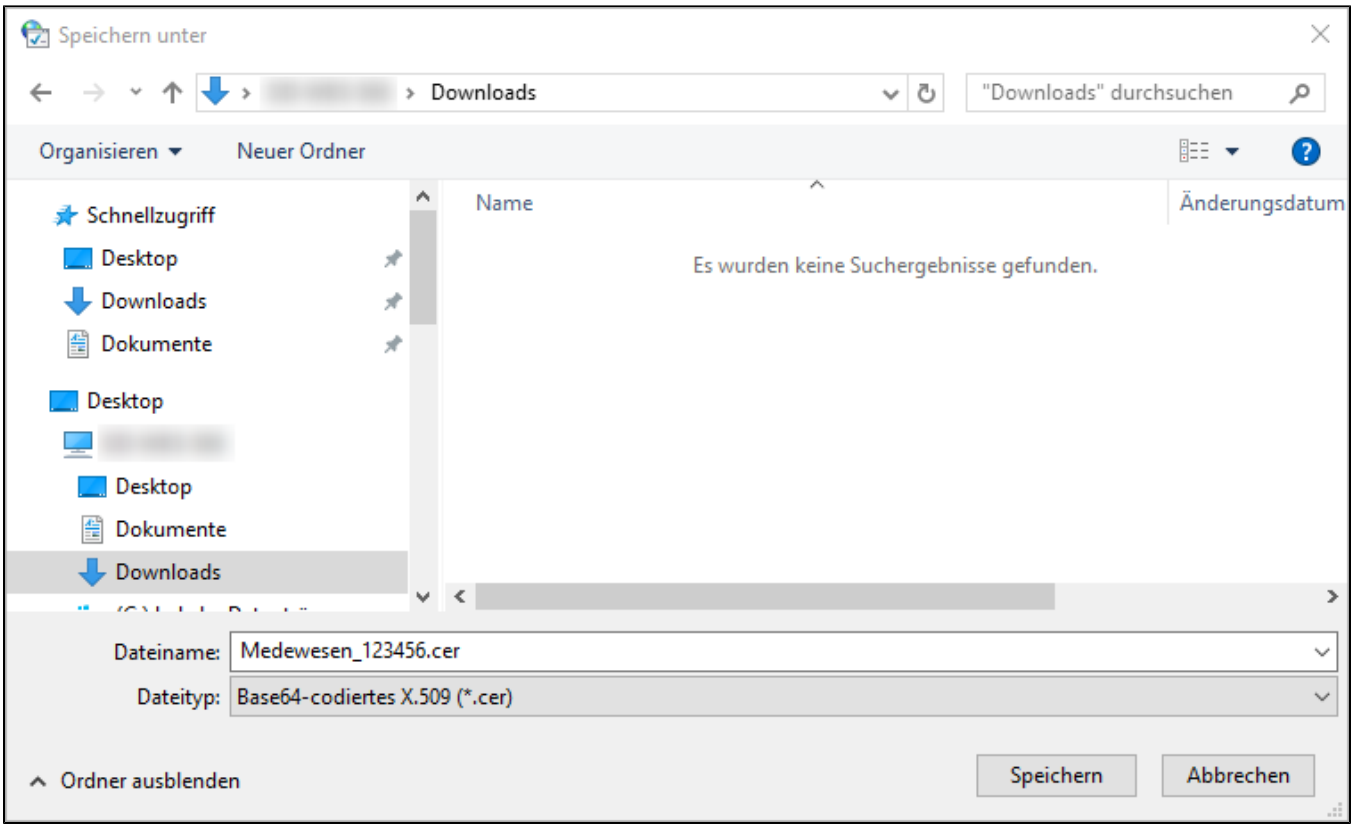
Sie werden nun nach dem Dateiformat gefragt. Aktivieren Sie Base-64-codiert X.509 (.CER) und bestätigen Sie Ihre Auswahl mit **Weiter**.



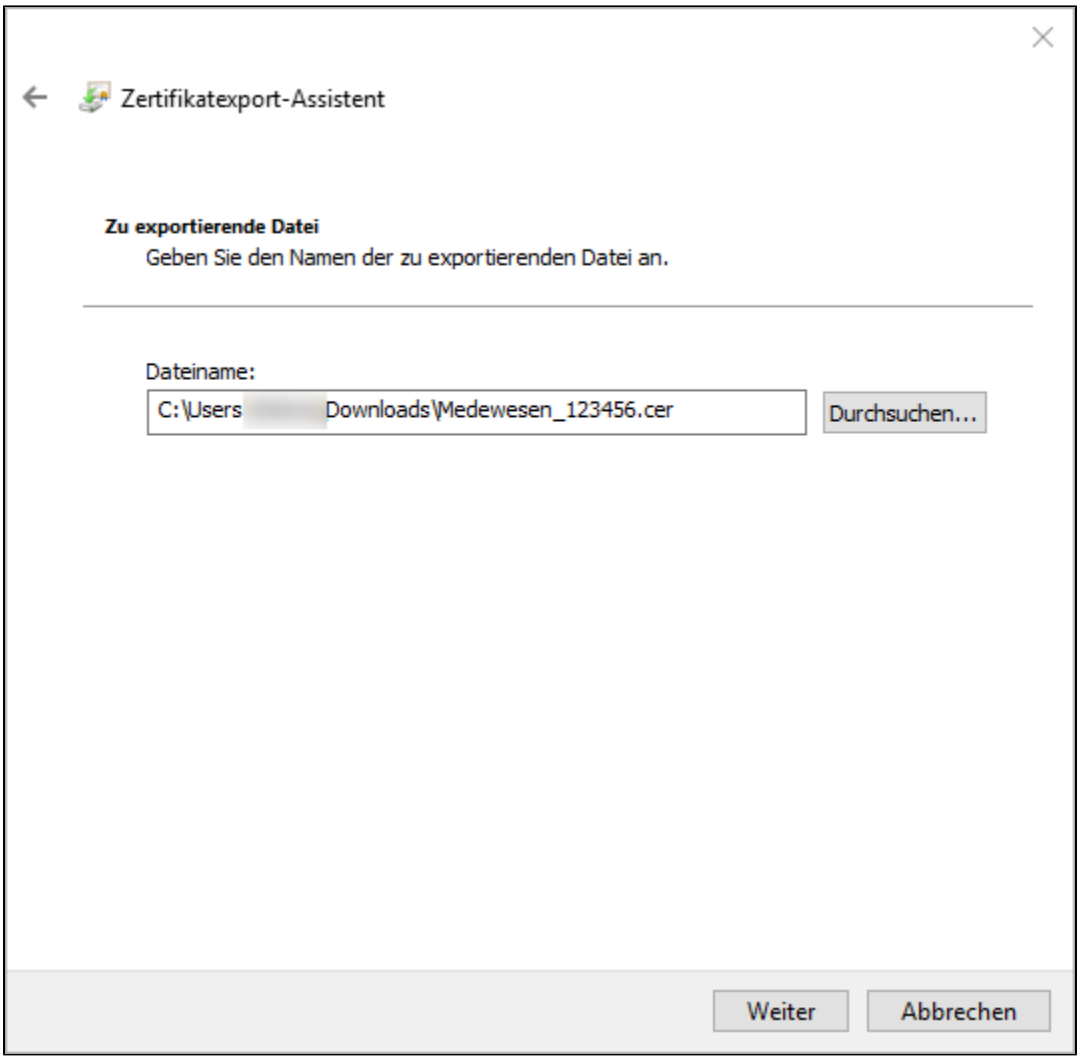
Klicken Sie auf **Durchsuchen**.



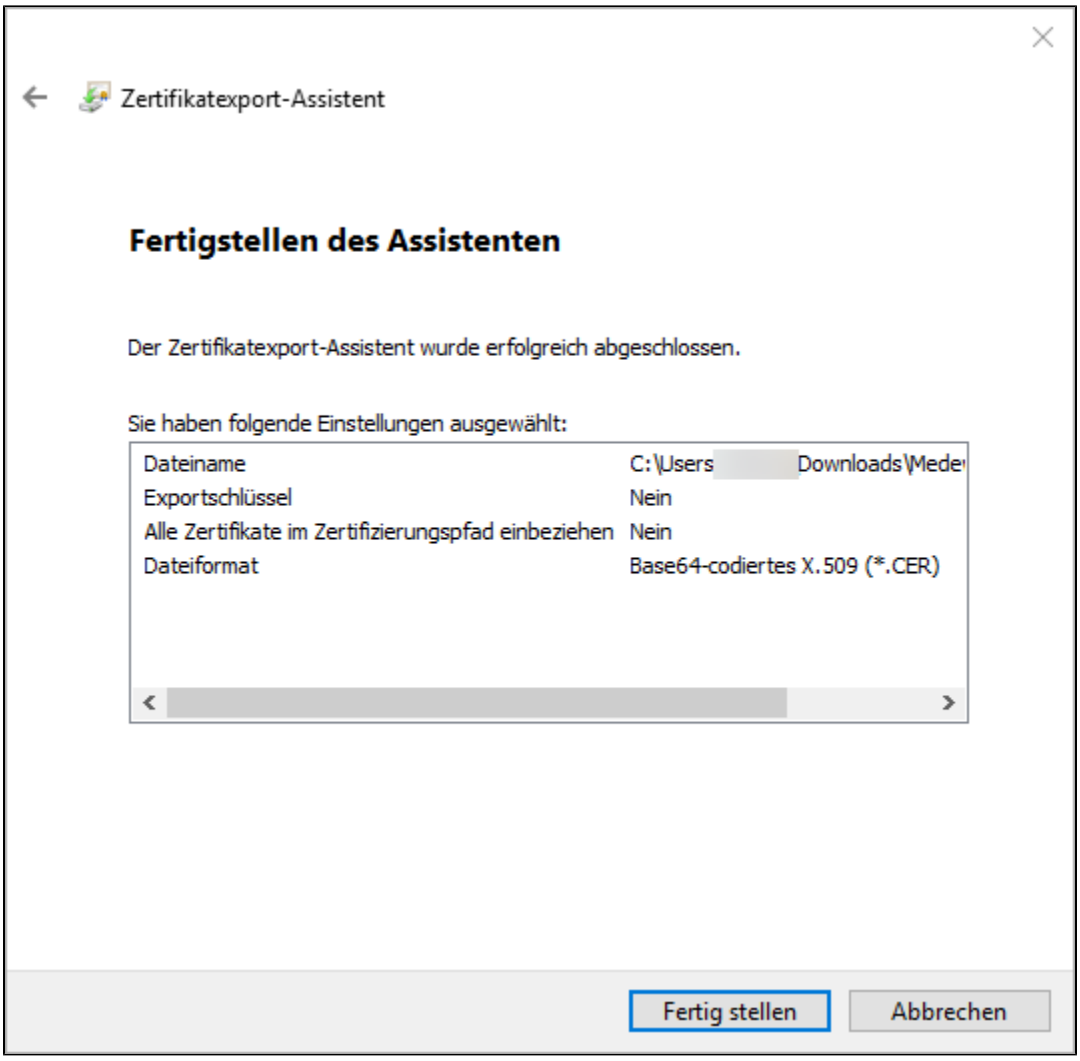
Wählen Sie hier den Speicherort aus, vergeben Sie den Dateinamen und klicken dann auf **Speichern**.



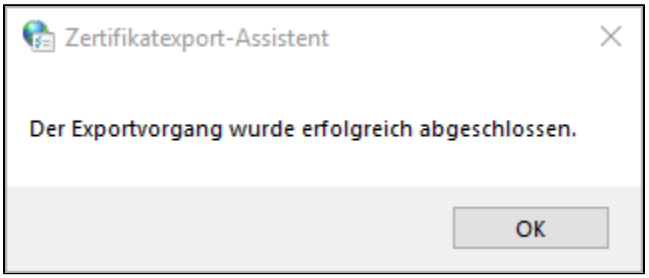
Klicken Sie auf **Weiter**.



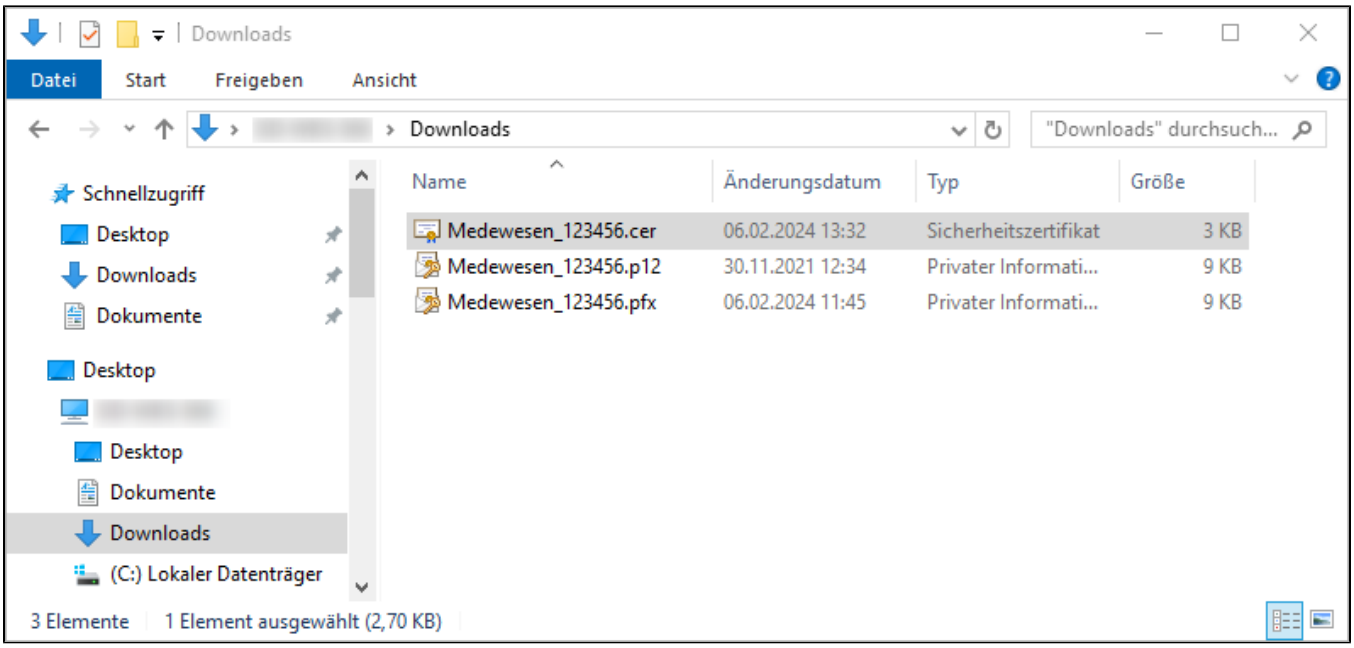
Im nächsten Menü werden Ihnen die Daten noch einmal angezeigt, bestätigen Sie dieses Menü mit "**Fertig stellen**".



Schließlich erhalten Sie eine Meldung, dass der Exportvorgang erfolgreich abgeschlossen wurde, quittieren Sie diese Meldung mit **OK**.



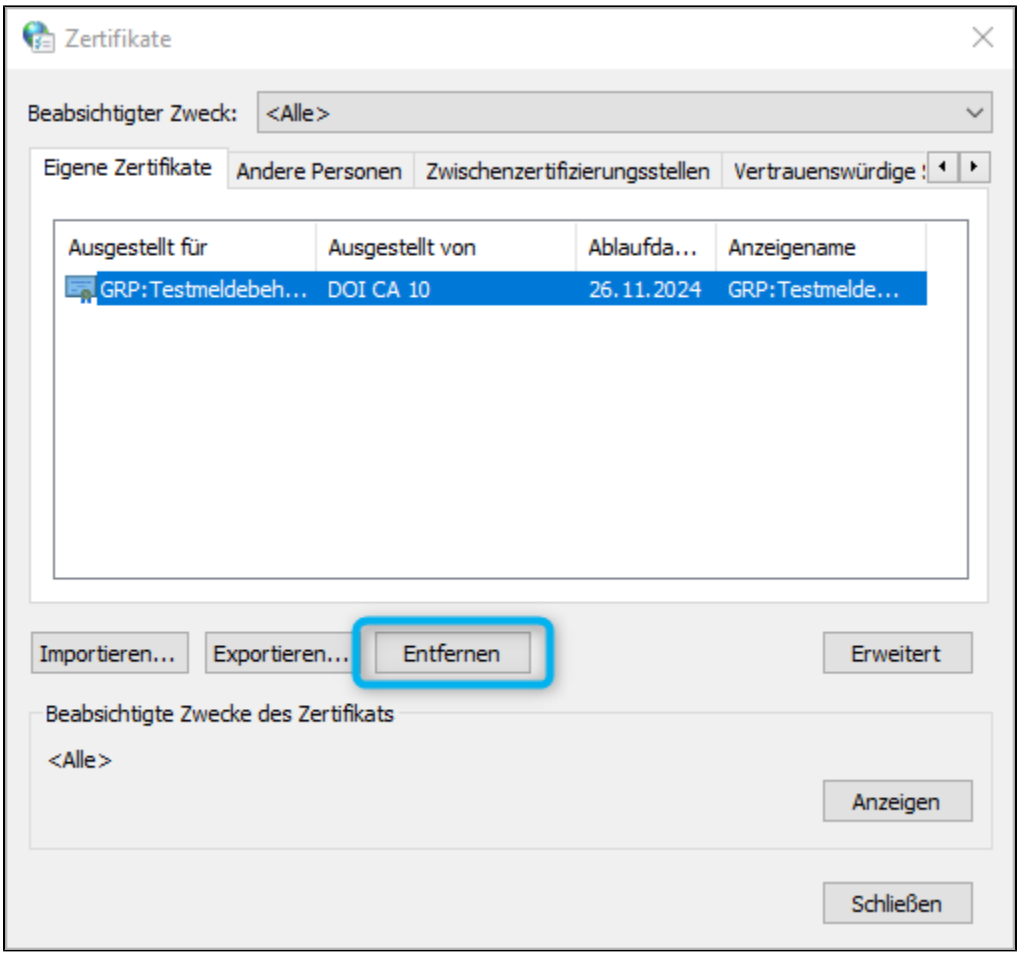
Ihr Zertifikat liegt jetzt in Dateiform in dem von Ihnen gewählten Ordner („*.cer“) vor. Diese Datei können Sie bedenkenlos weitergeben (z.B. für die Veröffentlichung im SaxDVDV bzw. DVDV).



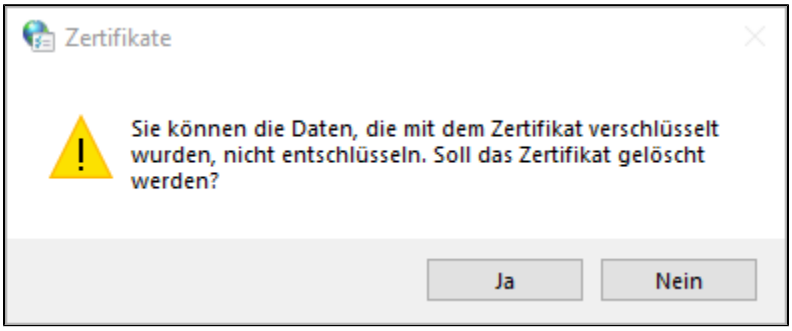
4 Zertifikat löschen

Zum Löschen eines Zertifikats aus dem Windows Zertifikatsspeicher, klicken Sie mit der linken Maustaste auf das zu löschende Zertifikat, sodass es farblich hinterlegt ist. Prüfen Sie nun nochmals, ob Sie dieses Zertifikat löschen möchten.

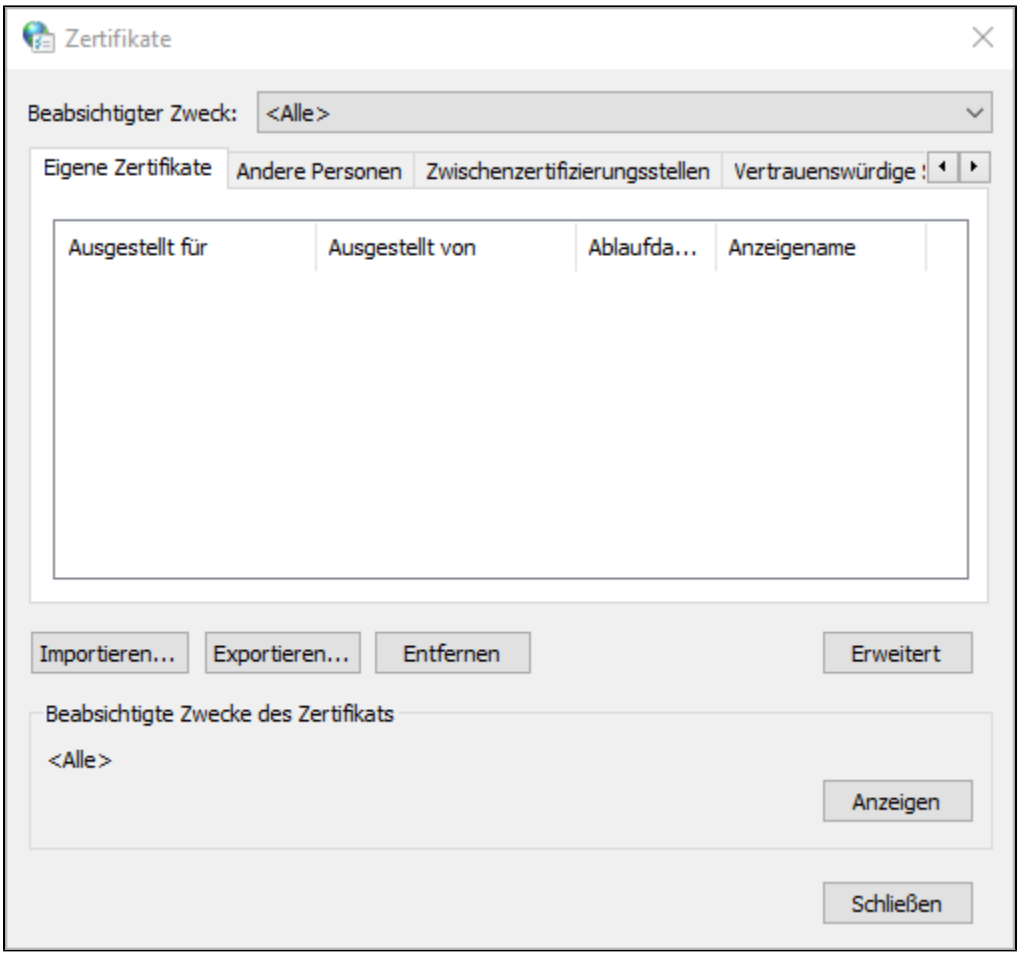
Klicken Sie dann auf **Entfernen**.

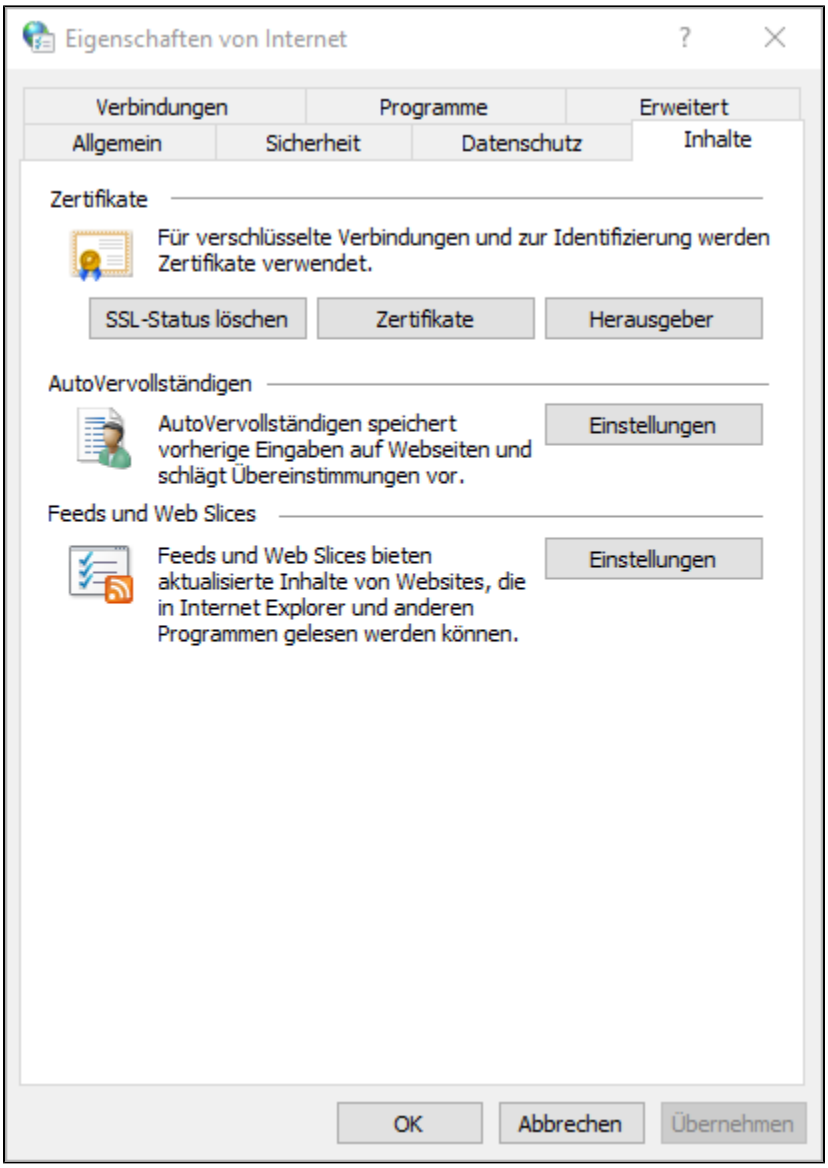


Es wird folgende Abfrage angezeigt. Klicken Sie zum Löschen des Zertifikats auf **Ja**.



Das Zertifikat ist damit gelöscht. Schließen Sie den Windows Zertifikatsspeicher und die Internetoptionen.


Zertifikate
Beabsichtigter Zweck:
<Alle>
Eigene Zertifikate
Andere Personen
Zwischenzertifizierungsstellen
Vertrauenswürdige
Ausgestellt für
Ausgestellt von
Ablaufda...
Anzeigename
Importieren...
Exportieren...
Entfernen
Erweitert
Beabsichtigte Zwecke des Zertifikats
<Alle>
Anzeigen
Schließen


Eigenschaften von Internet
Verbindungen
Programme
Erweitert
Allgemein
Sicherheit
Datenschutz
Inhalte
Zertifikate
Für verschlüsselte Verbindungen und zur Identifizierung werden Zertifikate verwendet.
SSL-Status löschen
Zertifikate
Herausgeber
AutoVervollständigen
AutoVervollständigen speichert vorherige Eingaben auf Webseiten und schlägt Übereinstimmungen vor.
Einstellungen
Feeds und Web Slices
Feeds und Web Slices bieten aktualisierte Inhalte von Websites, die in Internet Explorer und anderen Programmen gelesen werden können.
Einstellungen
OK
Abbrechen
Übernehmen

ENDE