VERWALTUNGS-PKI-ZERTIFIKATE

Beantragung V-PKI-Gruppenzertifikat für OZG / OSCI-Nutzung

Erstellt durch:
Registrierungsstelle der SIT
Sonnenblumenallee 3
58675 Hemer

IHR KONTAKT

Auskunft erteilt: Registrierungsstelle SIT

Durchwahl: +49 271 30 321-3333

Zentrale: +49 271 30 321-0

Email: pki@sit.nrw

Inhalt Seite

1. Wichtige Vorab-Informationen

Bitte führen Sie den kompletten Antragsprozess zeitnah ohne große Unterbrechungen durch. Der Prozess ist erst **nach dem erfolgreichen Import** des Zertifikats in den Browser abgeschlossen, nicht schon nach dem Absenden des Antrags oder dem Herunterladen der Signaturdatei vom Trust-Center. Bis zum **Abschluss** des Zertifizierungsprozesses dürfen am **Benutzerprofil auf dem Arbeitsplatzrechner der Antragstellerin bzw. des Antragstellers keine Veränderungen** vorgenommen werden. Dazu zählen insbesondere Passwortänderungen.

Hintergrund: Das Zertifikat besteht aus zwei verschiedenen Komponenten:

- **Öffentlicher Schlüssel**, der Ihnen vom Trust-Center signiert wird
- **Privater Schlüssel**, der beim Zertifikatsantrag erstellt und verborgen auf dem Antragsrechner verbleibt. Der private Schlüssel kann nicht explizit aufgerufen werden. Durch Veränderungen am Benutzerprofil auf Ihrem PC kann der private Schlüssel beschädigt werden bzw. verloren gehen.

Zum Abschluss des Zertifizierungsprozesses werden diese beiden Elemente zu einem persönlichen Zertifikat zusammengeführt. Nur zusammen funktionieren beide Teile als privates Zertifikat. Daher ist es besonders wichtig den Prozess zeitnah zu beenden und abschließend den erfolgreichen Import zu überprüfen. Lesen Sie hierzu bitte das Kapitel 3.4 bzw. 3.5).

Kurzportrait Gruppenzertifikat

Gültigkeitsdauer	3 Jahre Bei Wechsel der Förderperiode, des Standorts oder des Zertifikatsverantwortlichen kann ein gültiges Zertifikat weiter benutzt werden. Eine Neubeantragung ist nicht zwingend notwendig.
Aussteller	Trust-Center Südwestfalen-IT
Verantwortlichkeit	Eine Person pro Einrichtung
Browser	Die Beantragung erfolgt mit einem Browser. Die Generierung des digitalen Schlüsselmaterials erfolgt über das Windows-Betriebssystem. Hierzu erhalten Sie im Antragsprozess eine E-Mail mit einer vorkonfigurierten .bat-Datei, die Sie bitte ausführen.
Speicher	Automatisch unter Eigene/Ihre Zertifikate im Zertifikatsmanager von Microsoft Windows.
Schlüssellänge:	4096-Bit[1]

[1] Mit Stichtag 01. April 2023

2. Einleitung

Im Rahmen der OZG-Anbindung Wohngeld und später weiterer OZG-Dienste werden Antragsdaten verschlüsselt über das Internet transportiert. Um die Echtheit der Kommunikationspartner zu gewährleisten, werden an beiden Enden der Datenverbindung Zertifikate eingesetzt. Es werden nur Verbindungen von Stellen, die als **vertrauenswürdig** bekannt sind, akzeptiert. Zertifikate werden als Gruppenzertifikate (X.509) vergeben. Die Zertifikatverwaltung wird vom Trust-Center der SIT (vormals Citkomm) betrieben. Durch ein **Gruppenzertifikat** wird die Zugehörigkeit eines Systems zu einer Einrichtung authentifiziert. Neben öffentlichen Schlüsseln (Public-Key), die vom Trust-Center digital signiert werden (und damit Zertifikate werden), gehört dazu auch der korrespondierende private Schlüssel. Ohne diese beiden Teile ist eine Benutzung der Zertifikate zur Authentifizierung nicht möglich. Die Zertifikate sind **drei Jahre gültig**.

Diese Anleitung beschreibt die **Antragsstellung** und **Installation** der Gruppenzertifikate sowie den **Import** zugehöriger Zertifikate von Zertifizierungsstellen, um eine vollständige Vertrauenskette aufzubauen. Für die **korrekte Anwendung** der Gruppenzertifikate stellt die SIT (Citkomm) weitere Dokumente bereit, auf diese wird unter Abschnitt „Dokumentation“ verwiesen.

3. Der Zertifizierungsprozess

Die **Beantragung** erfolgt über den Browser eines Windows-Arbeitsplatzsystems. Der Prozess für ein Gruppenzertifikat teilt sich in mehrere Schritte:

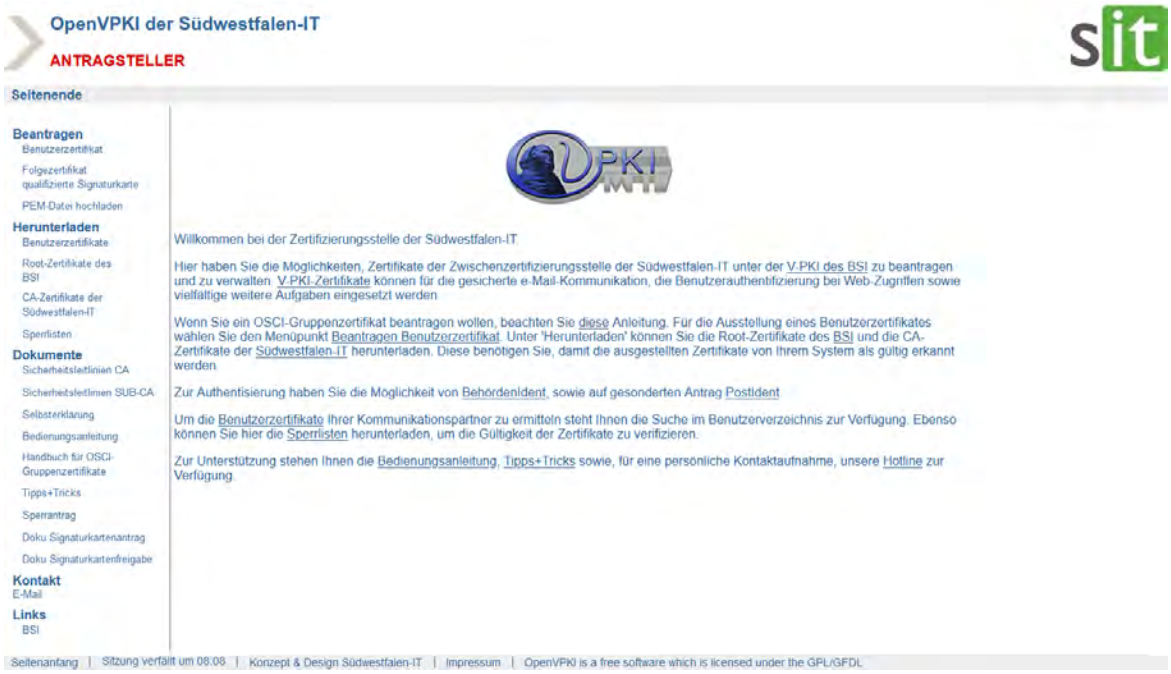
1. Antragsstellung über cas.citkomm.de
2. Drucken des Namensvergabedokuments und Versand an das Trust-Center der SIT
3. Generierung des digitalen Schlüsselmaterials (nur auf einem Windows-Arbeitsplatz möglich)
4. Authentisierung durch Post-Ident-Verfahren – ersatzweise Behörden-Ident
5. Herunterladen und Erst-Installation des Zertifikates
6. Export/Import des Zertifikates

Für den Zertifizierungsprozess wird in jeder Verwaltung eine **Verantwortliche bzw. ein Verantwortlicher** festgelegt. Diese Person führt die Beantragung des Zertifikats durch. Die Schritte bis zur Weitergabe des Zertifikates an die OSCI-Kommunikationssysteme finden auf **einem Rechner unter dem Nutzerkonto der verantwortlichen Person** statt.

3.1. Die Antragstellung

Bei der Antragsstellung wird ein Schlüsselpaar erstellt. Dieses Paar besteht aus einem öffentlichen und privaten Schlüssel. Der öffentliche Teil wird an das Trust-Center der SIT zur Signatur übermittelt. Zusammen fungiert das Schlüsselpaar später dann als „Gruppenzertifikat“.
Gehen Sie bitte wie folgt bei der Antragstellung vor:

- Öffnen Sie mit dem Browser die Seite **https://cas.citkomm.de**

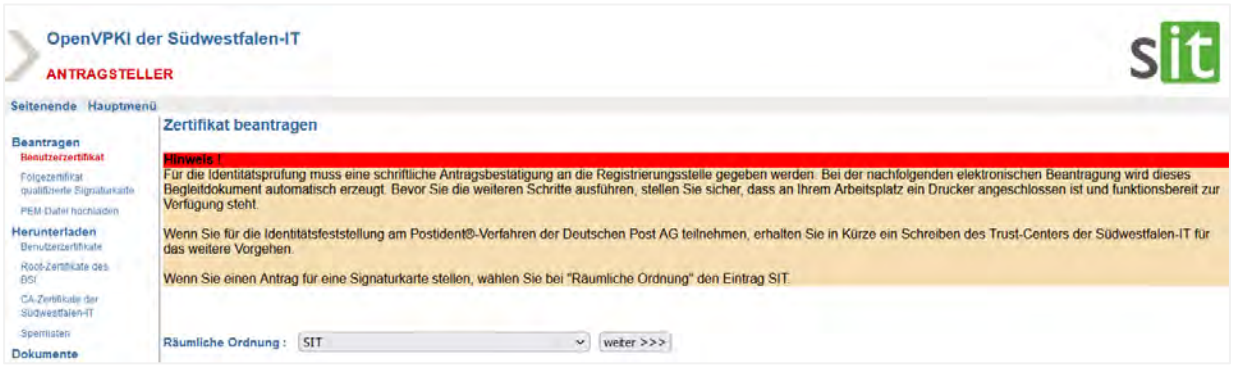


Bitte beachten Sie, dass die Bearbeitung des Antrags auf dieser Internetseite zeitlich begrenzt ist (siehe dazu Seitenende „Sitzung verfällt um xx.xx“).

Achtung: Für die Identitätsprüfung muss ein schriftliches Antragsdokument an das Trust-Center der SIT (Citkomm) gegeben werden. Bei der nachfolgenden elektronischen Beantragung wird dieses

Begleitdokument automatisch erzeugt. Bevor Sie die weiteren Schritte ausführen, stellen Sie sicher, dass an Ihrem Arbeitsplatz ein Drucker angeschlossen ist und funktionsbereit zur Verfügung steht. Sie können das Dokument auch als PDF-Datei speichern und zu einem späteren Zeitpunkt ausdrucken.

- Wählen Sie aus dem linken Menü „Beantragen“ > „Benutzerzertifikat" aus.
- Wählen Sie als *Räumliche Ordnung: -* ***SIT*** aus

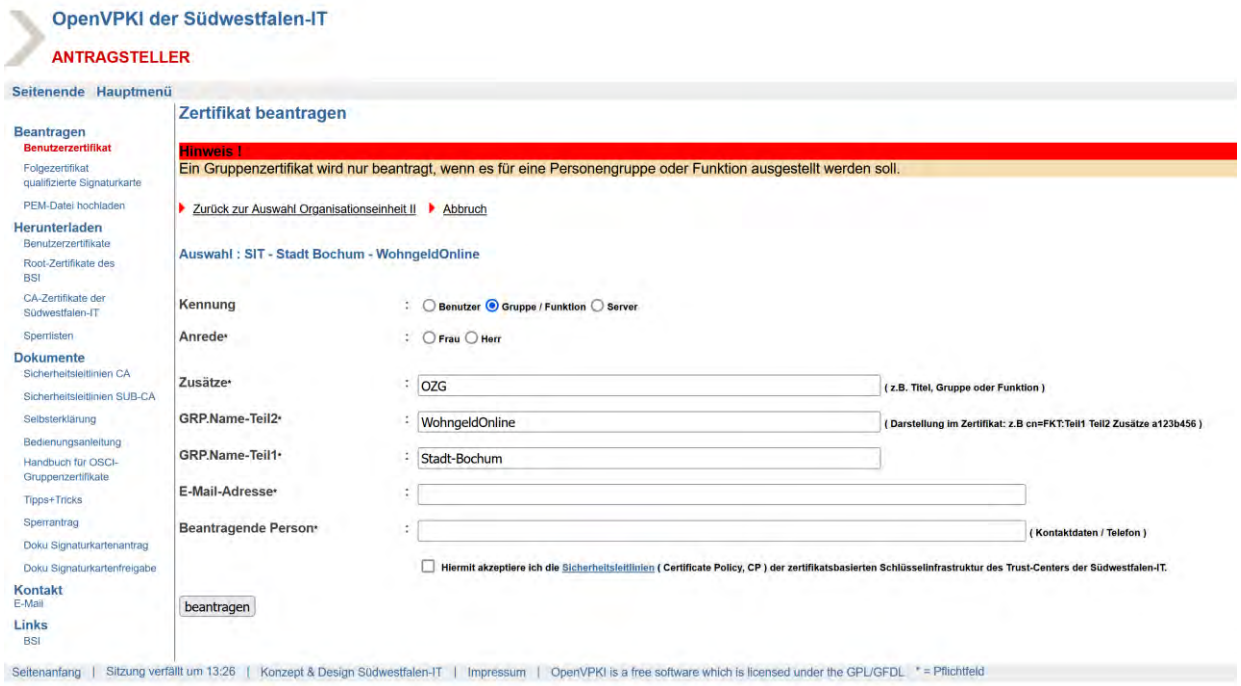


- Wählen Sie als *Organisationseinheit I: -* ***Ihre Verwaltung*** aus z.B. Stadt Hemer

- Wählen Sie als *Organisationseinheit II: -* ***WohngeldOnline*** aus

Sofern unter *Organisationseinheit II* die Auswahl *WohngeldOnline* nicht möglich ist, teilen Sie dies bitte an helpdesk@sit.nrw mit, damit die notwendige Ergänzung vorgenommen werden kann.

- Auf der folgenden Seite sind die Felder GRP.Name-Teil2 bereits mit „Wohngeld“ und GRP.Name-Teil1 mit dem Namen Ihrer Verwaltung vorbelegt. Hier sollten im Normalfall keine Änderungen erforderlich sein, bei Bedarf können Sie Inhalte gleichwohl abändern / korrigieren. Nehmen Sie bitte folgende weitere Einträge vor:



- Kennung — Gruppe / Funktion (vorbelegt)
- Zusätze — „OZG“ (vorbelegt, ggf. Ergänzung individueller Informationen)
- GRP.Name-Teil2 — „WohngeldOnline“ (vorbelegt)
- GRP.Name-Teil1 — <Verwaltungsname> (vorbelegt)
- E-Mail-Adresse — E-Mail-Adresse des Zertifikatsverantwortlichen
- Beantragende Person — Name, Vorname und ggf. Telefonnummer oder E-Mail-Adresse

Bitte beachten Sie, dass keine Umlaute verwendet werden dürfen.

Die Felder GRP.Name-Teil1, GRP.Name-Teil2 und Zusätze dürfen in Summe nur 48 Zeichen umfassen.

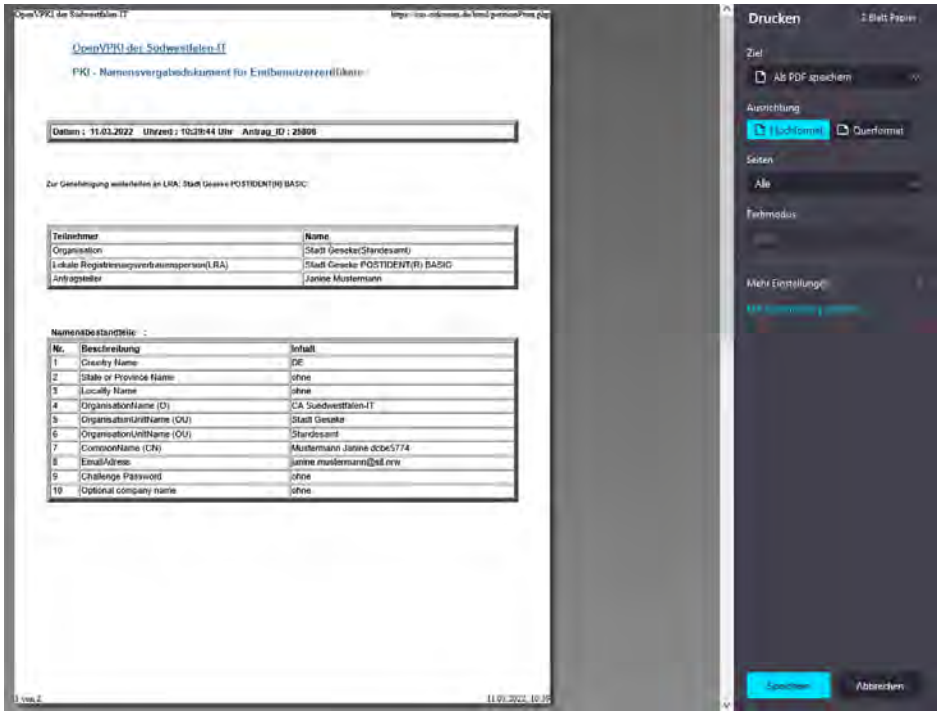
Die Anrede muss nicht gewählt werden.

Über die angegebene E-Mail-Adresse wird der weitere Antragsprozess abgewickelt.

- Anschließend akzeptieren Sie bitte die Sicherheitsleitlinien – diese sind verlinkt und können nachgelesen werden – und klicken Sie auf die Schaltfläche *beantragen*.

3.2. Drucken des Namensvergabedokumentes

Es folgt nun ein Hinweis, dass der Zertifikatsantrag (Namensvergabedokument) gedruckt wird. Sie können den Auftrag entweder direkt drucken, in dem Sie ihren Drucker auswählen und auf *Drucken* drücken oder den Auftrag als PDF-Datei speichern und zu einem späteren Zeitpunkt ausdrucken.

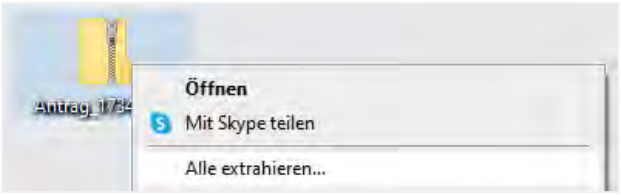


Ohne diesen Ausdruck kann Ihr Zertifikat nicht erstellt werden. Bitte unterschreiben Sie das Dokument als Antragsteller auf der 2. Seite unten.

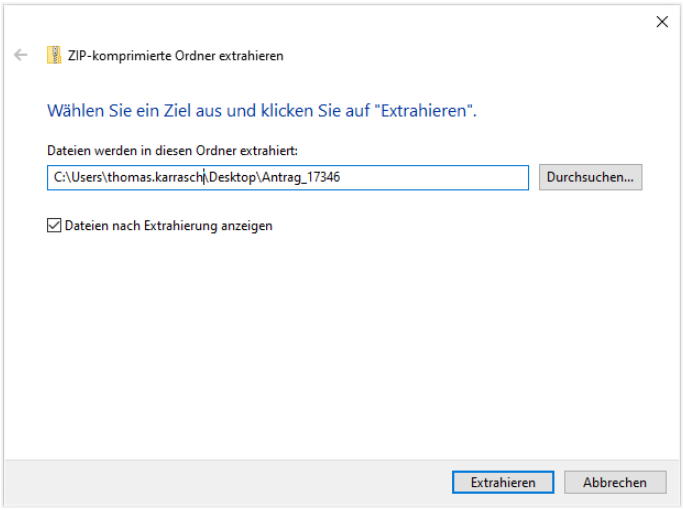
3.3. Generierung des digitalen Schlüsselmaterials

Nach abgeschlossener Beantragung eines Zertifikats erhalten Sie eine E-Mail, in dessen Anhang sich eine Zip-Datei befindet.

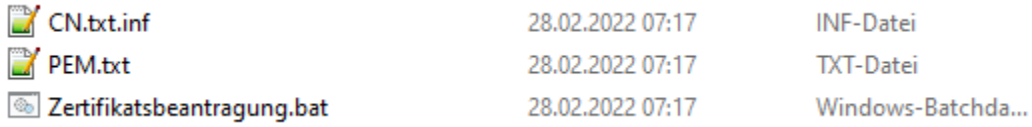
Diese müssen Sie auf dem Desktop oder einem anderen Ordner entpacken. Hierzu machen Sie einen rechtsklick auf die Datei und wählen *Alle extrahieren…* aus.



Im Folgedialog klicken Sie bitte auf *Extrahieren*



Alle für die Beantragung benötigten Dateien befinden sich innerhalb des entpackten Ordners. In der CN.txt.inf befinden sich alle Informationen, die bei der Beantragung hinterlegt wurden, in der PEM.txt die aktuelle Auftragsnummer.



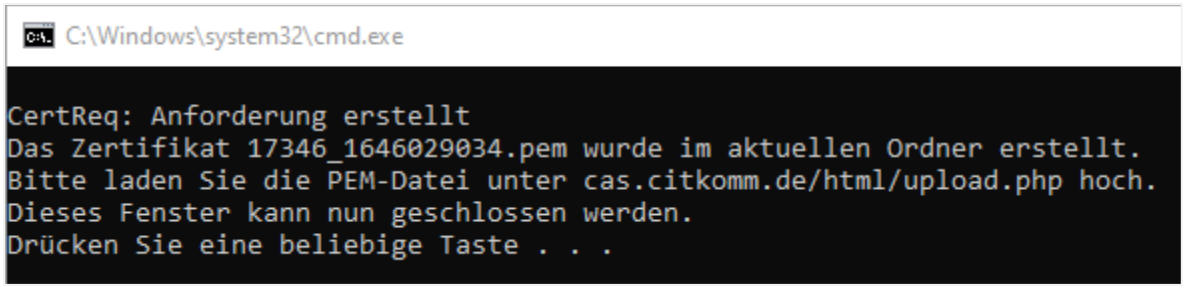
Mit der Ausführung der Datei Zertifikatsbeantragung.bat wird das digitale Schlüsselmaterial für die Zertifizierung erzeugt und ein technischer Antrag an die SIT übertragen. Dieser ist mit dem formalen Antrag, den Sie vorab über cas.citkomm.de gestellt haben, verknüpft und daher zwingend für die weitere Antragsbearbeitung erforderlich.

3.3.1. Durchführung

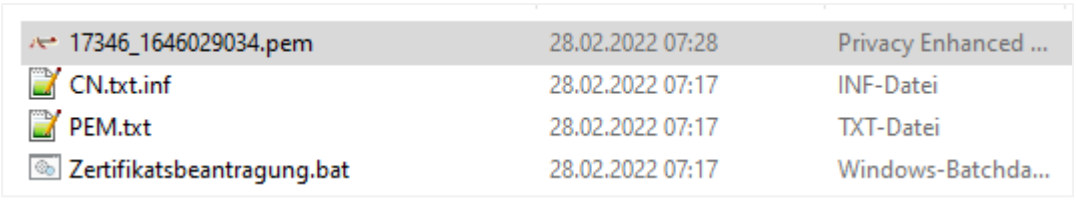
Die Beantragung wird durch das Ausführen der Datei *Zertifikatsbeantragung.bat* durchgeführt. Rufen Sie die Datei mit einem Doppelklick auf, **nicht** *Als Administrator ausführen*.
Es kann auf Grund von Sicherheitseinstellungen folgende Fehlermeldung erscheinen:

Um mit der Beantragung fortzufahren, klicken Sie im unteren Teil der Fehlermeldung auf *Weitere Informationen* und im Folgedialog auf *Trotzdem ausführen.*

Es öffnet sich ein neues Fenster und die Beantragung wird durchgeführt:



Durch die Zertifikatsbeantragung wird der öffentliche Schlüssel als .pem-Datei, die für die Beantragung benötigt wird, im aktuellen Ordner generiert. Der private Schlüssel des Zertifikats wird im Windows internen Zertifikatsspeicher hinterlegt, in der .pem-Datei befindet sich nur der öffentliche Schlüssel, der zur weiteren Beantragung benötigt wird.



3.3.2. Versendung der Datei

Im Anschluss an die Erstellung wird der Default-Browser geöffnet und die Seite zum Hochladen der .pem-Datei geöffnet (https://cas.citkomm.de/html/upload.php).

An dieser Stelle müssen Sie über den Durchsuchen-Button die generierte .pem-Datei auswählen und hochladen.

Mit dem Upload ist der technische Teil des Antragsprozesses abgeschlossen. Bitte führen Sie als nächstes die persönliche Antrags- und Identitätsfeststellung gemäß dem von Ihrer Verwaltung gewählten Verfahren (Behördenident, Postident oder über eine lokale Ansprechperson) durch.

Achtung: Der private Schlüssel als privater Teil des Zertifikats wird auf Ihrem PC gespeichert und nicht an die SIT weiter gegeben. Auf diesem PC muss nach Fertigstellung des Zertifikats durch das Trust-Center auch die Installation erfolgen. Bitte beachten Sie, dass zwischen Antrag und Installation keine Änderungen am Benutzerprofil des Betriebssystems (insbesondere Kennwortänderung) vorgenommen werden dürfen. Daher sollten Sie den Prozess zeitnah abschließen.

Setzen Sie sich bei Problemen ggf. Ihrer lokalen IT/TUI in Verbindung – der Antrag muss bei versäumtem Ausdruck nicht erneut gestellt werden.

Senden Sie das unterschriebene Namensvergabedokument als per E-Mail an pki@sit.nrw und bewahren Sie es sorgfältig auf.

3.4. Postident

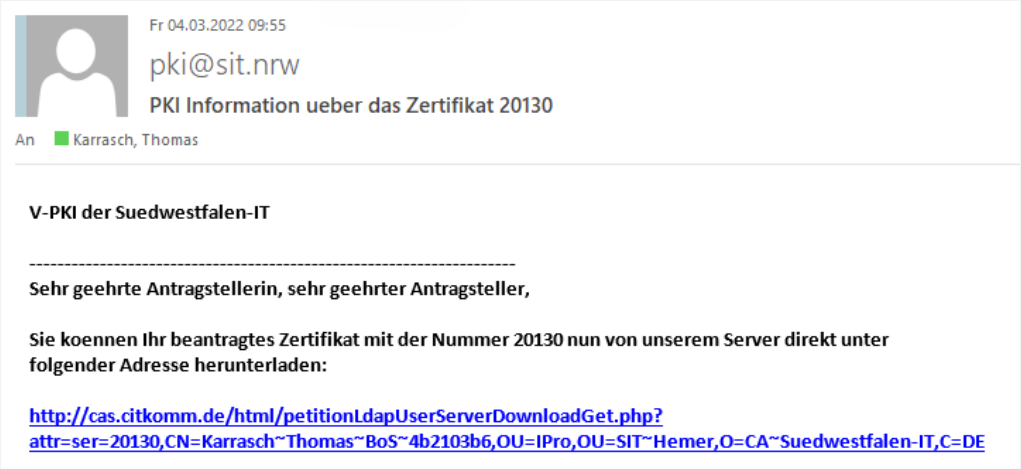
Sie erhalten in Kürze ein Schreiben bzw. eine Mail der Südwestfalen-IT, in dem die weiteren Vorgehensweisen erklärt wird. Die persönliche Authentisierung kann auch in einer beliebigen Filiale der Deutschen Post AG vorgenommen werden. Die Südwestfalen-IT bietet dafür das Verfahren POSTIDENT an. Dieser zertifizierte Dienst der Deutschen Post AG übernimmt dann Teilaufgaben der LRA-Instanz. Der dafür notwendige Post-Coupon wird Ihnen zugeschickt.

3.5. Behördenident

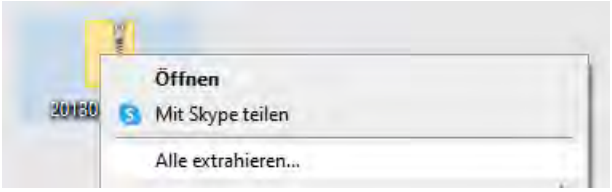
Stellen Sie den Zertifikatantrag als mitarbeitende Person in einer Behörde, so kann eine Identitätsfeststellung per Behördenident erfolgen. Hierzu finden Sie einen entsprechenden Bestätigungsvorduck zum Download auf der Startseite der Registrierungsstelle (cas.citkomm.de).
Mit dem Vordruck und dem Zertifikatsantrag lassen Sie Ihre Identität bitte bei einer Siegleführenden Stelle in Ihrer Behörde bestätigen.
Die Dokumente senden Sie im Anschluss bitte an die SIT unter pki@sit.nrw.

4. Herunterladen des Zertifikats nach Mail vom Trust Center

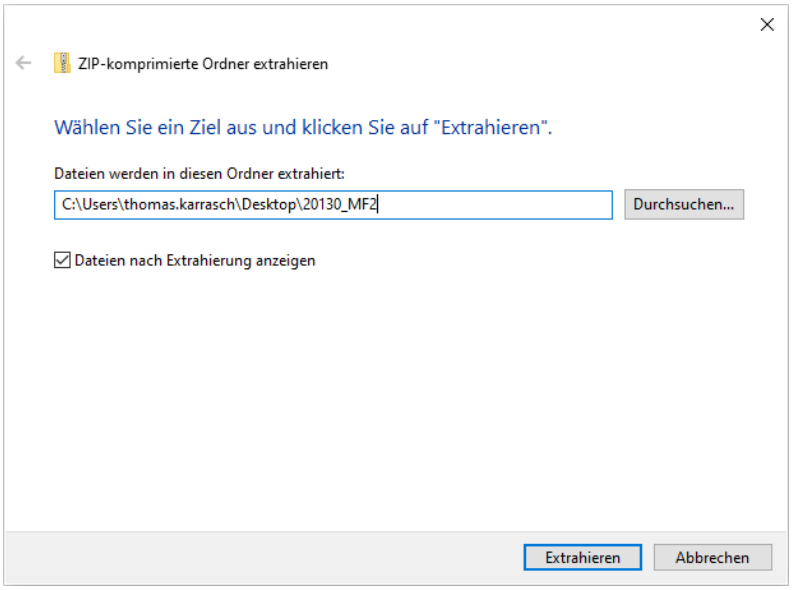
Nachdem die Bearbeitung ihres Zertifikats abgeschlossen ist, erhalten Sie eine E-Mail mit einem Download-Link, unter welchem Sie sich das Zertifikat herunterladen können.



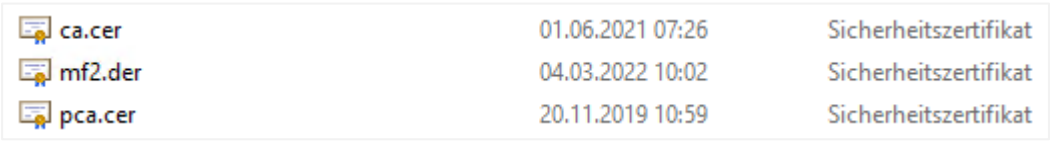
Diese müssen Sie auf dem Desktop entpacken. Zum Entpacken machen Sie einen Rechtsklick auf die Datei und wählen *Alle extrahieren…* aus.



Im Folgedialog klicken Sie bitte auf *Extrahieren:*

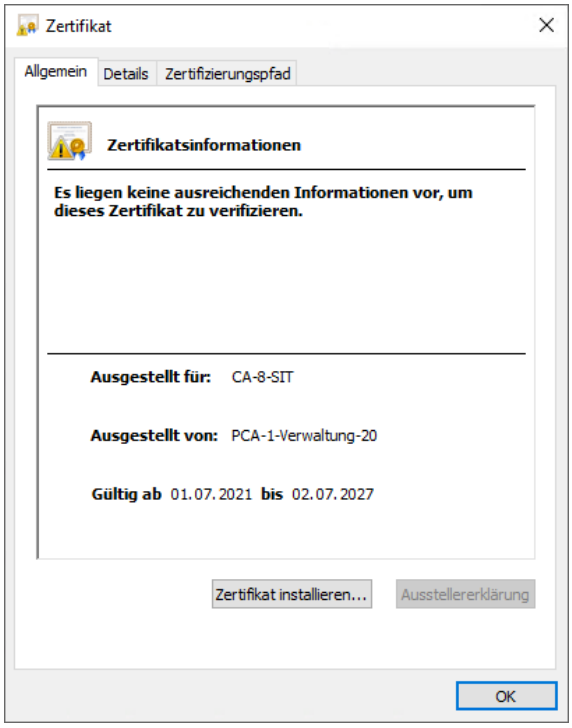


Im entpackten Ordner befinden sich folgende Zertifikatsdateien:

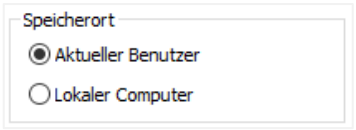


Für die Installation der Zertifikate führen Sie bitte folgende Schritte für **alle drei Dateien** durch:

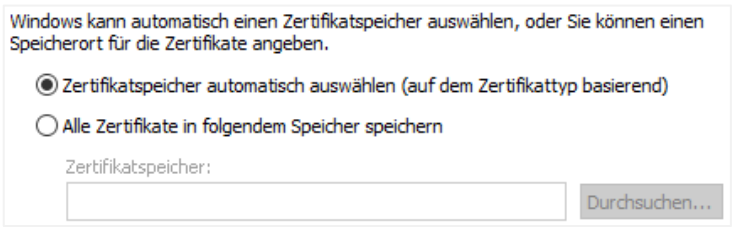
- Öffnen Sie die Zertifikatsdatei
- Wählen Sie bitte *Zertifikat installieren…* aus



- Wählen Sie bei *Speicherort* den Punkt *Aktueller Benutzer* (Voreinstellung) aus

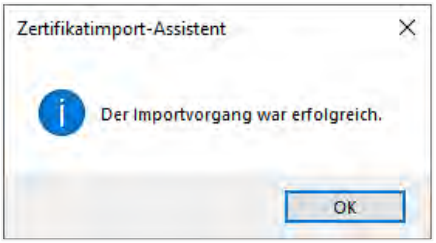


- Wählen Sie *Zertifikatspeicher automatisch auswählen (auf Zertifikattyp basierend)* aus



- Klicken Sie auf *Fertig stellen*

Sie erhalten nach Abschluss der Installation folgende Meldung:

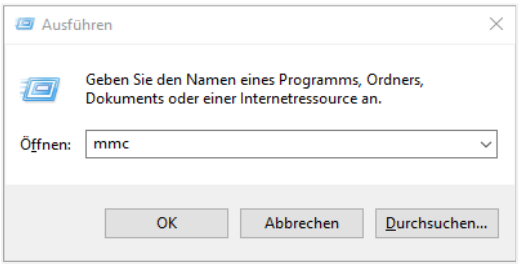


Führen Sie diese Schritte auch für die zwei verbleibenden Zertifikatdateien durch. Sobald dies durchgeführt wurde, ist das vollständige Zertifikat auf Ihrem System installiert.

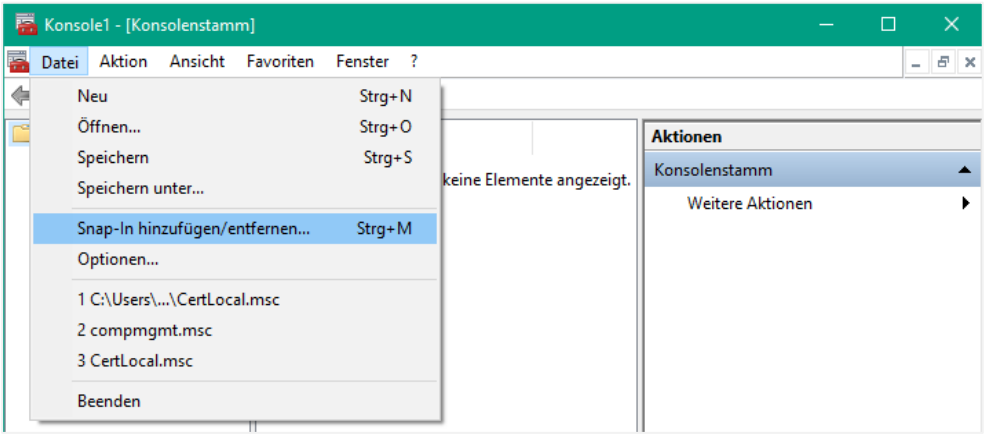
5. Sicherung des Zertifikates

Das vollständige Zertifikat ist im Windows eigenen Zertifikatsspeicher hinterlegt. Dieser kann vollständig zur Übertragung auf andere Computer exportiert werden oder nur, falls gewünscht, nur der öffentliche Teil des Schlüssels zur Weitergabe. An dieser Stelle werden beide Varianten Schritt für Schritt erklärt.

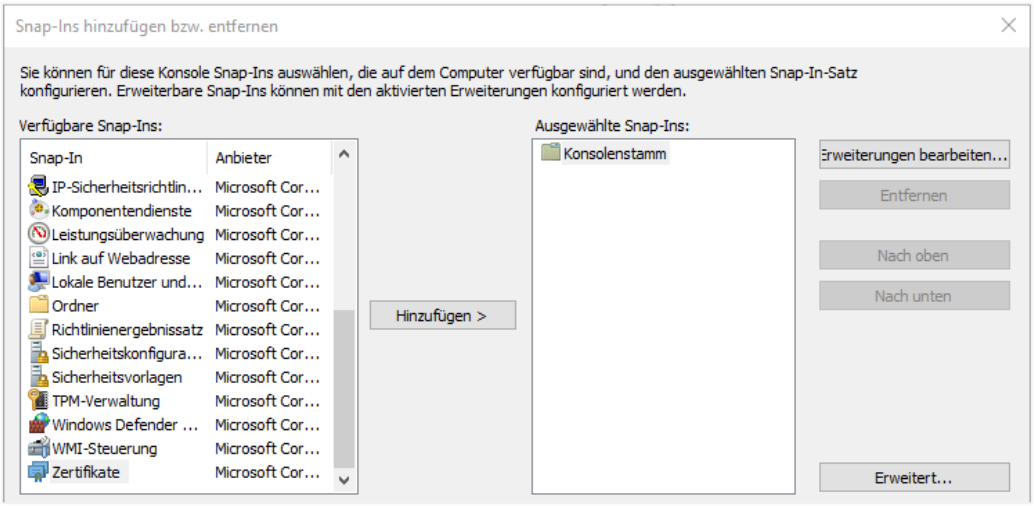
- Zum Öffnen der Konsole drücken Sie *Windows-Taste + R.* Es erscheint ein Fenster mit dem Titel *Ausführen.* Tippen Sie die Buchstaben *mmc* ein und drücken Sie auf *OK.*



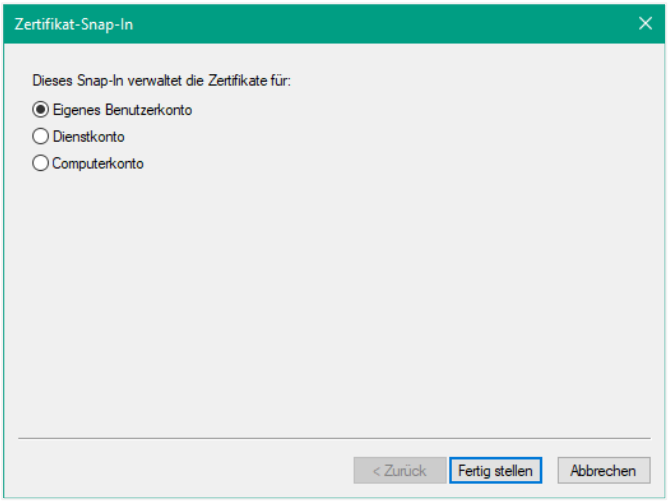
- Im neu erschienen Konsolenfenster fügen Sie ein neues Snap-In hinzu. Diesen Menüpunkt finden Sie unter *Datei → Snap-in hinzufügen/entfernen*.



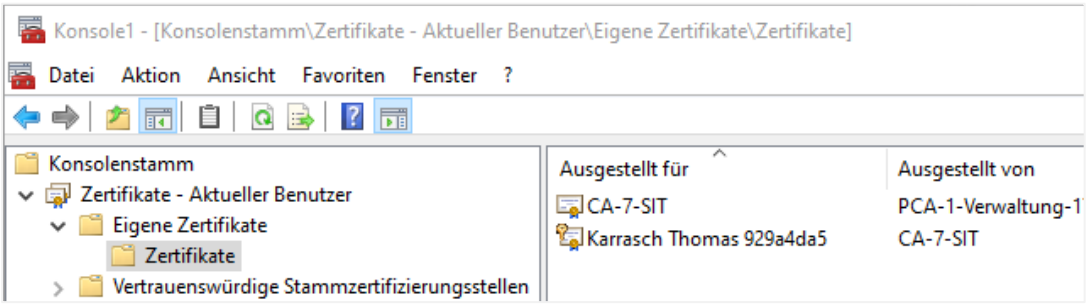
- Wählen Sie unter *Verfügbare Snap-Ins* (linkes Feld) *Zertifikate* aus und drücken Sie auf *Hinzufügen*



- Wählen Sie im Folgedialog *Zertifikat-Snap-In* den Punkt *Eigenes Benutzerkonto* aus und drücken Sie auf *Fertig stellen,* anschließend im Ursprungsfenster *OK*.



- Ihr bereitgestelltes Zertifikat sehen Sie unter dem Punkt Zertifikate – Aktueller Benutzer → Eigene Zertifikate → Zertifikate

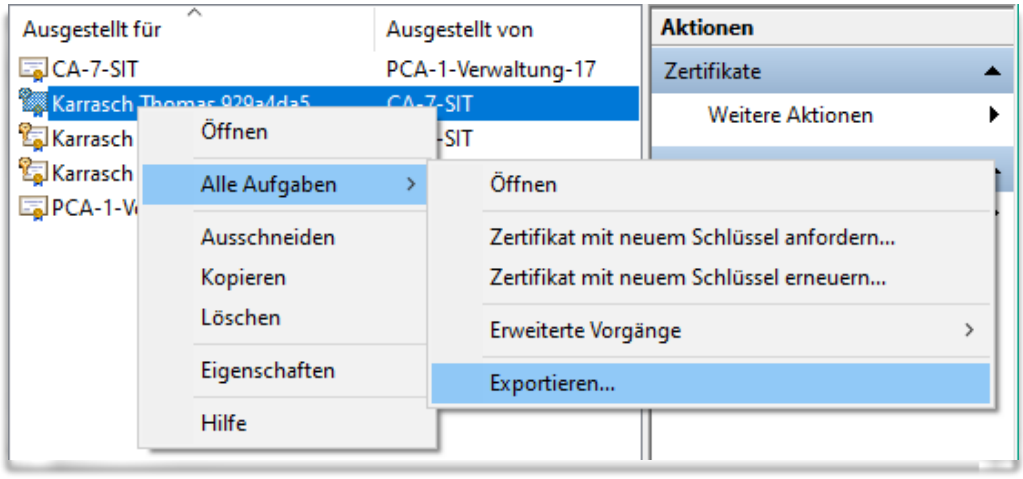


5.1. Bereitstellung des öffentlichen Zertifikats

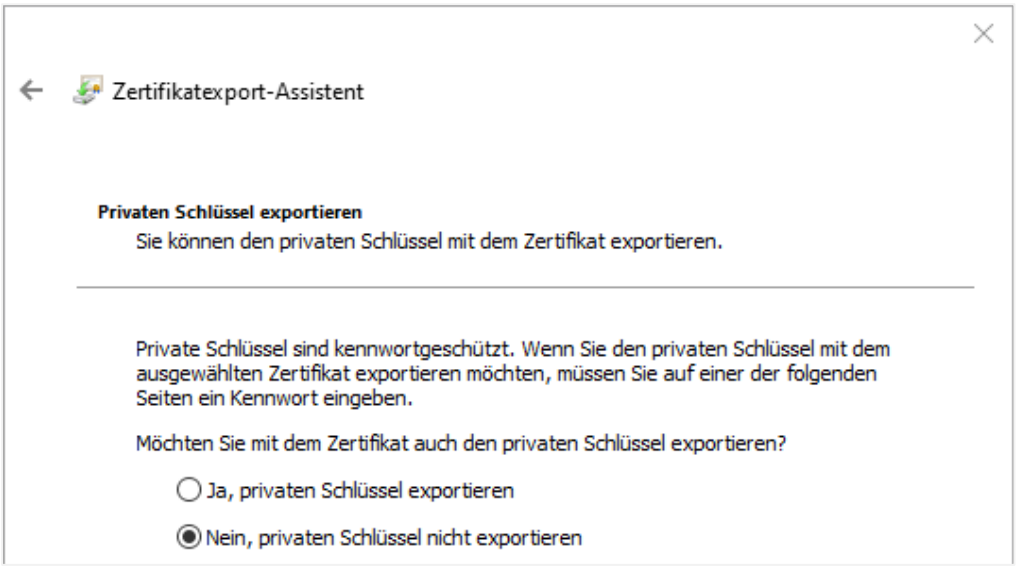
Diesen Schritt benötigen Sie zur Bereitstellung des öffentlichen Zertifikates gegenüber dem OZG-Portal Wohngeld.

Wird das öffentliche Zertifikat zur Weitergabe an andere Stellen benötigt, gehen Sie folgt vor:

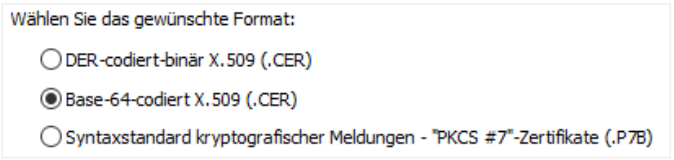
- Öffnen Sie den Zertifikatspeicher wie zu Beginn von Punkt 8 beschrieben
- Wählen Sie Ihr Zertifikat aus der Liste aus, machen Sie einen Rechtsklick und wählen Sie *Alle Aufgaben → Exportieren…* aus



- Bestätigen Sie den Willkommen-Dialog mit *Weiter* und wählen Sie im Folge-Dialog die Option *Nein, privaten Schlüssel nicht exportieren* aus und drücken Sie auf *Weiter*

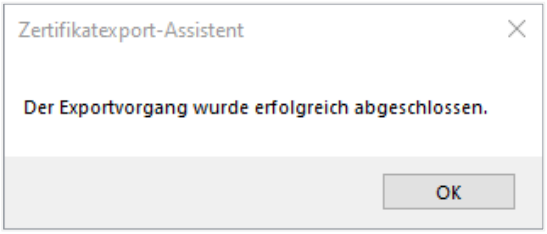


- Wählen Sie nun folgenden Punkt aus und drücken Sie auf *Weiter*



- Klicken Sie auf *Durchsuchen…* und speichern Sie das Zertifikat auf Ihrem Desktop oder an einer beliebigen Stelle.
- Klicken Sie auf *Fertig stellen*

Nach Abschluss des Exports erscheint folgende Meldung:



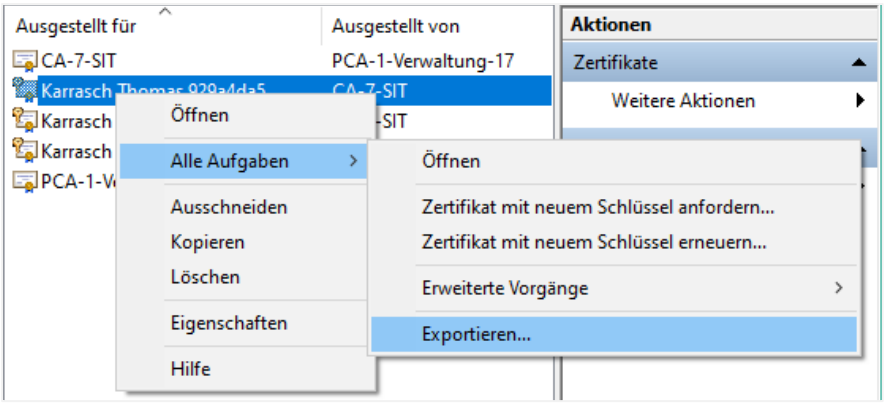
Damit ist der Export des öffentlichen Schlüssels abgeschlossen. Sichern Sie das Zertifikat ggf. mehrfach auf einem externen Datenträger oder einem gesicherten Laufwerk.

Das öffentliche Zertifikat dient zur Weitergabe an alle Stellen, die Ihr Zertifikat zur Verarbeitung benötigen.

5.2. Sicherung des gesamten Zertifikats

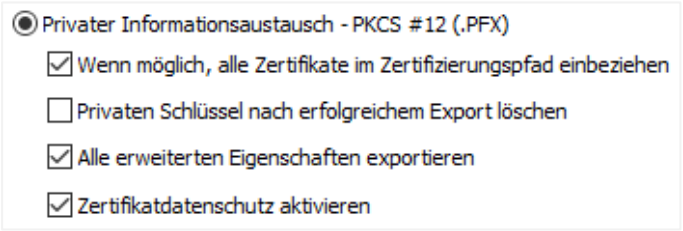
Diesen Schritt benötigen Sie, um das Zertifikat später in das örtliche empfangende System (Fachverfahren) einzuspielen. Bitte führen Sie diesen Export zeitnah nach der Zertifizierung durch, da das private Schlüsselmaterial sonst ausschließlich im Kontext des beantragenden Benutzers auf dem beantragenden Arbeitsplatz verfügbar ist.

- Wählen Sie Ihr Zertifikat aus der Liste aus, machen Sie einen Rechtsklick und wählen Sie *Alle Aufgaben → Exportieren…* aus

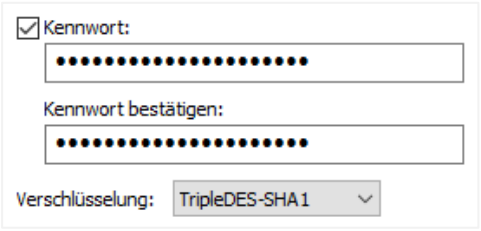


- Bestätigen Sie den Willkommen-Dialog mit *Weiter* und wählen Sie im Folge-Dialog die Option *Ja, privaten Schlüssel exportieren* aus und drücken Sie auf *Weiter*

- Wählen Sie nun folgende Punkte aus und drücken Sie auf *Weiter*



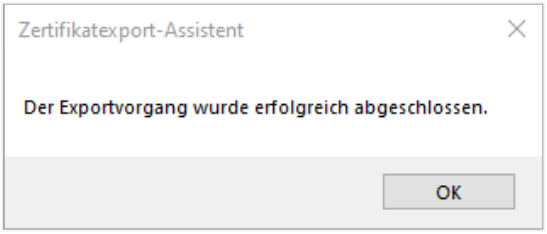
- Aktivieren Sie das Kontrollkästchen Kennwort und vergeben Sie ein Passwort. Dieses wird für den Import auf einem anderen Computer benötigt.



Hinweis: Bitte sichern Sie das Kennwort da ein Import ohne dieses nicht möglich ist!

- Klicken Sie auf *Durchsuchen…* und speichern Sie das Zertifikat auf Ihrem Desktop oder an einer beliebigen Stelle.
- Klicken Sie auf *Fertig stellen*

Nach Abschluss des Exports erscheint folgende Meldung:



Damit ist der Export des Zertifikats mit privatem und öffentlichem Schlüssel abgeschlossen. Sichern Sie das Zertifikat zusammen mit dem Passwort ggf. mehrfach auf einem externen Datenträger oder einem gesicherten Laufwerk.
Stellen Sie sicher, dass der Zugriff auf diese Sicherung des privaten Schlüssels auch im Abwesenheits- / Vertretungsfall gewährleistet ist.