

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

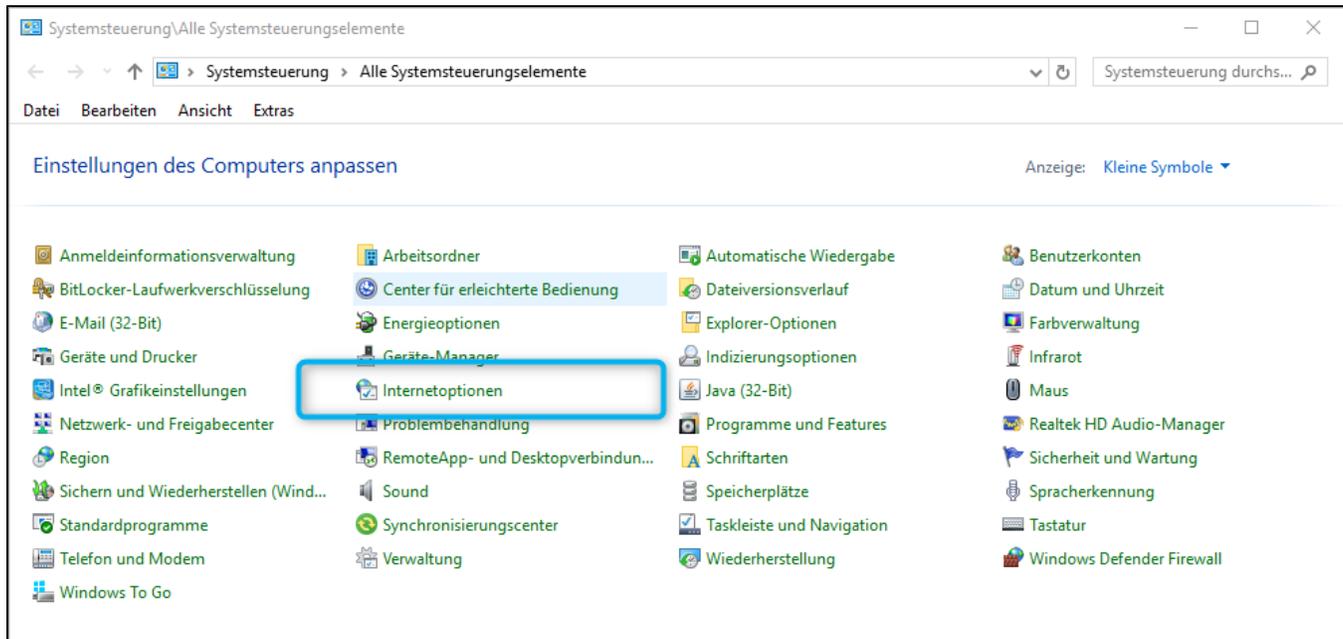
- Anleitung zum Stand - 21.02.2024
 - erstellt durch den
 - Staatsbetrieb Sächsische Informatik Dienste
- 1 Windows-Zertifikatsspeicher öffnen
- 2 Zertifikat (*.p12) importieren
- 3 Zertifikat exportieren
 - 3.1 Export „privates Zertifikat“ aus dem Windows Zertifikatsspeicher
 - 3.2 Export „öffentliches Zertifikat“ aus dem Windows Zertifikatsspeicher
- 4 Zertifikat löschen

1 Windows-Zertifikatsspeicher öffnen

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

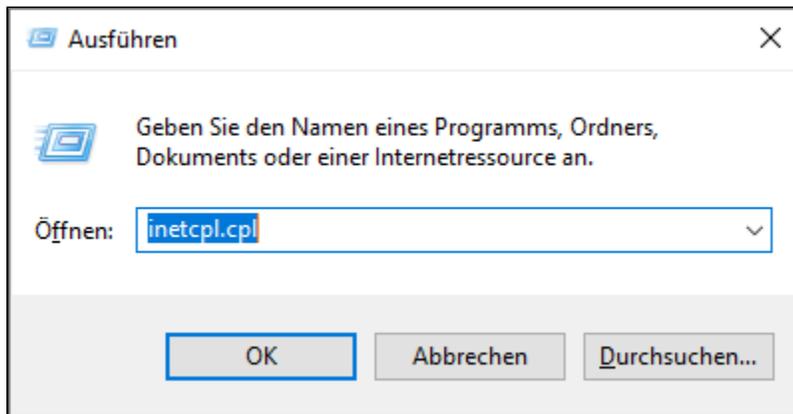
Der Windows-Zertifikatsspeicher kann über die Internetoptionen erreicht werden.

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

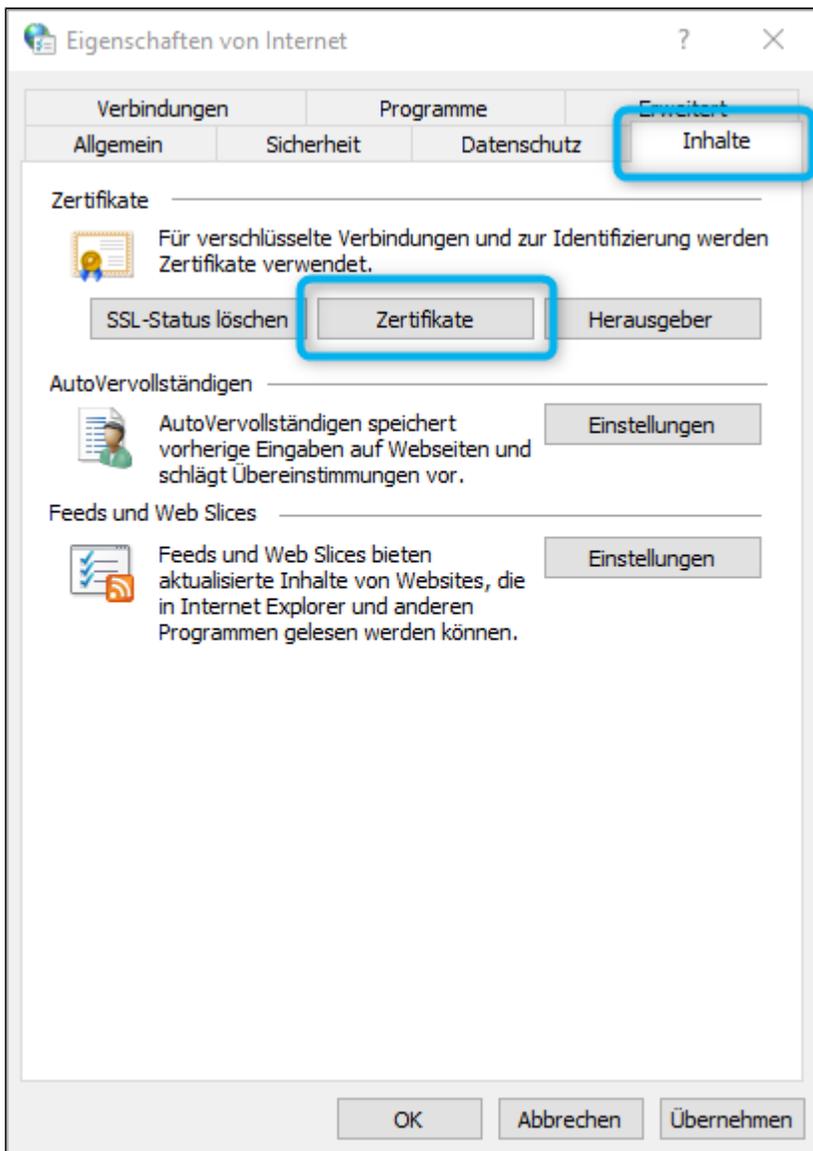


oder

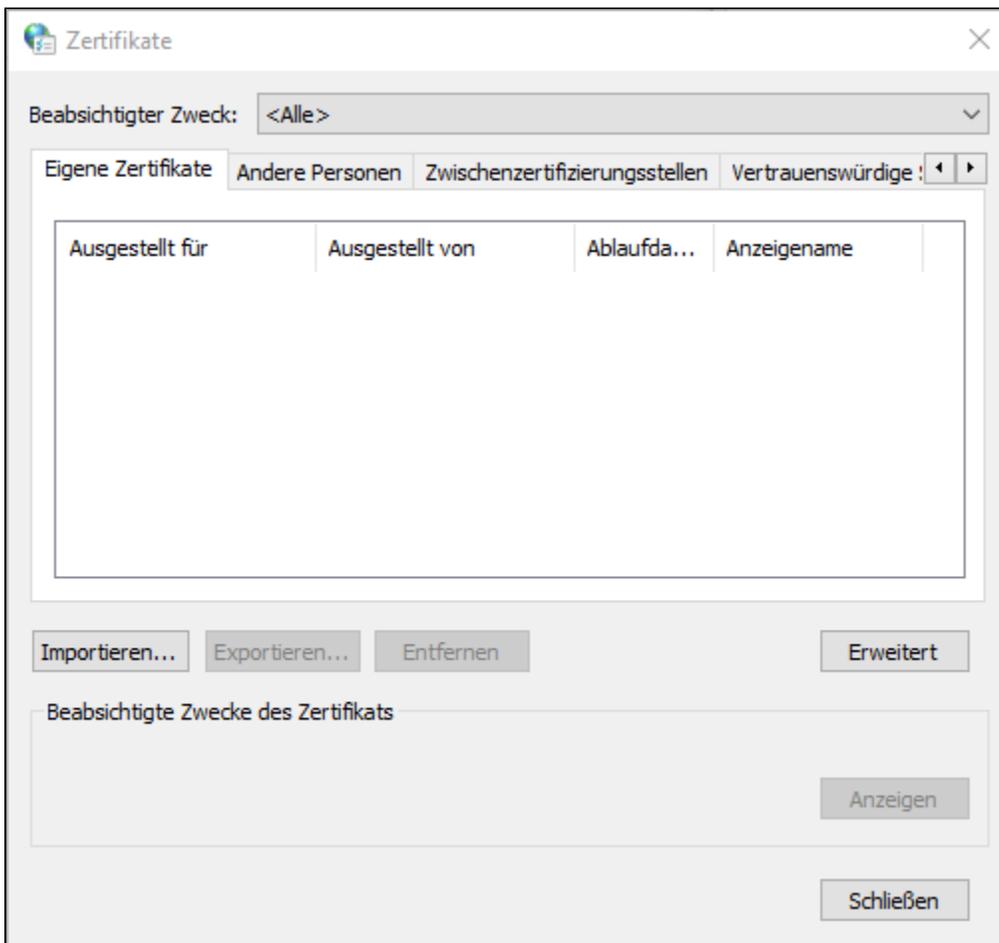
Starten Sie den "Ausführen Dialog" mit [**Windows +R**]. Geben Sie dazu den Befehl: **inetcpl.cpl** ein und schließen mit der [Taste Enter] oder '**OK**' ab.



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

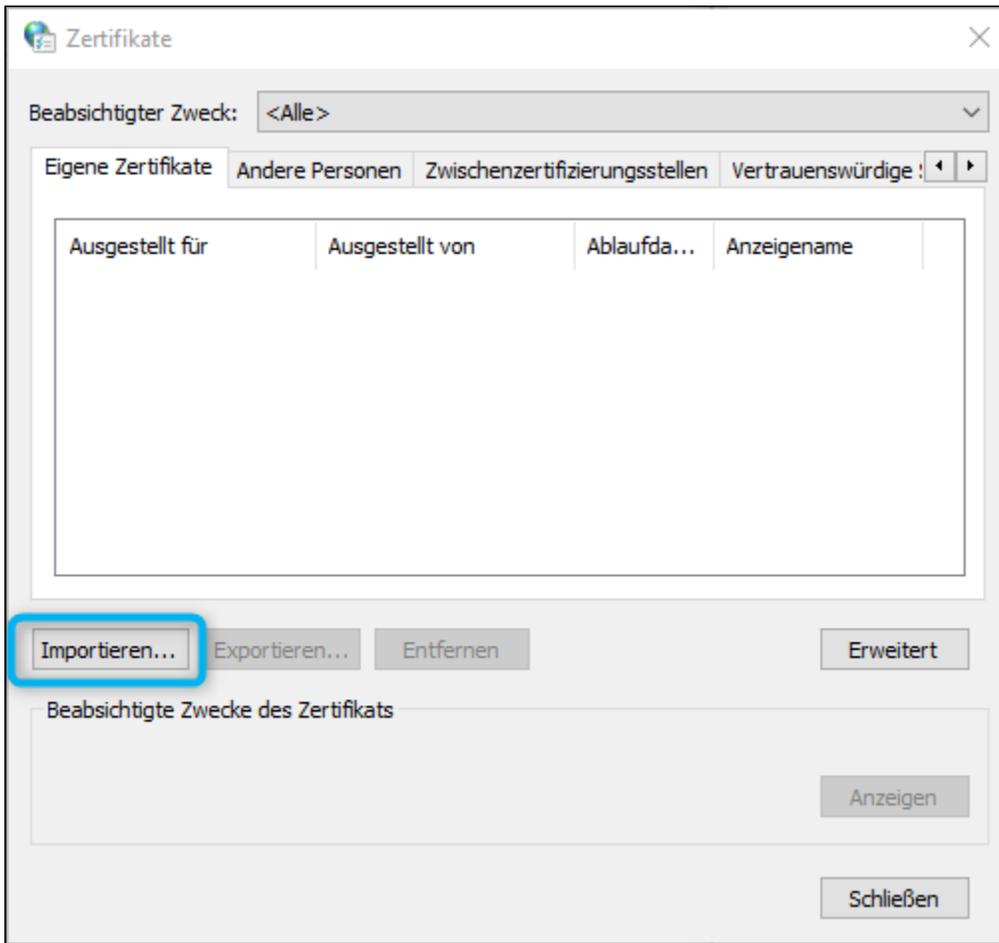


Daraufhin sehen Sie eine Übersicht der bereits installierten Zertifikate im Zertifikatsspeicher. Wenn noch keine eigenen Zertifikate installiert sind, existieren keine Einträge.



2 Zertifikat (*.p12) importieren

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



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



←  Zertifikatimport-Assistent

Willkommen

Dieser Assistent hilft Ihnen beim Kopieren von Zertifikaten, Zertifikatvertrauenslisten und Zertifikatssperrlisten vom Datenträger in den Zertifikatspeicher.

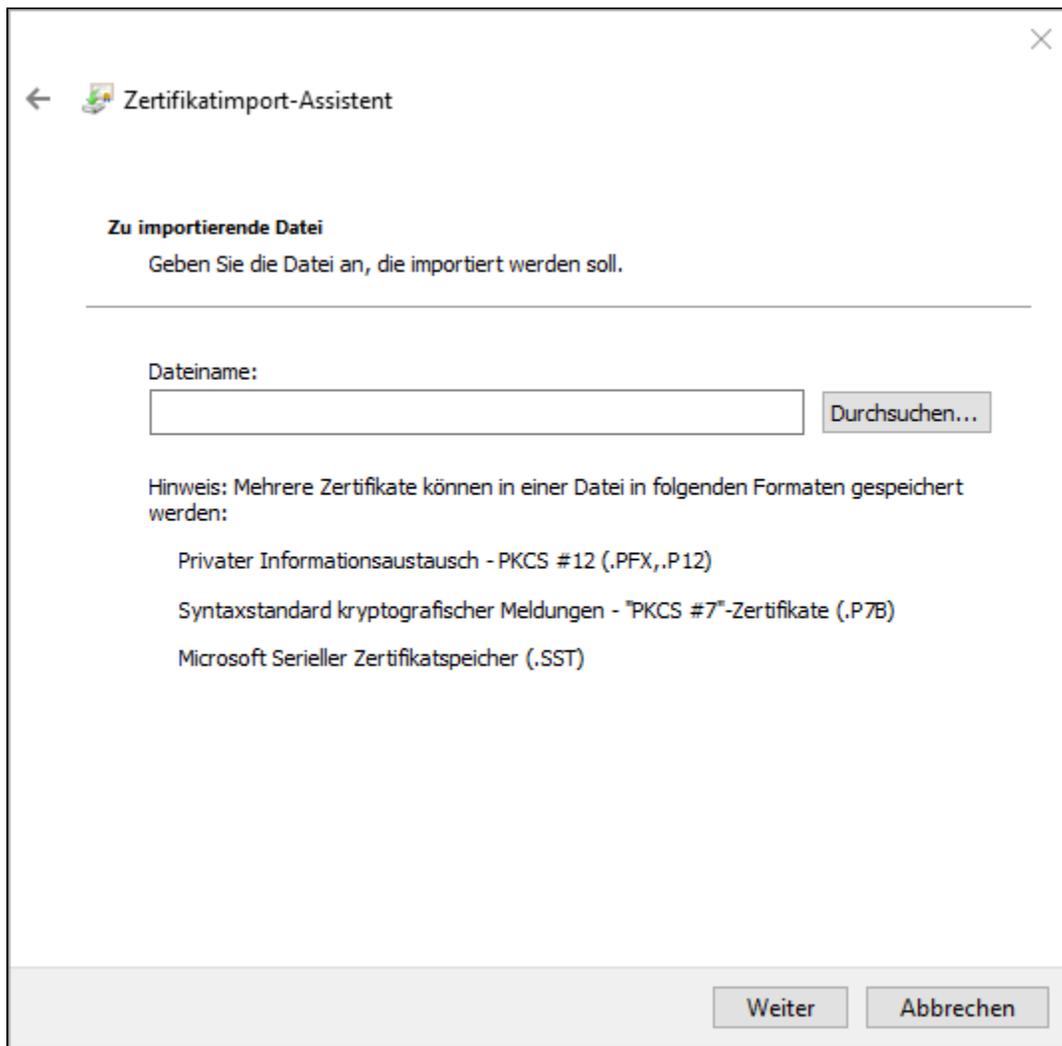
Ein von einer Zertifizierungsstelle ausgestelltes Zertifikat dient der Identitätsbestätigung. Es enthält Informationen für den Datenschutz oder für den Aufbau sicherer Netzwerkverbindungen. Ein Zertifikatspeicher ist der Systembereich, in dem Zertifikate gespeichert werden.

Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.

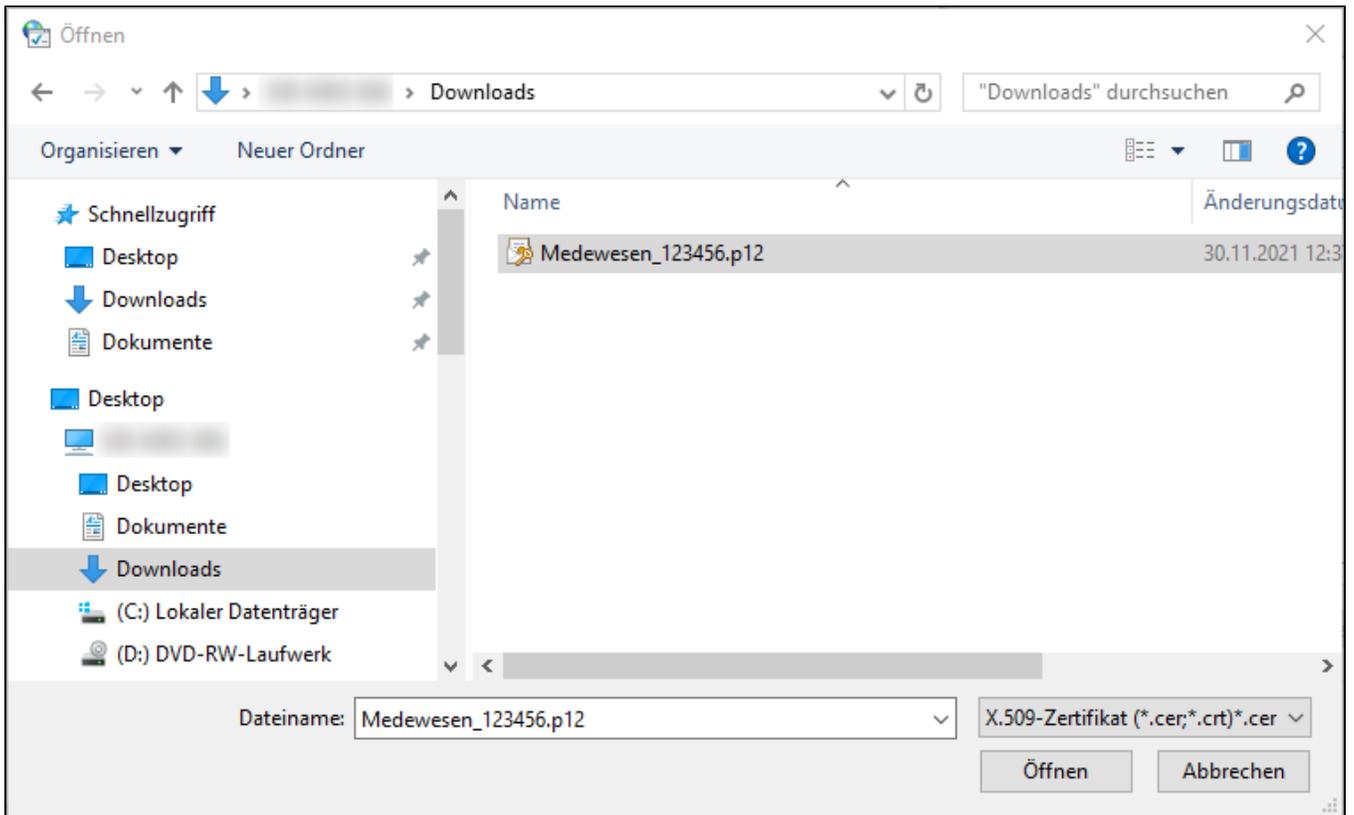
Weiter

Abbrechen

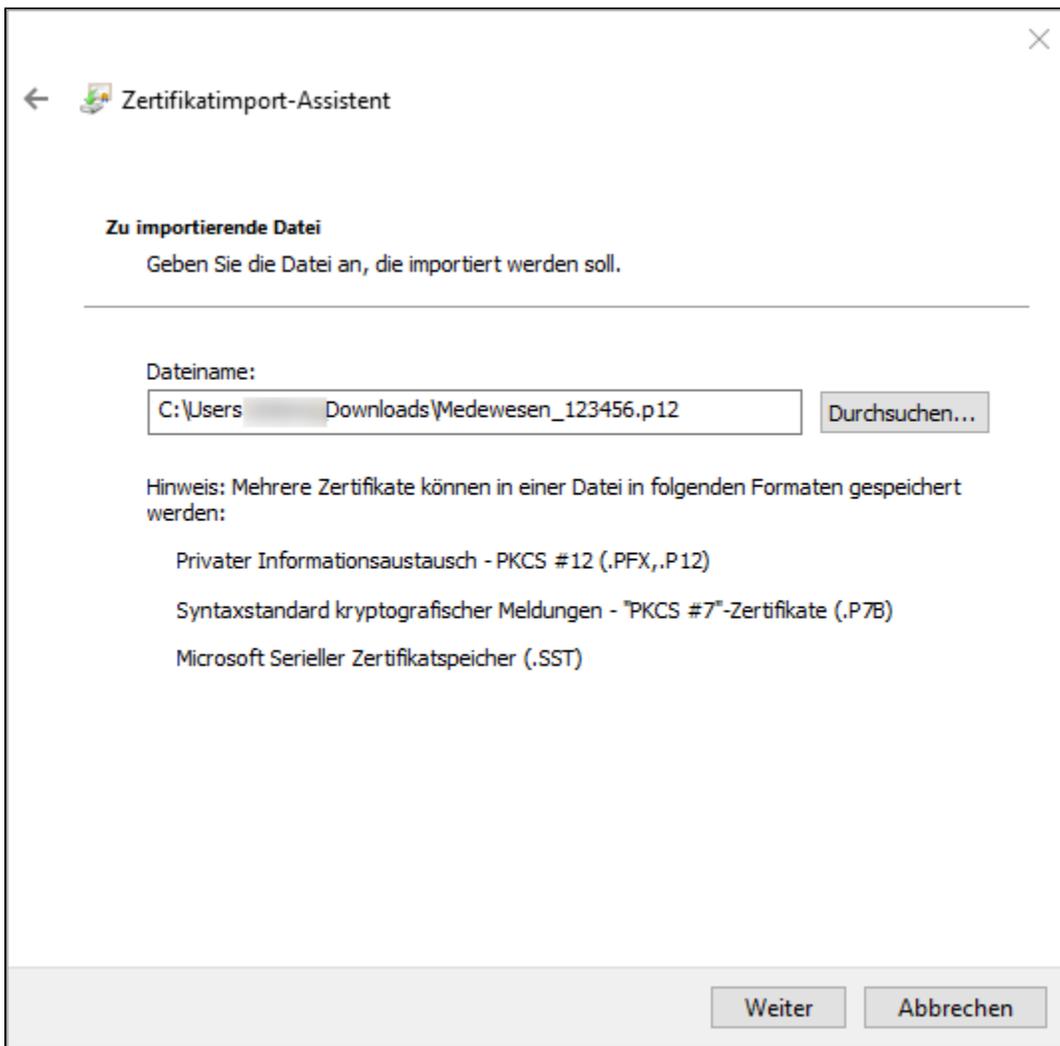
Der Zertifikatsimport-Assistent fordert Sie zur Auswahl der zu importierenden Zertifikatsdatei auf. Sie können den kompletten Dateipfad direkt eingeben oder durch Klicken auf **Durchsuchen** die Dateiauswahlbox benutzen.



Wählen Sie den Datenträger aus und öffnen Sie dann ggf. das Verzeichnis, in dem das Zertifikat gespeichert ist. Wählen Sie dann das Zertifikat aus, das 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**.

←  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.

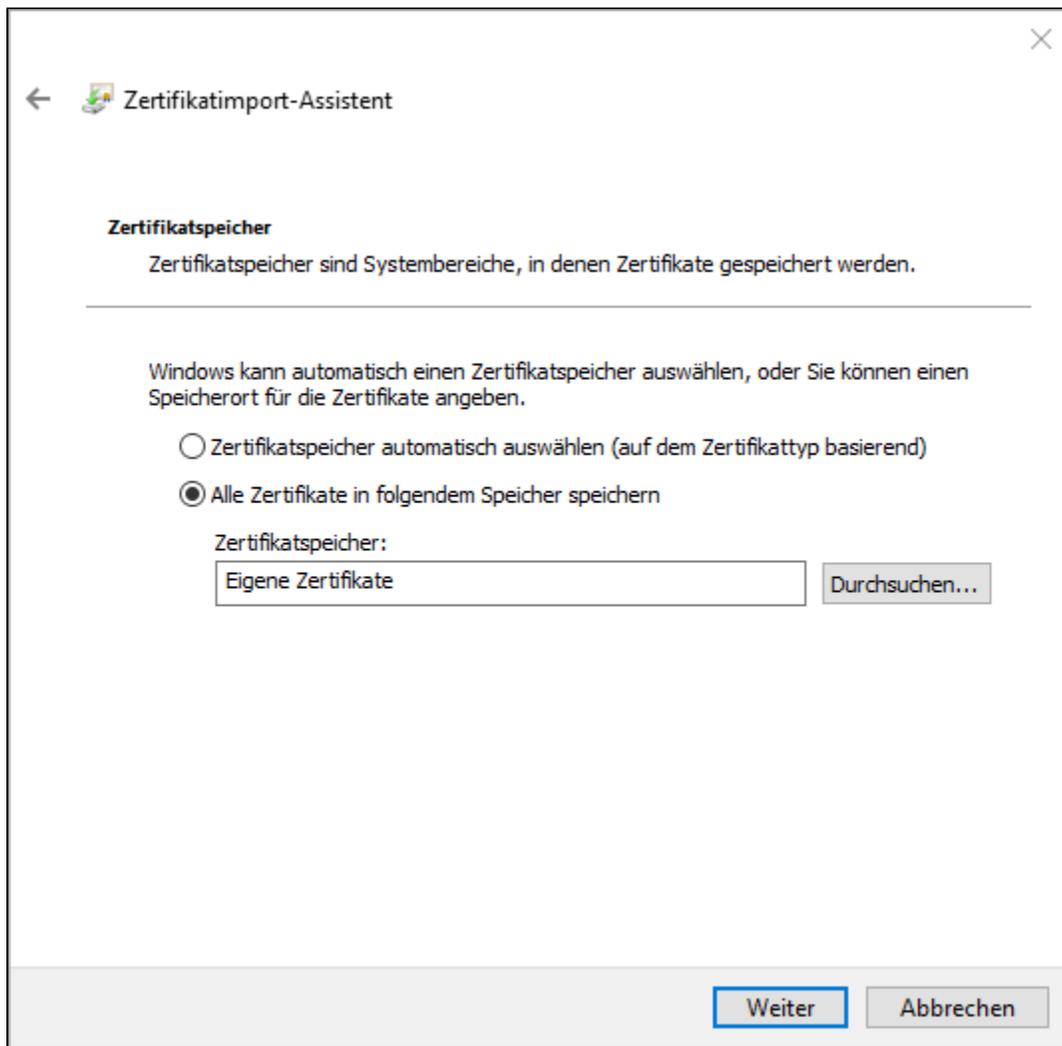
Kennwort:

Kennwort anzeigen

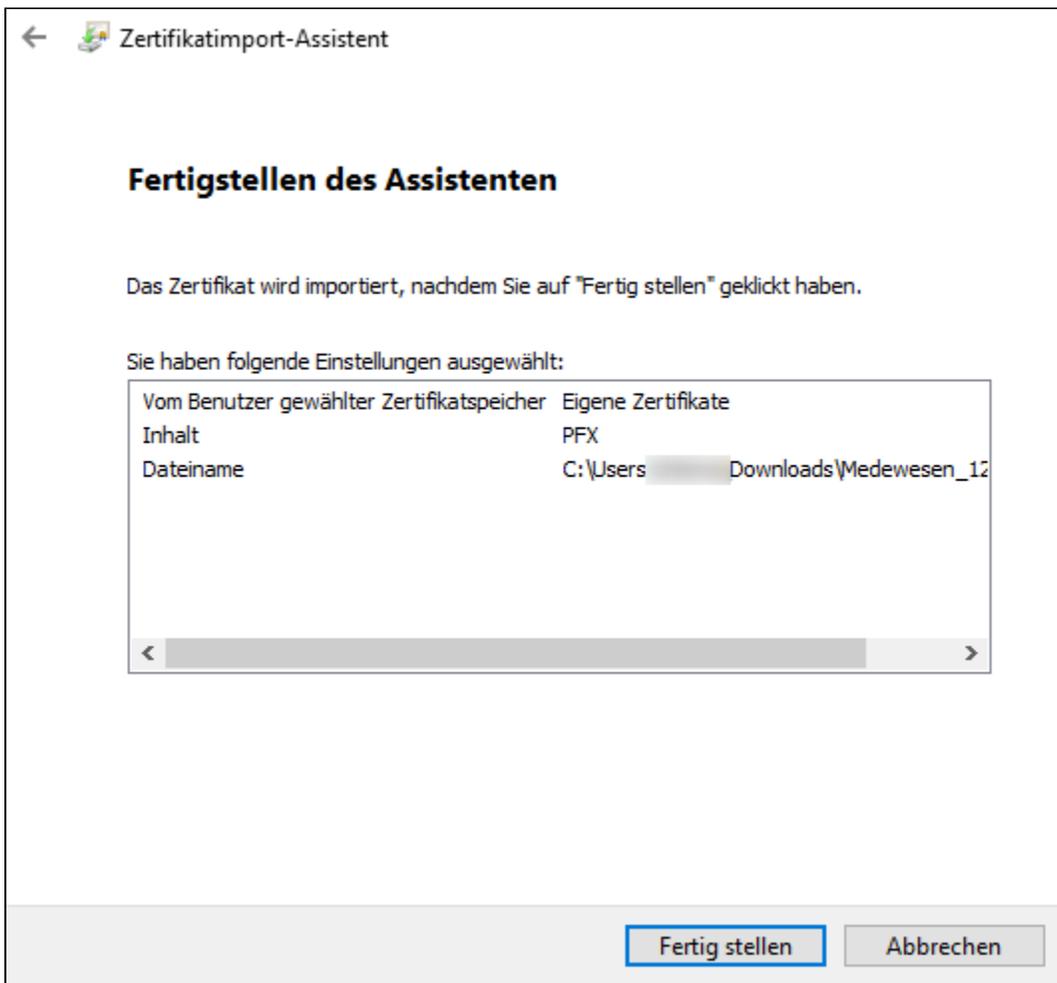
Importoptionen:

- 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

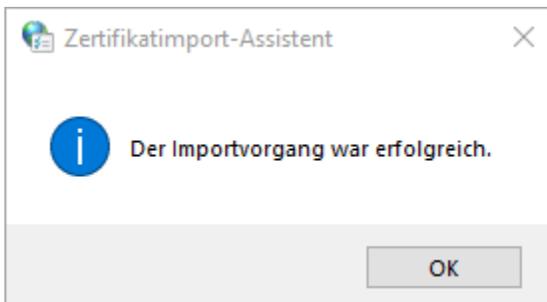
Anschließend können Sie noch den Zertifikatsspeicher auswählen. Für das hier beschriebene Zertifikat wählen Sie den Zertifikatsspeicher "Eigene Zertifikate". Klicken Sie dann auf **Weiter**.



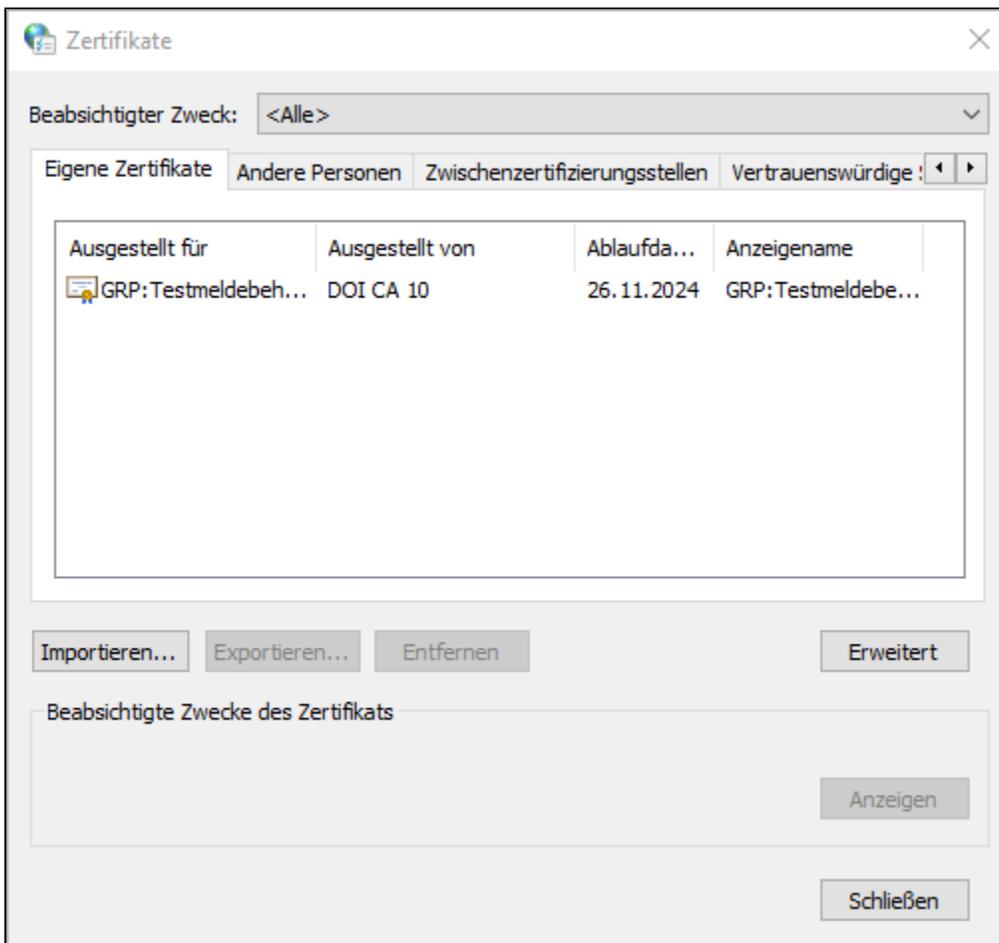
Die Installation wird abgeschlossen. Klicken Sie jetzt auf "**Fertig stellen**".



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.

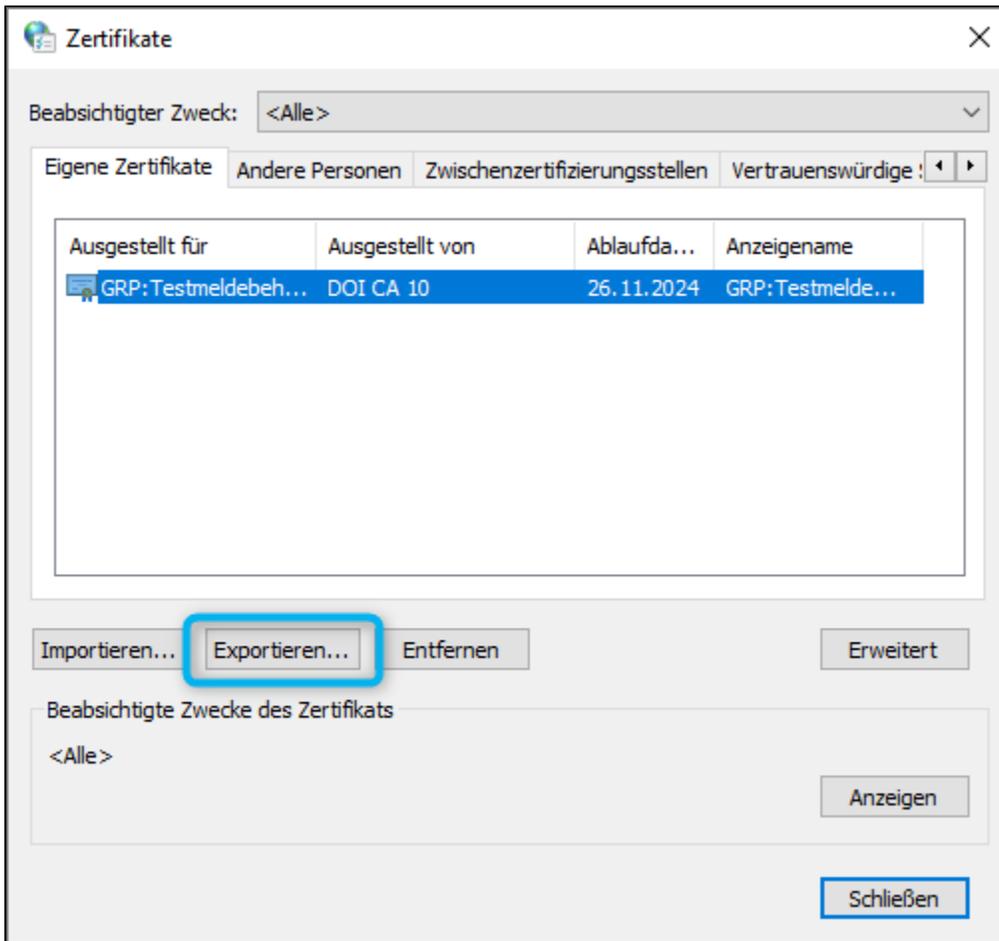
Um Ihr Zertifikat in weiteren Anwendungen aktiv verwenden zu können, müssen Sie Ihren privaten Schlüssel und alle Zertifikate im Zertifizierungspfad exportieren. Sie erhalten dabei eine Datei mit der Endung „.pfx“ bzw. „.p12“.

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**.



Zertifikatexport-Assistent

Willkommen

Dieser Assistent hilft Ihnen beim Kopieren von Zertifikaten, Zertifikatvertrauenslisten und Zertifikatssperlisten vom Zertifikatspeicher auf den Datenträger.

Ein von einer Zertifizierungsstelle ausgestelltes Zertifikat dient der Identitätsbestätigung. Es enthält Informationen für den Datenschutz oder für den Aufbau sicherer Netzwerkverbindungen. Ein Zertifikatspeicher ist der Systembereich, in dem Zertifikate gespeichert werden.

Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.

Weiter

Abbrechen

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



Privaten Schlüssel exportieren

Sie können den privaten Schlüssel mit dem Zertifikat exportieren.

Private Schlüssel sind kennwortgeschützt. Wenn Sie den privaten Schlüssel mit dem ausgewählten Zertifikat exportieren möchten, müssen Sie auf einer der folgenden Seiten ein Kennwort eingeben.

Möchten Sie mit dem Zertifikat auch den privaten Schlüssel exportieren?

Ja, privaten Schlüssel exportieren

Nein, privaten Schlüssel nicht exportieren

Weiter

Abbrechen

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

←  Zertifikatexport-Assistent ×

Format der zu exportierenden Datei
Zertifikate können in verschiedenen Dateiformaten exportiert werden.

Wählen Sie das gewünschte Format:

- DER-codiert-binär X.509 (.CER)
- Base-64-codiert X.509 (.CER)
- Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)
 - Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
- Privater Informationsaustausch - PKCS #12 (.PFX)
 - Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
 - Privaten Schlüssel nach erfolgreichem Export löschen
 - Alle erweiterten Eigenschaften exportieren
 - Zertifikatdatenschutz aktivieren
- Microsoft Serieller Zertifikatspeicher (.SST)

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**.



Sicherheit

Zur Gewährleistung der Sicherheit müssen Sie den privaten Schlüssel mit einem Sicherheitsprinzipal oder mithilfe eines Kennworts schützen.

Gruppen- oder Benutzernamen (empfohlen)

Hinzufügen

Entfernen

Kennwort:

●●●●●●●●

Kennwort bestätigen:

●●●●●●●●

Verschlüsselung: TripleDES-SHA1 ▾

Weiter

Abbrechen

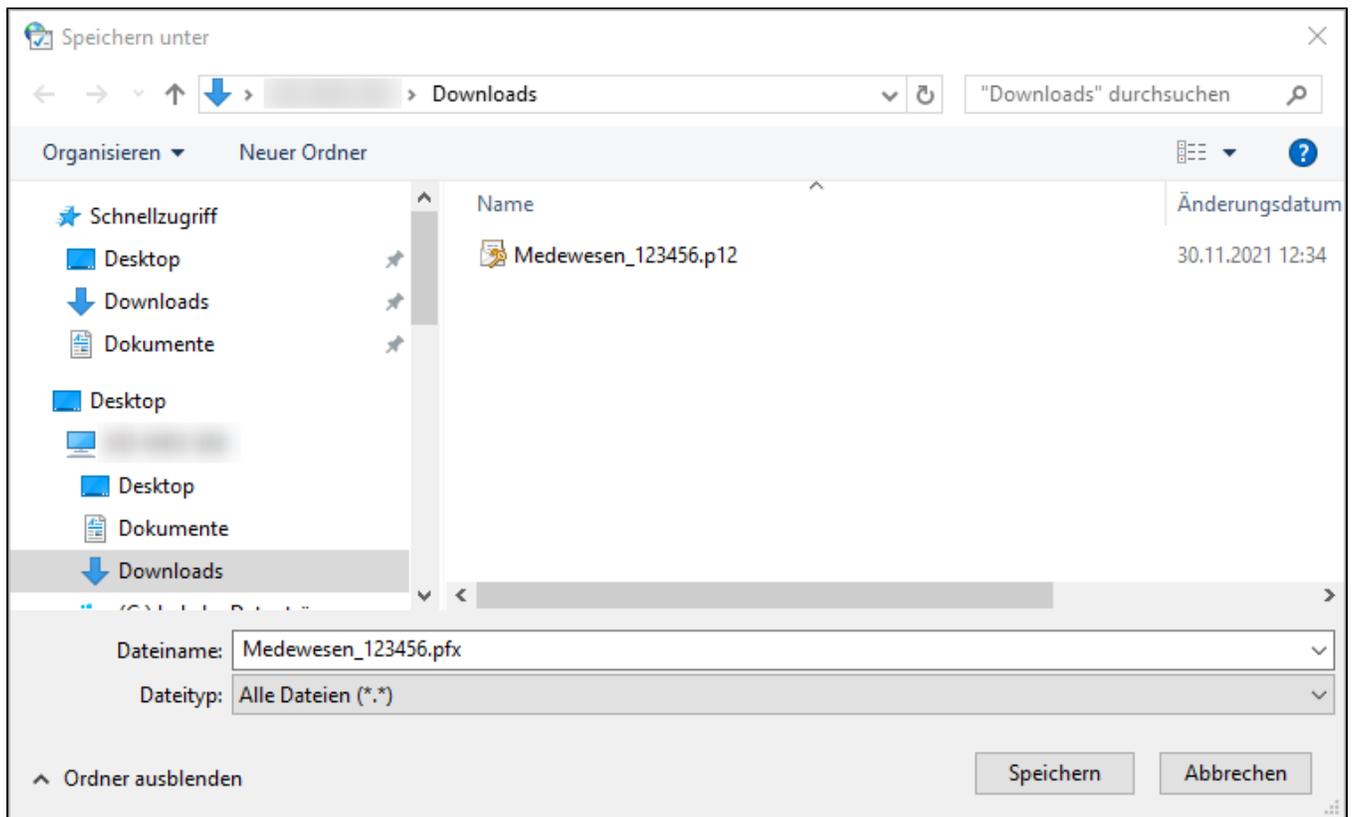
Klicken Sie auf **Durchsuchen**.

←  Zertifikatexport-Assistent ×

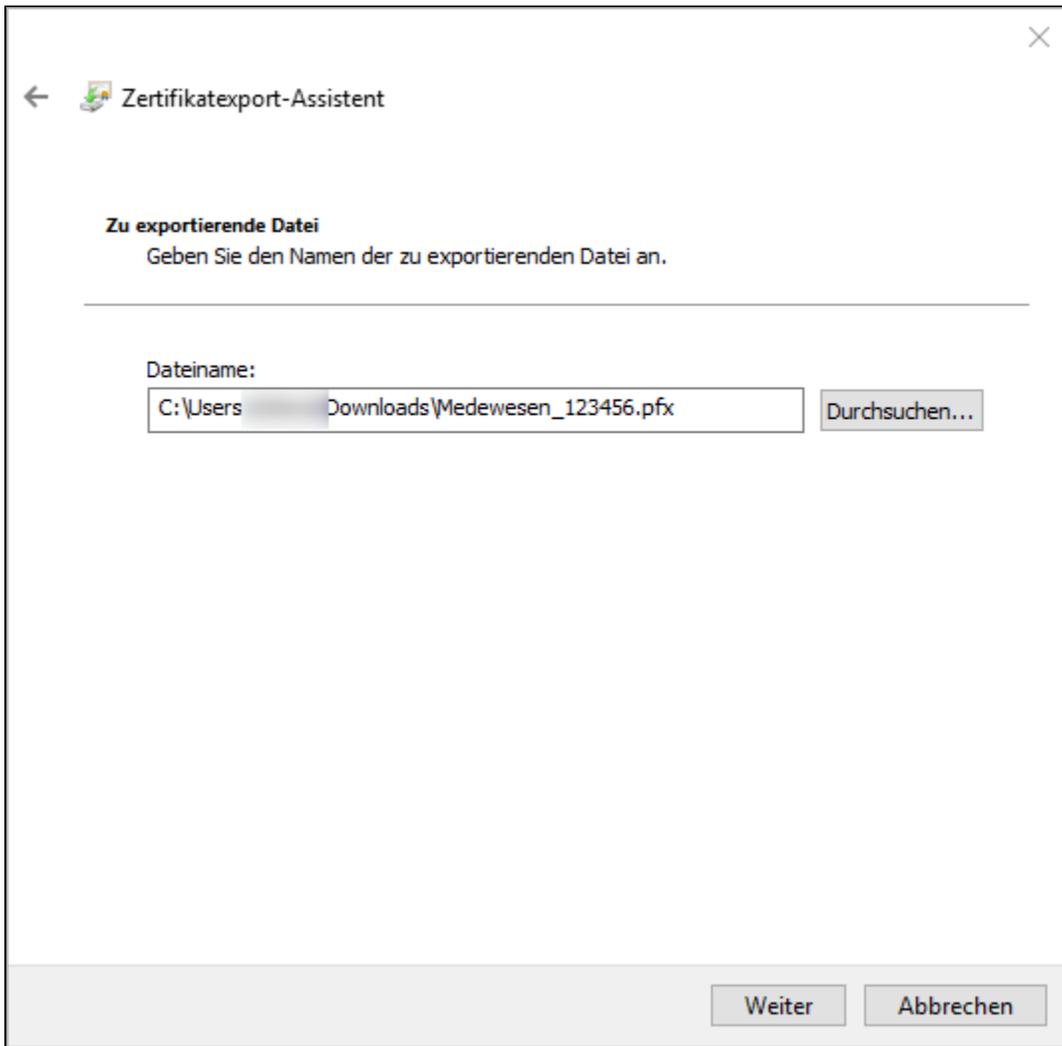
Zu exportierende Datei
Geben Sie den Namen der zu exportierenden Datei an.

Dateiname:

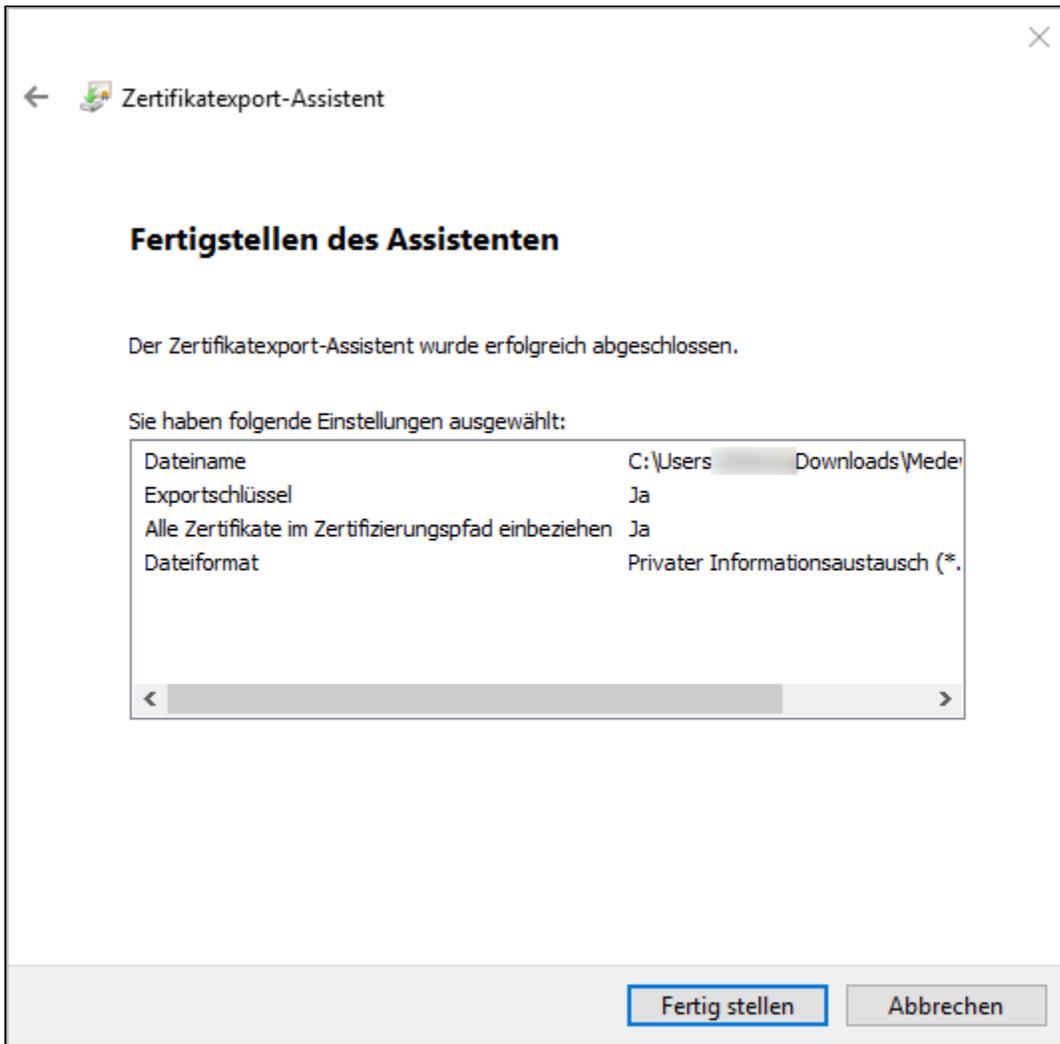
Wählen Sie hier den Speicherort aus, vergeben Sie den Dateinamen und klicken dann auf **Speichern**.



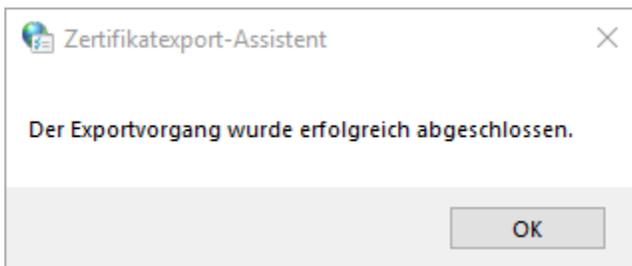
Klicken Sie auf **Weiter**.



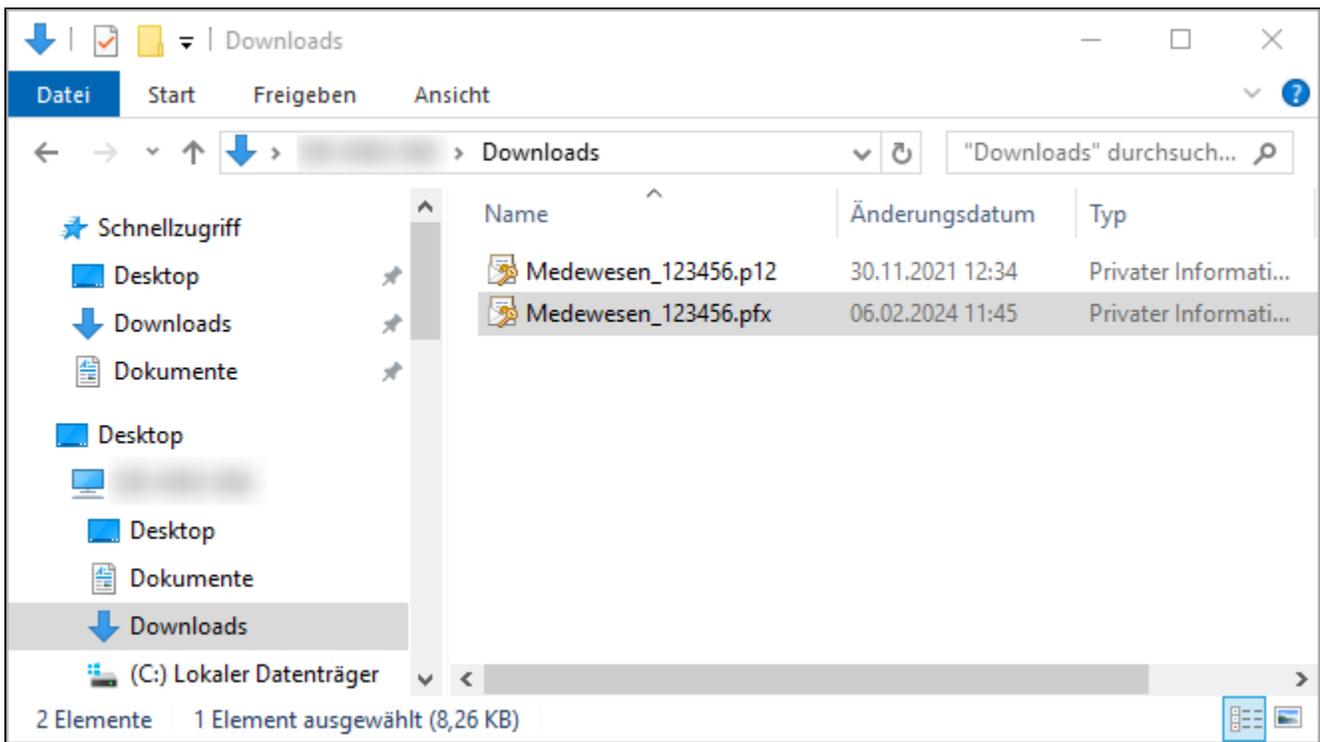
Es werden alle Eingaben eingeblendet. Nach dem Klicken auf "**Fertig stellen**" ist der Exportvorgang abgeschlossen



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



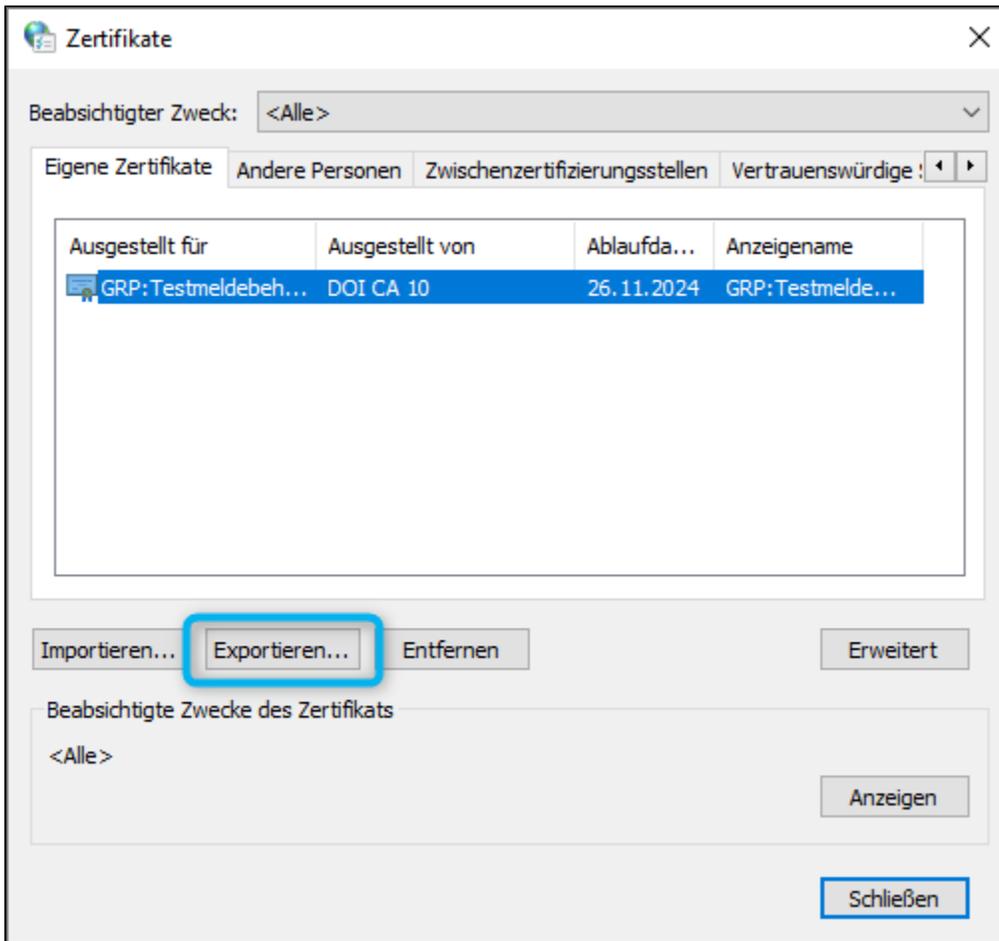
Das neue private Zertifikat "**Medewesen_123456.pfx**" wurde erstellt.



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**.



←  Zertifikatexport-Assistent

Willkommen

Dieser Assistent hilft Ihnen beim Kopieren von Zertifikaten, Zertifikatvertrauenslisten und Zertifikatssperrlisten vom Zertifikatspeicher auf den Datenträger.

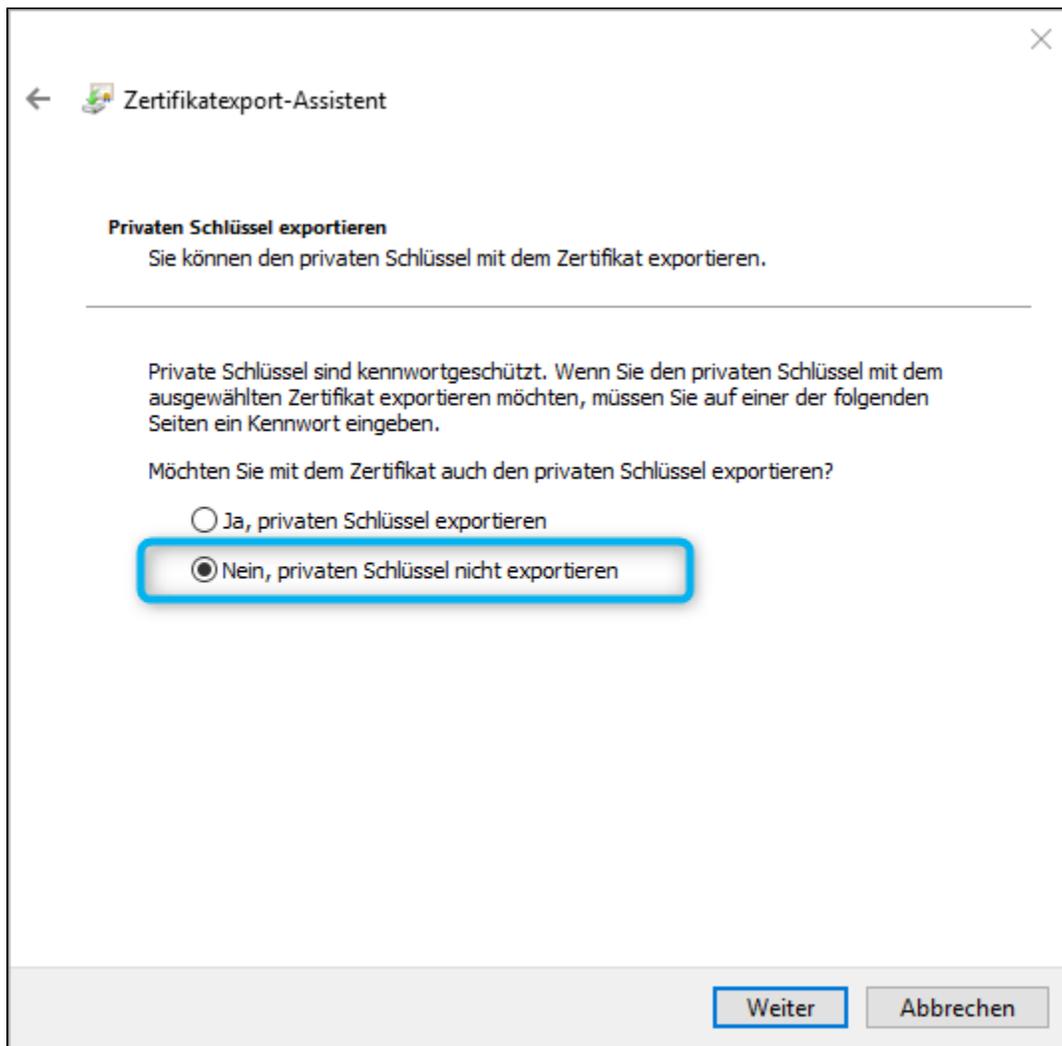
Ein von einer Zertifizierungsstelle ausgestelltes Zertifikat dient der Identitätsbestätigung. Es enthält Informationen für den Datenschutz oder für den Aufbau sicherer Netzwerkverbindungen. Ein Zertifikatspeicher ist der Systembereich, in dem Zertifikate gespeichert werden.

Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.

Weiter

Abbrechen

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**.



Format der zu exportierenden Datei

Zertifikate können in verschiedenen Dateiformaten exportiert werden.

Wählen Sie das gewünschte Format:

- DER-codiert-binär X.509 (.CER)
- Base-64-codiert X.509 (.CER)
- Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)
 - Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
- Privater Informationsaustausch - PKCS #12 (.PFX)
 - Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
 - Privaten Schlüssel nach erfolgreichem Export löschen
 - Alle erweiterten Eigenschaften exportieren
 - Zertifikatdatenschutz aktivieren
- Microsoft Serieller Zertifikatspeicher (.SST)

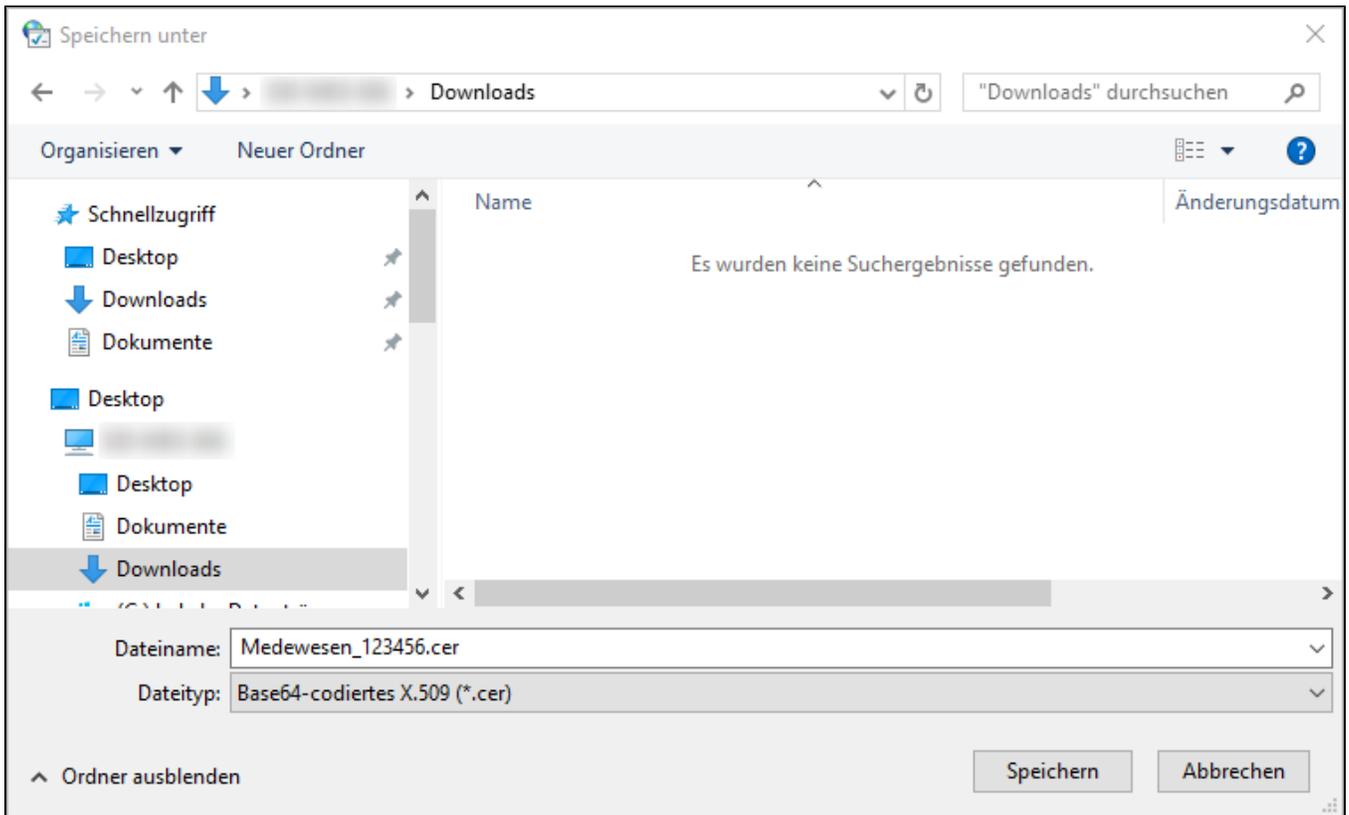
Klicken Sie auf **Durchsuchen**.

←  Zertifikatexport-Assistent ×

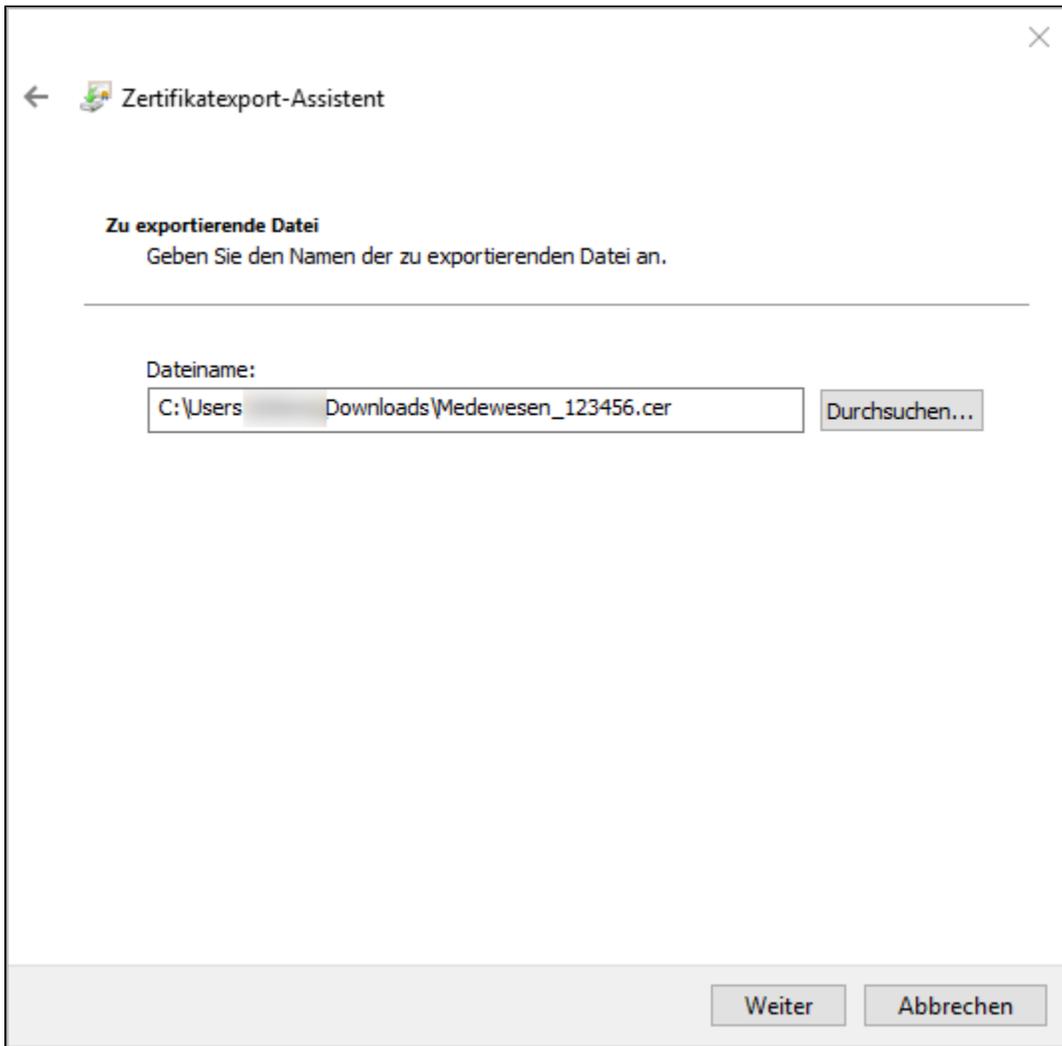
Zu exportierende Datei
Geben Sie den Namen der zu exportierenden Datei an.

Dateiname:

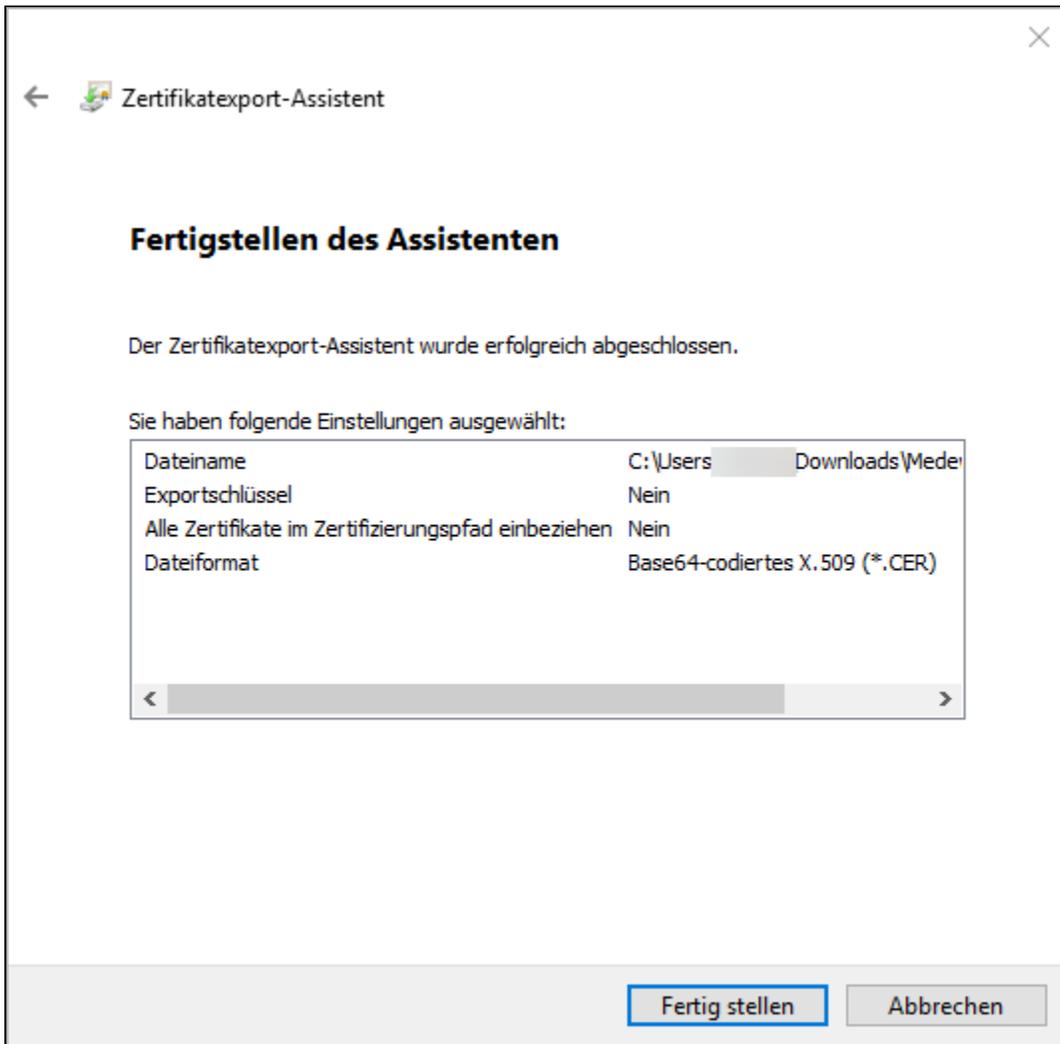
Wählen Sie hier den Speicherort aus, vergeben Sie den Dateinamen und klicken dann auf **Speichern**.



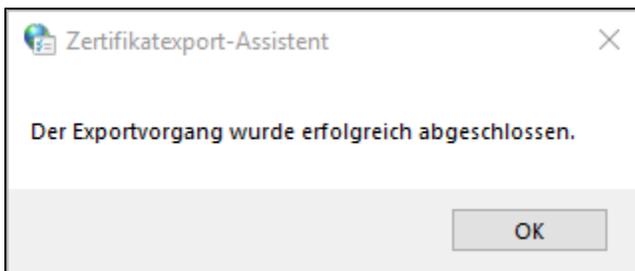
Klicken Sie auf **Weiter**.



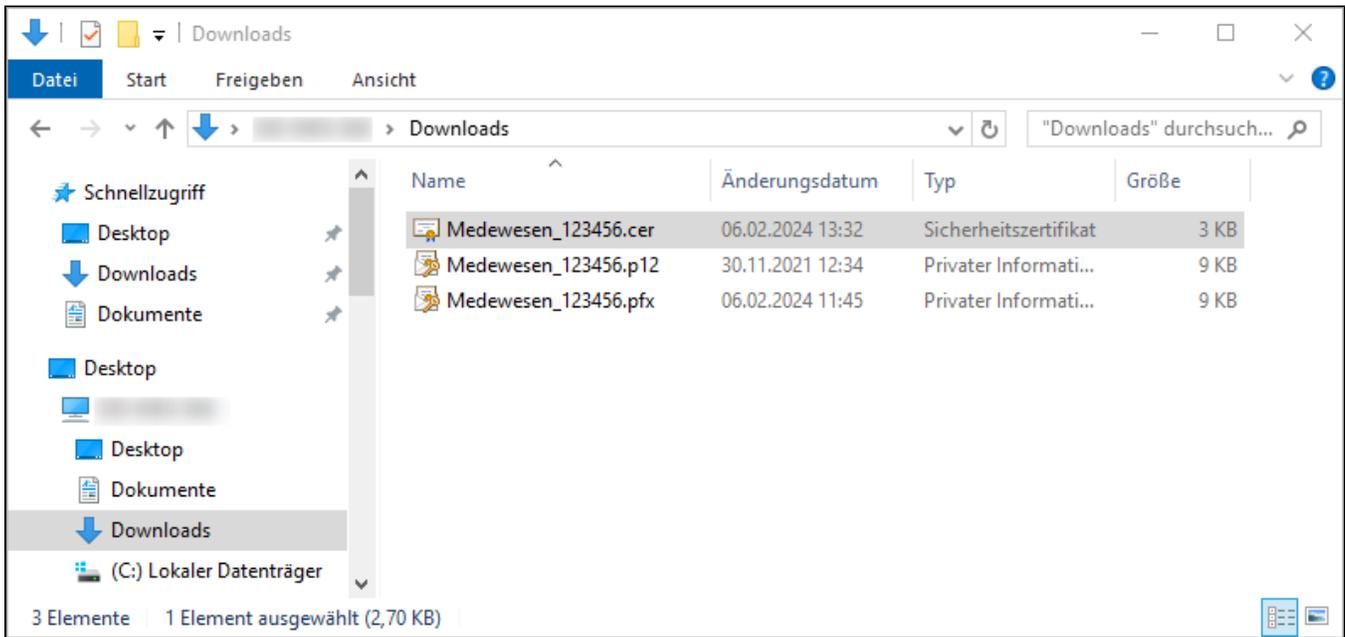
Im nächsten Menü werden Ihnen die Daten noch einmal angezeigt, bestätigen Sie dieses Menü mit "**Fertig stellen**".



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



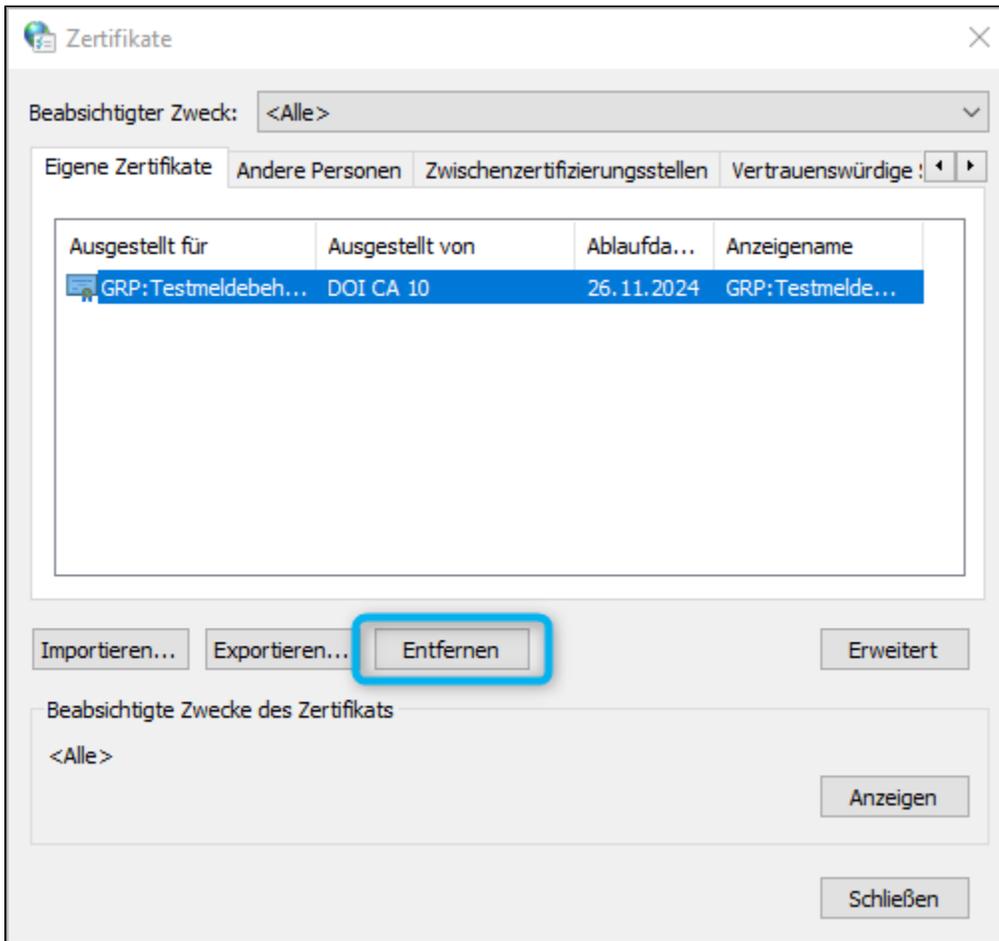
Ihr Zertifikat liegt jetzt in Dateiform in dem von Ihnen gewählten Ordner („*.cer“) vor. Diese Datei können Sie bedenkenlos weitergeben (z.B. für die Veröffentlichung im SaxDVDV bzw. DVDV).



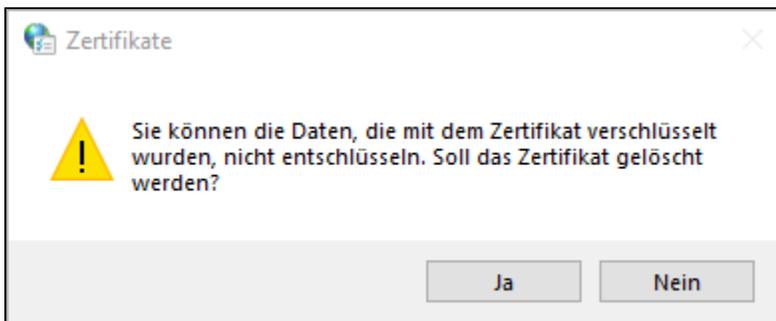
4 Zertifikat löschen

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.

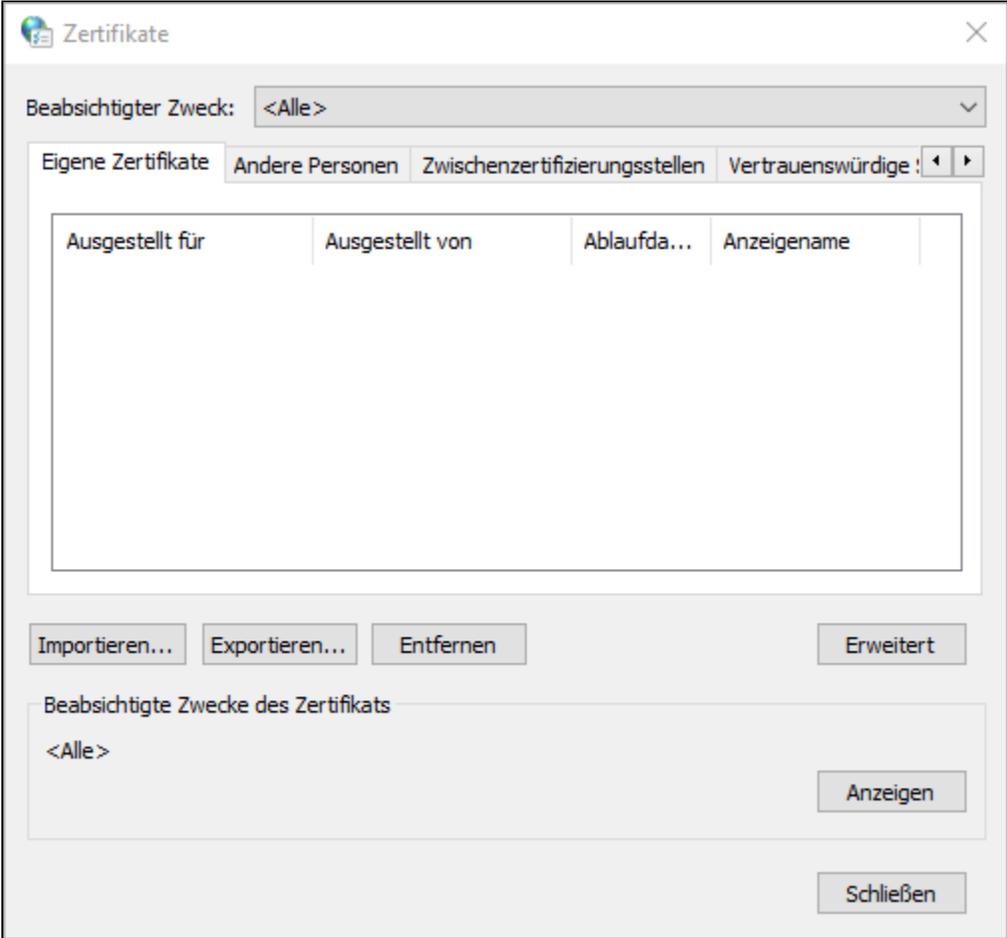
Klicken Sie dann auf **Entfernen**.

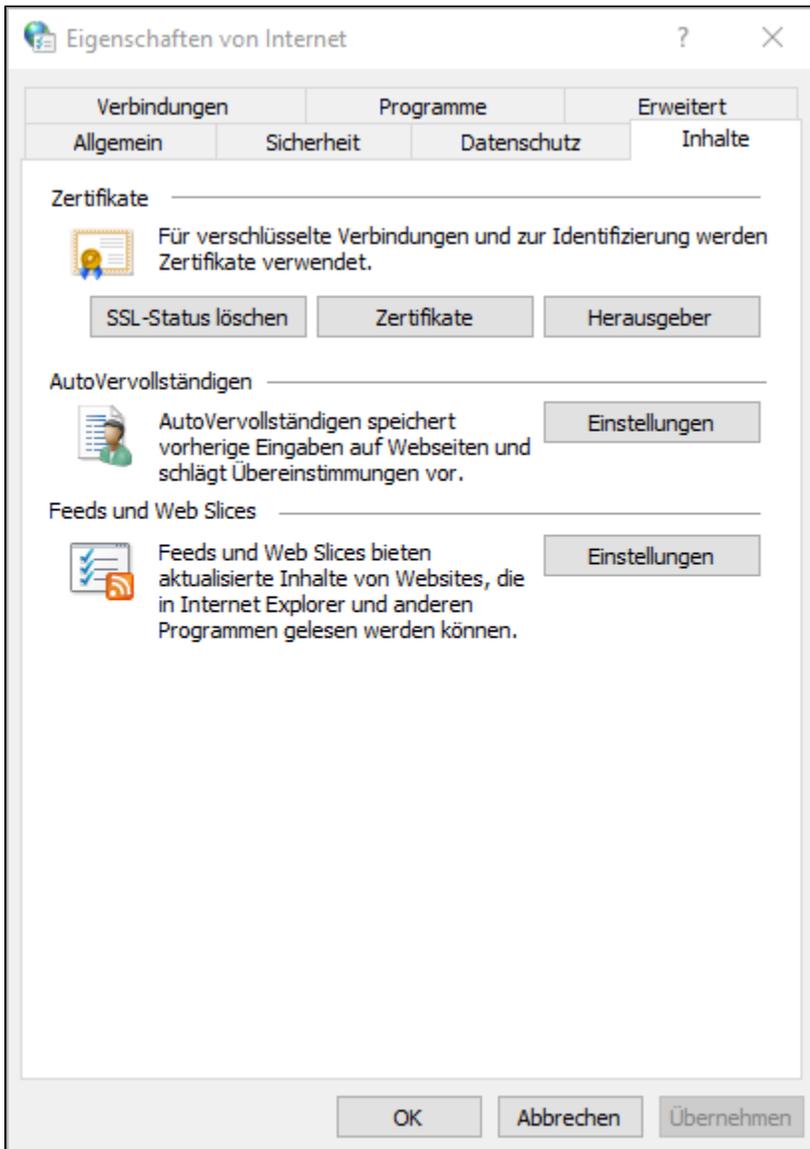


Es wird folgende Abfrage angezeigt. Klicken Sie zum Löschen des Zertifikats auf **Ja**.



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





ENDE