Anmerkung zum

i-mpuls JMD Funktionszertifikat 2025

Stand 8.9.2025

Die Entscheidung zur Ausstellung von Funktionszertifikaten für i-mpuls JMD fiel sehr kurzfristig, so dass die Dokumentation noch im Aufbau ist:

- Die Online-Beantragung des Funktionszertifikats entfällt.
- Sie erhalten in Rücksprache mit dem Servicebüro JMD:
  - per E-Mail eine Import-Datei, aus der sie das Funktionszertifikat in Ihren Browser importieren können.
    Dieses Zertifikat müssen Sie auch an Kolleginnen und Kollegen weitergeben, die Zugriff auf i-mpuls JMD erhalten sollen.
    Die Import-Datei ist verschlüsselt und mit einem Passwort geschützt.
  - per Brief erhalten Sie von uns das Passwort für diese Import-Datei.

Für den Import verweisen wir zunächst auf den Abschnitt „3.6 Verteilung des Zertifikates“ des folgenden „Handbuch Gruppenzertifikat, 2019“. Der Import im Microsoft Edge Browser funktioniert ähnlich wie im beschriebenen Microsoft Internet Explorer. Unterstützt werden ebenso Mozilla Firefox und Google Chrome.

Mit freundlichen Grüßen

Ihre Intevation GmbH

JUGEND
MIGRATIONS
DIENSTE

JMD i-mpuls

Web-Anwendungs-Server für computergestützte Fallakten

Handbuch Gruppenzertifikat

Stand: 21.08.19

Inhaltsverzeichnis

Abkürzungen:

BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority, auch Trust-Center oder Zertifizierungsstelle
SIT (Citkomm)	ehem. „Citkomm“, Südwestfalen-IT, Betreiber der für i-mpuls eingesetzten CA unter der V-PKI.
CP	Certificate Policy, d.h. die Sicherheitsleitlinien
FF	Mozilla Firefox
ggf.	gegebenenfalls
IE	Internet Explorer
PKI	Public Key Infrastruktur, ein System zur Ausstellung, Verteilung und Prüfung digitaler Zertifikate. JMD nutzt ein System unter der V-PKI (Verwaltungs-PKI) des BSI.
PostIdent	Dieses Verfahren bietet eine zertifizierte Methode zur sicheren Identifikation des Antragstellers durch Mitarbeiter der Deutschen Post AG.
PW	Passwort
Trust-Center	Dies ist eine vertrauenswürdige Instanz, die in der elektronischen Kommunikation die jeweilige Identität bescheinigt

1 Wichtiges vorab

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[1] vom Trust-Center. Bis zum **Abschluss** des Antragsprozesses dürfen am **Benutzerprofil auf dem Arbeitsplatzrechner der Antragstellerin bzw. des Antragstellers keine Veränderungen** vorgenommen werden. Dazu zählen z.B. auch Passwortänderungen und die Installation von Software, insbesondere Updates des Microsoft Internet Explorers bzw. des Mozilla Firefox.

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.

Nur zusammen funktionieren beide Teile als Zertifikat. Daher ist es besonders wichtig den Prozess zeitnah zu beenden und abschließend den erfolgreichen Import zu überprüfen. Lesen Sie hierzu bitte das Kapitel 3.5.2 bzw. 3.5.4).

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	Beantragung und Erst-Installation des Zertifikates sind mit dem Microsoft Internet Explorer und Mozilla Firefox möglich, die Verwendung ist auch mit Opera, Safari u.a. Browsern möglich.
Speicher	Automatisch unter Eigene/Ihre Zertifikate im jeweiligen Zertifikatsmanager.

[1] Die Signaturdatei heißt userCertifcate.p7b nur beim IE.

2 Einleitung

JMD i-mpuls ist eine Web-Anwendung, bei der die Mitarbeiterinnen bzw. Mitarbeiter verschlüsselt über das Internet mit dem Server kommunizieren. Um die Echtheit der Kommunikationspartner zu gewährleisten, werden an beiden Enden der Datenverbindung Zertifikate eingesetzt. Die Web-Anwendung akzeptiert nur Verbindungen von Stellen, die ihr als **vertrauenswürdig** bekannt sind. Im Gegenzug ist auch für die Einrichtungen sichergestellt, dass sie direkt und über eine gesicherte Verbindung mit i-mpuls kommunizieren. Zertifikate für einzelne Einrichtungen werden als Gruppenzertifikate (X.509) vergeben. Die Zertifikatverwaltung wird vom Trust-Center der SIT (Citkomm) betrieben.

Insgesamt wird ein dreistufiges Verfahren implementiert: Zunächst wird über das **Serverzertifikat** das JMD i-mpuls System gegenüber der Anwenderin bzw. dem Anwender authentifiziert. Durch das **Gruppenszertifikat** wird die Anwenderin bzw. der Anwender als Mitarbeiterin bzw. Mitarbeiter einer Einrichtung authentifiziert. Im letzten Schritt authentifiziert sich die Mitarbeiterin bzw. der Mitarbeiter durch **Benutzername und Passwort** persönlich.

Die Gruppenzertifikate basieren auf einer Public-Key-Infrastruktur. Neben öffentlichen Schlüsseln (Public-Key), die vom Trust-Center digital signiert werden (und damit Zertifikate werden), gehört dazu auch der private Schlüssel einer jeden Einrichtung. Ohne diese beiden Teile ist eine Benutzung der Zertifikate zur Authentifizierung nicht möglich. Die Zertifikate sind maximal **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 4.1 „Dokumentation“ verwiesen.

3 Der Zertifizierungsprozess

Die **Beantragung** eines Zertifikats ist aus technischen Gründen **nur** unter **Microsoft Windows** über einen **Internet-Explorer (IE) oder über Mozilla Firefox (FF) möglich**. Andere Browser werden bei der Beantragung nicht unterstützt. Bereits erstellte Zertifikate können jedoch mit anderen Browsern benutzt werden.

Der Prozess für ein Gruppenzertifikat teilt sich in mehrere Schritte:

1. Antragsstellung über cas.citkomm.de (nur mit IE oder FF unter Microsoft Windows möglich)
2. Drucken des Namensvergabedokuments und Versand an das Trust-Center der SIT (Citkomm)
3. Authentisierung durch PostIdent-Verfahren
4. Herunterladen und Erst-Installation des Zertifikates
5. Export/Import des Zertifikates (Verteilung an Mitarbeiterinnen bzw. Mitarbeiter, alle Browser)

Für den Zertifizierungsprozess wird in jeder Einrichtung eine **Verantwortliche bzw. ein Verantwortlicher** festgelegt. Diese Person führt die Beantragung des Zertifikats durch. Name und E-Mail Adresse dieser Person müssen dem Servicebüro Jugendmigrationsdienste mitgeteilt werden. Die Schritte bis zum Verteilen des Zertifikates an die einzelnen Mitarbeiterinnen und Mitarbeiter der Einrichtungen finden auf **einem Rechner unter dem Nutzerkonto der verantwortlichen Person** statt.

3.1 Notwendige Vorbereitungen und Hinweise

- Windows Internet Explorer Version 11

Der Zertifizierungsprozess kann mit dem Microsoft Windows Internet Explorer ab Version 11 nur noch im Kompatibilitätsmodus durchgeführt werden. Folgen Sie dazu bei Bedarf der Anleitung unter Punkt 9 der „FAQ“, Abschnitt 4.2.

- Microsoft Windows 7 (und neuer) mit Windows Internet Explorer

Für den Zertifizierungsprozess mit Windows Internet Explorer sind ab Microsoft Windows 7 weitere Einstellungen notwendig, unabhängig von der Version des Windows Internet Explorers. Folgen Sie dazu bei Bedarf der Anleitung unter Punkt 10 der „FAQ“, Abschnitt 4.2.

3.2 Die Antragsstellung

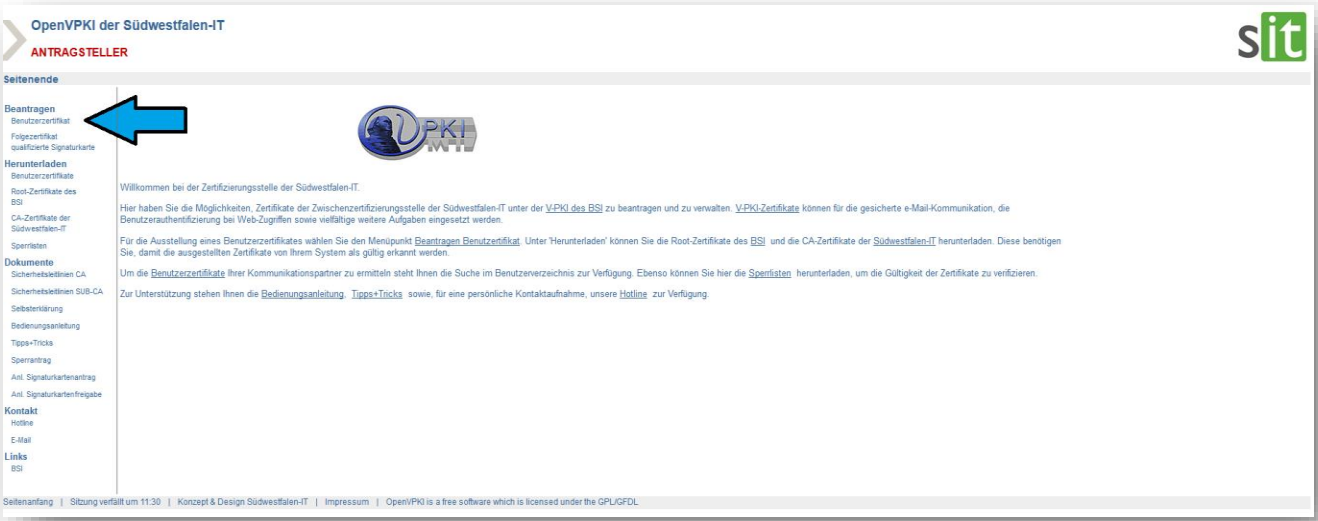
Im Schritt der Antragsstellung wird ein Schlüsselpaar erstellt. Dieses Paar besteht aus einem öffentlichen und privaten Schlüssel. Der öffentliche Teil wird an das Trust-Center der SIT (Citkomm) zur Signatur übermittelt. Zusammen fungiert das Schlüsselpaar später dann als „Gruppenzertifikat“.

Gehen Sie bitte wie folgt bei der Antragstellung vor:

a. Öffnen Sie mit dem Microsoft Internet Explorer bzw. mit dem Mozilla Firefox 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“).



b. Wählen Sie aus dem linken Menü „Beantragen“ > „Benutzerzertifikat" aus. Es werden nun schrittweise die notwendigen Angaben zum öffentlichen Schlüssel abgefragt:

(1) Räumliche Ordnung: Wählen Sie „SIT (Citkomm)".

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.

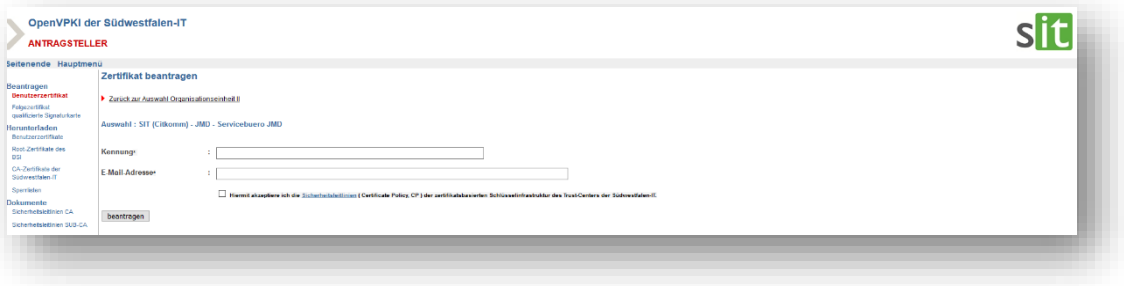
(2) Organisationseinheit I: Wählen Sie „JMD“.

(3) Organisationseinheit II: Wählen Sie hier den Namen Ihrer Einrichtung.

(4) Es öffnet sich ein Dialog mit zwei Eingabeelementen:

- Kennung: Geben Sie hier bitte den vierstelligen Ziffernblock der Förderkennziffer[2] an. Über diese Angabe wird später Ihre Einrichtung identifiziert.
- E-Mail-Adresse: Geben Sie hier bitte Ihre E-Mail-Adresse ein (verwenden Sie die gleiche Adresse, die Sie dem Servicebüro Jugendmigrationsdienste mitgeteilt haben), diese ist für den weiteren Ablauf der Zertifikatsvergabe notwendig!

c. Abschließend akzeptieren Sie bitte die Sicherheitsleitlinien. Diese sind verlinkt und können nachgelesen werden.



d. Klicken Sie auf „beantragen".

e. Prüfen Sie die getroffenen Angaben im folgenden Dialog und bestätigen Sie diese - oder gehen Sie zurück („Zurück zur Auswahl Organisationseinheit II“), um die Angaben zu korrigieren.

Achtung: Nach der Bestätigung wird der private Schlüssel als Teil des Zertifikats auf Ihrem PC gespeichert. 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.

[2]Die Kennung können Sie vom Servicebüro Jugendmigrationsdienste erfragen

Hinweise zu möglichen Fehlermeldungen:

Nach der Bestätigung kann es zu einer Fehlermeldung kommen, die je nach dem installierten Betriebssystem anders lautet und auch andere Reaktionen erfordert.

- *Beim Betriebssystem MS/Win 7 lautet die Meldung:*

  „Automatisierungsserver kann Objekt nicht erstellen".

- *Hier müssen Sie die Seite https://cas.citkomm.de zu den vertrauenswürdigen Sites hinzufügen. Hinweise hierzu finden Sie im Dokument „Tipps und Tricks" auf der Seite https://cas.citkomm.de im Bereich „Dokumente".*

- *Beim Betriebssystem MS/XP lautet die Meldung:*

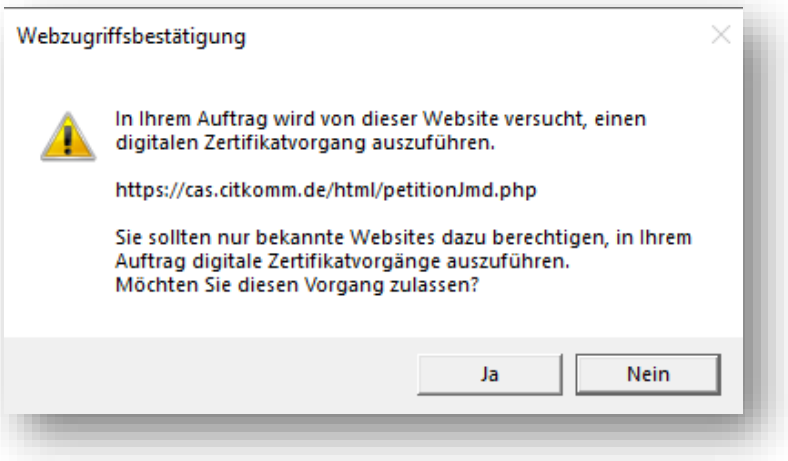
  „Objekt unterstützt diese Eigenschaft oder Methode nicht".

  - *Es fehlt meist eine für die Schlüsselerstellung notwendige Funktion die sich jedoch leicht aktivieren lässt.*
  - *Hinweise zur Lösung finden Sie unter der Nummer 8 der „FAQ" unter Abschnitt 4.2.*

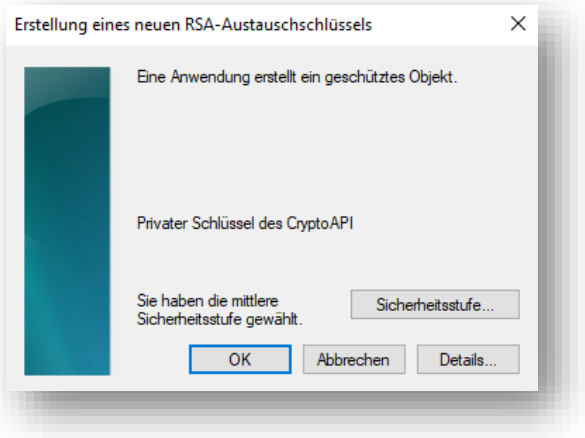
f. Nach der Bestätigung unterscheiden sich die Dialoge je nachdem, ob der Internet Explorer oder Mozilla Firefox verwendet wird:

Internet Explorer:

a. Es folgt eine **Sicherheitsabfrage** („Webzugriffsbestätigung"), die Sie bitte mit „Ja" bestätigen



b. In den folgenden Dialogen werden weitere Einstellungen für das **Schlüsselpaar** abgefragt:

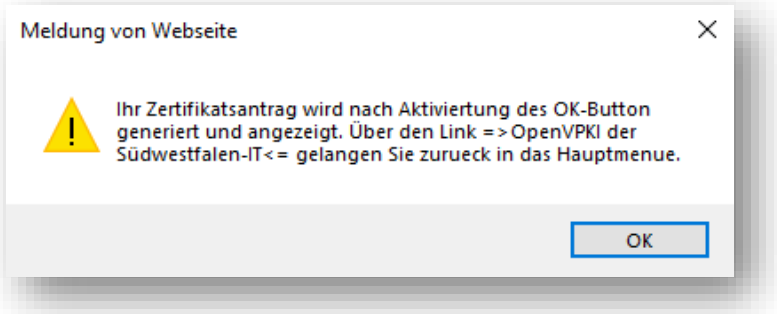


c. Bestätigen Sie die folgenden Dialoge mit „OK“.

d. Das Schlüsselpaar wird erstellt und der öffentliche Teil an das Trust-Center übermittelt.

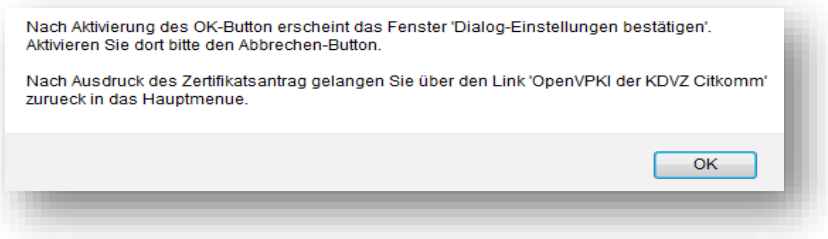
Achtung: Durch eventuelle Veränderungen am Benutzerprofil auf dem Antragsrechner könnte der **private Schlüssel** vor Abschluss des Zertifizierungsprozess **unbenutzbar** werden.

e. Anschließend erfolgt eine Bestätigung und die Aufforderung, den Zertifikatsantrag zu drucken; spätestens mit dieser Aufforderung sollte der angeschlossene Drucker betriebsbereit sein:

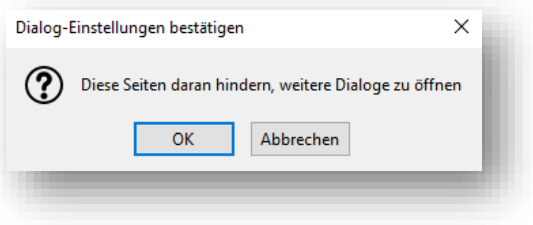


Firefox:

a. Nach dem Klicken auf „Bestätigung“ wird der Schlüssel generiert:



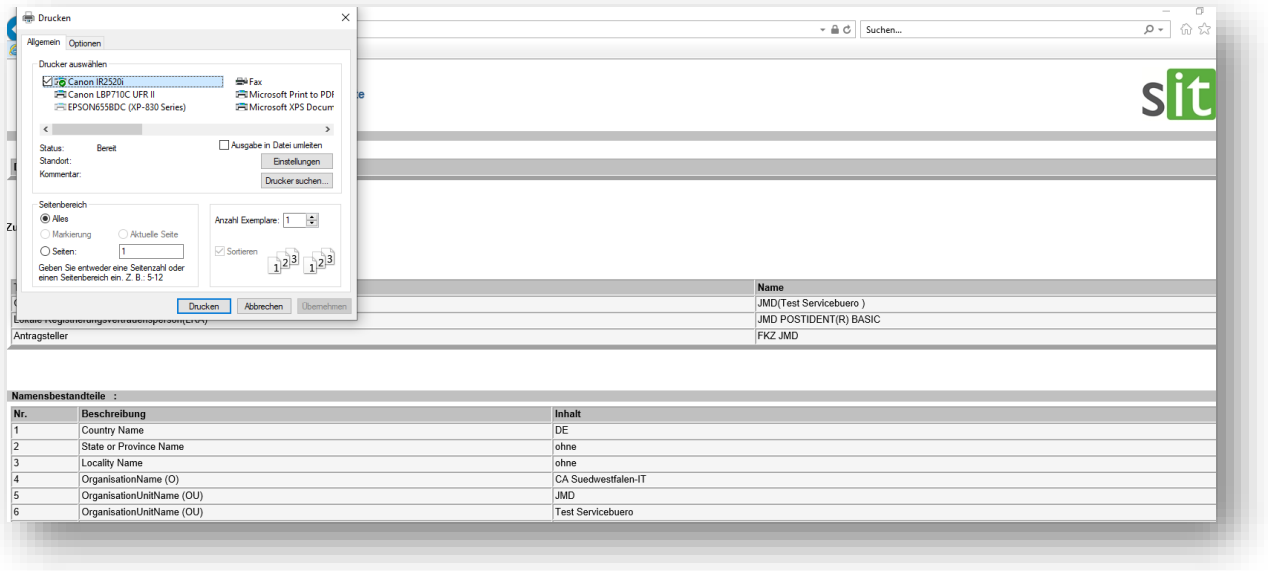
b. Klicken Sie auf „OK“



c. Klicken Sie auf „Abbrechen“

Achtung: Es wichtig, dass Sie hier auf „Abbrechen“ klicken, damit Ihr Zertifikatsantrag (Namensvergabedokument) gedruckt werden kann.

3.3 Drucken des Namensvergabedokumentes



Drucken Sie den Zertifikatsantrag (Namensvergabedokument) aus und unterschreiben Sie diesen als Antragssteller auf der zweiten Seite unten, er wird im weiteren Verfahren benötigt.

Ohne diesen Ausdruck kann kein Zertifikat erstellt werden!

Setzen Sie sich bei Problemen ggf. mit der Hotline oder dem Servicebüro Jugendmigrationsdienste in Verbindung – der Antrag muss bei versäumtem Ausdruck nicht erneut gestellt werden.

Faxen Sie das Namensvergabedokument an die Faxnummer, die im Anhang der u.g. E-Mail genannt ist, oder senden Sie als per E-Mail an pki@citkomm.de und bewahren Sie es sorgfältig auf.

Damit sind die ersten zwei Schritte des Zertifizierungsprozesses abgeschlossen. Den Browser können Sie jetzt wieder schließen. Sie erhalten eine E-Mail, welche Sie bestätigen sollen, diese enthält als Anhang eine PDF-Datei. Die PDF-Datei ist ein Brief des Trust-Centers der SIT (Citkomm). Drucken Sie ihn aus und schneiden Sie den Coupon ab. Diesen Coupon brauchen Sie für das PostIdent-Verfahren.

3.4 Authentisierung durch PostIdent-Verfahren

Die Prüfung eines Antrags und die damit verbundene Authentisierung der Antragstellerin bzw. des Antragstellers sind notwendig, wenn sich die in der Einrichtung für das Zertifikat verantwortliche Person oder deren Namen geändert hat. Diese kann in einer beliebigen Filiale der Deutschen Post AG vorgenommen werden. Das Trust-Center der SIT (Citkomm) bietet dafür das PostIdent-Verfahren an. Dieser zertifizierte Dienst der Deutschen Post AG übernimmt dann Teilaufgaben der Überprüfung.

Achtung: Vor dem Hintergrund der persönlichen Authentisierung ist es notwendig, Änderungen in der Zuständigkeit für die Zertifikatsbeantragung mit einem formlosen Schreiben dem Servicebüro Jugendmigrationsdienste mitzuteilen.

Sie erhielten innerhalb der Antragsstellung via E-Mail ein Schreiben (PDF-Brief) des Trust-Centers mit einem Coupon für das PostIdent-Verfahren (s.o.).

Um das PostIdent-Verfahren abzuschließen benötigen Sie folgende Dokumente:

- Ihren **gültigen** Personalausweis oder Reisepass, für die Identifikation bei der Post
- Den abgetrennten Coupon aus dem PDF-Brief

Gehen Sie mit Ihrem gültigen Ausweisdokument und dem Coupon persönlich zu einer Filiale der Deutschen Post AG. Die weiteren Schritte werden am Schalter durchgeführt.

3.5 Herunterladen und Erst-Installation des Zertifikates

Nach erfolgreicher Durchführung des PostIdent-Verfahrens **signiert** das Trust-Center der SIT (Citkomm) Ihren **öffentlichen Schlüssel** und stellt ein Zertifikat zur Verfügung. Die Antragstellerin bzw. der Antragsteller erhält automatisch eine entsprechende E-Mail an die im Zertifikatsantrag angegebene Adresse.

Wichtig: Es ist zwingend notwendig das Zertifikat am Antragsrechner in den für die Antragstellung verwendeten Internet-Browser einzuspielen. Erst in diesem Schritt werden der private und jetzt signierte öffentliche Schlüssel wieder zusammengefügt, so dass diese als „Gruppenzertifikat“ fungieren können.

*V-PKI der KDVZ Citkomm

Sehr geehrte Antragstellerin, sehr geehrter Antragsteller,

Sie koennen Ihr beantragtes Zertifikat mit der Nummer 3364 nun von unserem Server direkt unter folgender Adresse herunterladen:

http://cas.citkomm.de/html/petitionLdapUserServerDownloadGet.php?attr=ser=3364,CN=Mustermann~Erika~8477efa9,OU=Standesamt,OU=Stadt Geseke,O=Citkomm,C=DE

Eine Anleitung zur Installation und Sicherung des Zertifikats finden Sie unter folgender Adresse: http://cas.citkomm.de/dokument/Install_Zert.pdf

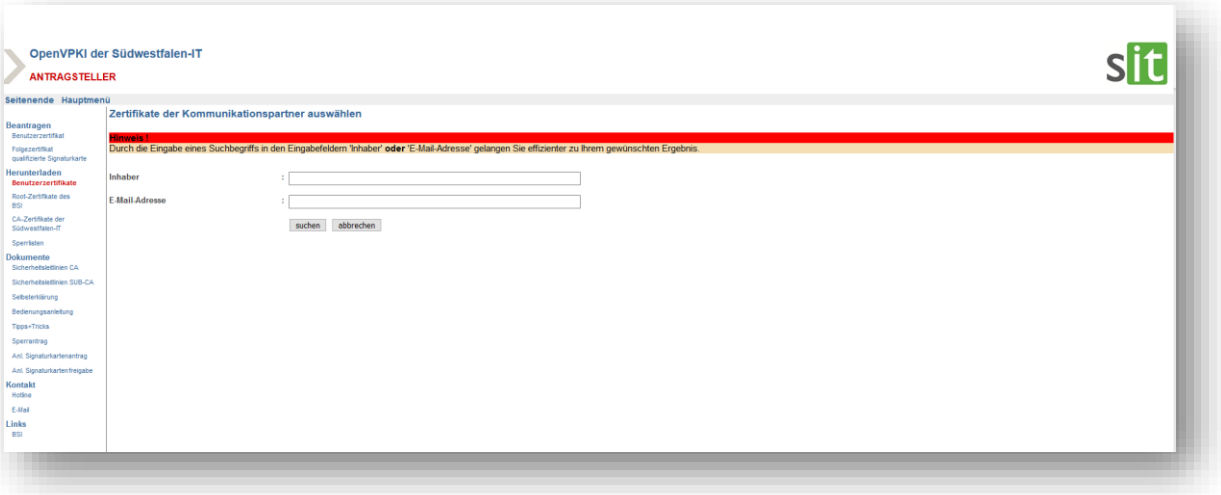
Bitte beachten Sie, dass Sie eine Sicherungskopie Ihres Zertifikates mit Ihrem privaten Schluessel erzeugen. Wenn der private Schluessel verloren geht, sind Sie nicht mehr in der Lage, mit diesem Zertifikat zu arbeiten.

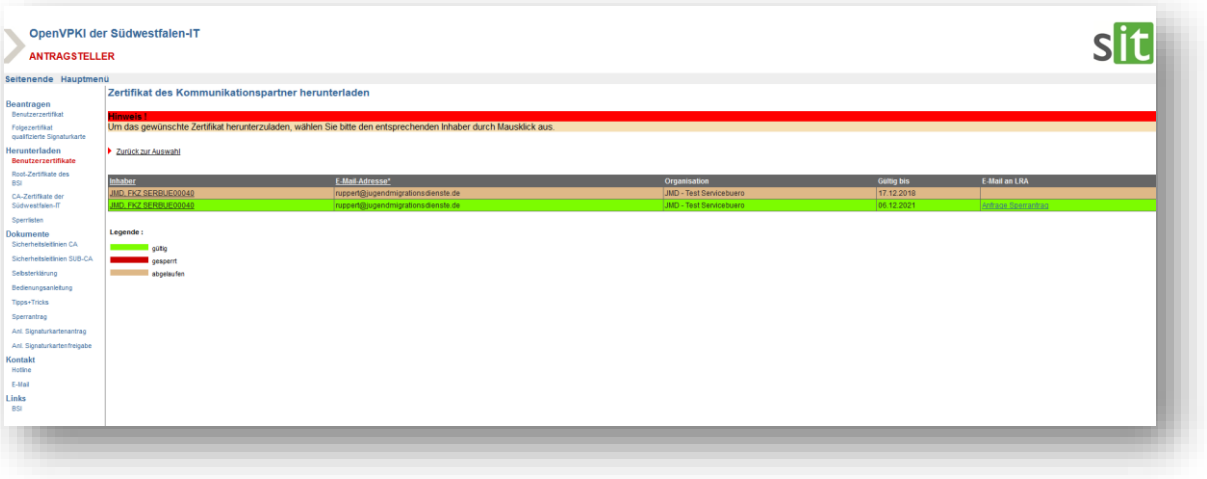
Sollten Sie diese Mail erhalten haben, obwohl Sie persoenlich kein Zertifikat beantragt haben, senden Sie bitte diese Mail an pki@citkomm.de der KDVZ Citkomm.

Wenn der angegebene Link in der E-Mail (siehe oben blau unterlegt) nicht läuft und es zu einer Fehlermeldung kommt, kann das an der Konfiguration Ihres E-Mail-Programms liegen, das Dokument „Tipps+Tricks“ (auf der Seite https://cas.citkomm.de im Bereich „Dokumente“) enthält entsprechende Hinweise. In diesem Fall haben Sie die Möglichkeit das Zertifikat über das Webportal cas.citkomm.de herunterzuladen:

a. Wählen Sie bitte „Herunterladen“ > „Benutzerzertifikate“ und geben Ihre E-Mail-Adresse ein, die Sie bei der Antragstellung benutzt haben.

b. Klicken Sie auf den Button „Suchen“



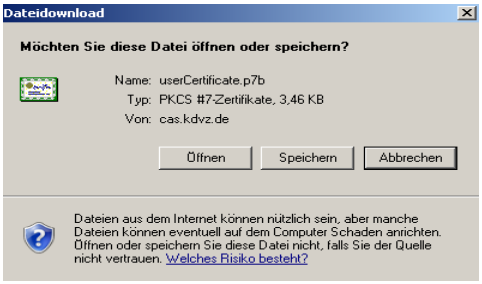


Die bisherigen Schritte sind für den Internet Explorer (IE) und Firefox (FF) identisch. Die folgenden Schnitte unterschieden sich bei den Browsern. Zunächst wird der weitere Verlauf für den Internet Explorer und anschließend für Mozilla Firefox beschrieben.

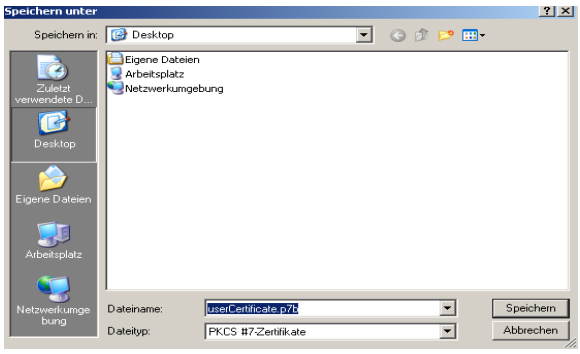
3.5.1 Herunterladen und Erst-Installation (Internet-Explorer)

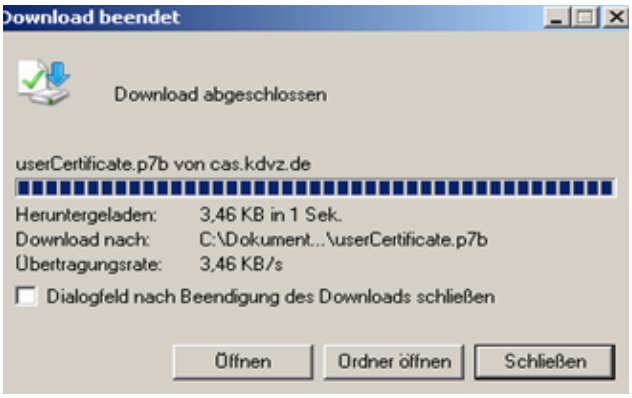
Die folgenden Schritte sind am gleichen Rechner, mit dem gleichen Benutzerprofil auszuführen, an dem auch der Zertifikatsantrag gestellt wurde. Sie benötigen erneut den Microsoft **Internet-Explorer**:

a) Benutzen Sie den in der E-Mail enthaltenen Link oder den oben beschriebenen Weg über das Webportal cas.citkomm.de, um eine Datei mit der Endung *.p7b* herunterzuladen. Die Datei kann mit Klick auf den **„Speichern-Knopf“** auf dem lokalen Rechner in einem beliebigen Verzeichnis oder auf dem Desktop (wovon in der folgenden Erläuterung ausgegangen wird) gespeichert werden:



b) Speichern Sie die Transport-Datei „userCertifcate.p7b“ auf dem Desktop ab.



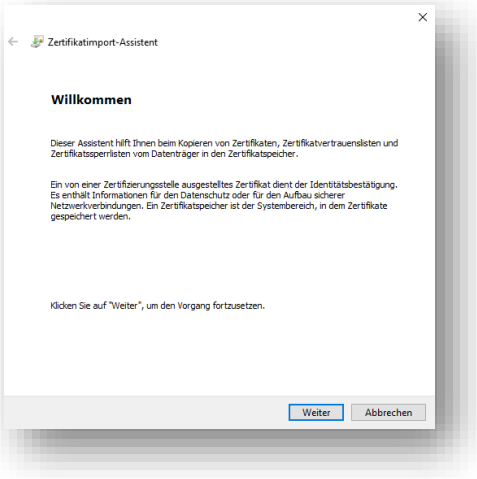


c) Nach dem Ende des Downloads können Sie das Fenster schließen. Auf dem Desktop, bzw. dem entsprechen gewählten Verzeichnis finden Sie die Datei „userCertificate.p7b“.

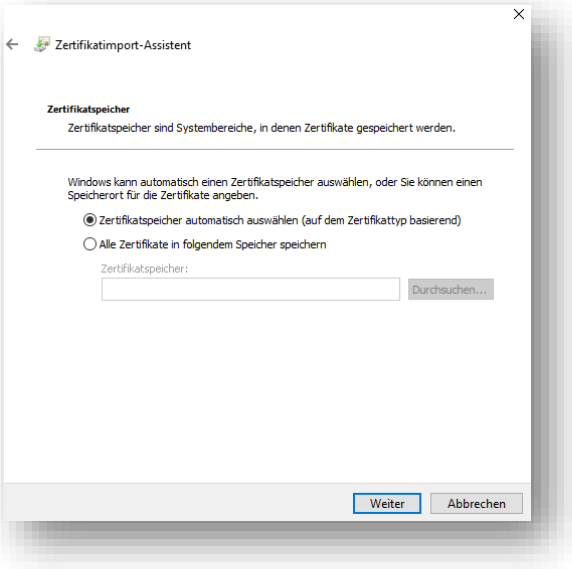
d) Klicken Sie anschließend die Datei mit der rechten Maustaste an und rufen den Installationsassistenten mit einem Klick auf **„Zertifikat installieren“** auf.

e) Der **Assistent** führt Sie durch die einzelnen Schritte des Imports, die Abfragen sind jeweils zu bestätigen.

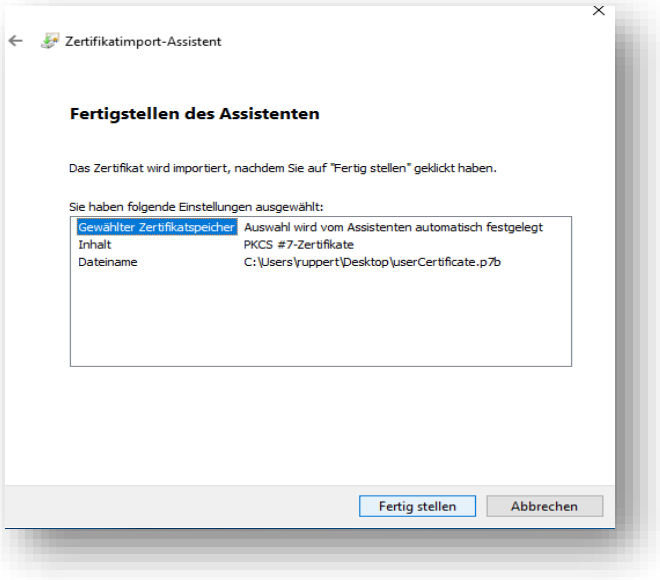
(1) „Willkommen“: Bestätigen Sie mit „Weiter“.



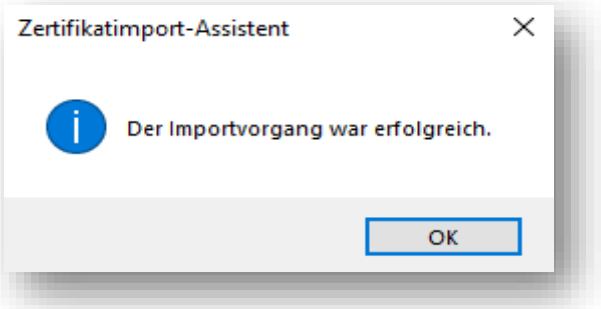
(2) „Zertifikatsspeicher“: Ohne Änderung – bestätigen Sie mit „Weiter“



(3) Bestätigen Sie mit Klick auf „Fertig stellen“



(4) Bestätigen Sie den abschließenden Dialog mit „OK“



f) Es werden das eigene Zertifikat unter Eigene Zertifikate, das Zertifikat der SIT (Citkomm) als vertrauenswürdige Zwischentertifizierungsstelle und das Zertifikat der Wurzelzertifizierungsstelle des BSI (Bundesamt für Sicherheit in der IT) als vertrauenswürdige Stammzertifizierungsstelle im Zertifikatspeicher installiert. Dabei erfolgt ggf. eine Sicherheitsabfrage bezüglich des Wurzelzertifikats/Stammzertifikats PCA-1-Verwaltung-15. Sie können sich das Zertifikat anzeigen lassen und die Korrektheit anhand des Fingerabdrucks überprüfen (Groß-/Kleinschreibung und Füllzeichen wie Doppelpunkte sind dabei nicht relevant) **Fingerabdruck (SHA-1):**

PCA-1-Verwaltung-17:

```
97 74 0f 27 83 b9 85 4d ad 72 4b 13 f3 d6 c7 52 f7 f4 6c c3
```

CA-7-SIT:

```
18 eb c7 c1 5e f9 df e7 da 25 78 36 72 65 ae ab 86 60 2f cb
```

- Stimmt der Fingerabdruck mit diesem Wert überein, so handelt es sich um das korrekte Zertifikat. Sie können dem Zertifikat vertrauen und es daher entsprechend weiter installieren.
- Stimmt der Fingerabdruck nicht überein, kontaktieren Sie bitte die Hotline der SIT (Citkomm) oder das Servicebüro Jugendmigrationsdienste.

Wichtig! Bitte überprüfen Sie den Fingerabdruck des Wurzelzertifikats immer an dieser Stelle.

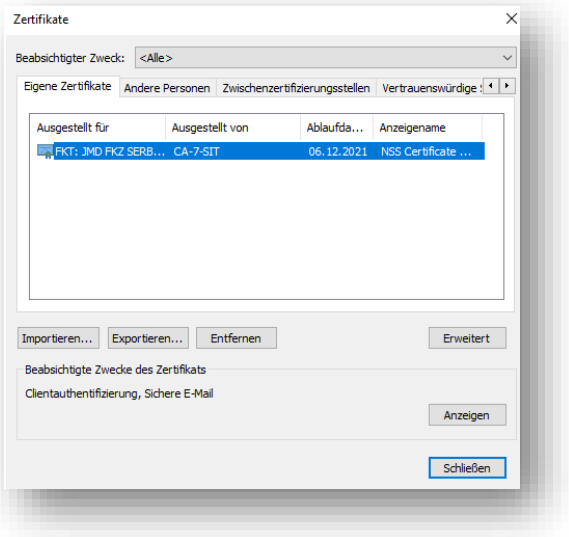
Damit ist die Installation abgeschlossen. Bitte fahren Sie anschließend damit fort, den Import zu überprüfen.

Import überprüfen

Der erfolgreiche Import sollte in jedem Fall überprüft werden. Insbesondere wenn Sie noch ein gültiges Zertifikat installiert haben und somit erst nach dessen Auslaufen feststellen, ob der Import tatsächlich erfolgreich war, ist dieser Schritt wichtig.

Öffnen Sie hierzu bitte den **Zertifikatsmanager des Internet-Explorer:**

> Menü „Extras“ > „Internetoptionen“ > „Inhalte“ > „Zertifikate“ > „**Eigene Zertifikate**“ anzeigen



Der Reiter „Eigene Zertifikate“ zeigt nach einem erfolgreichen Import das neue Zertifikat, mit maximal drei Jahren Gültigkeitsdauer.

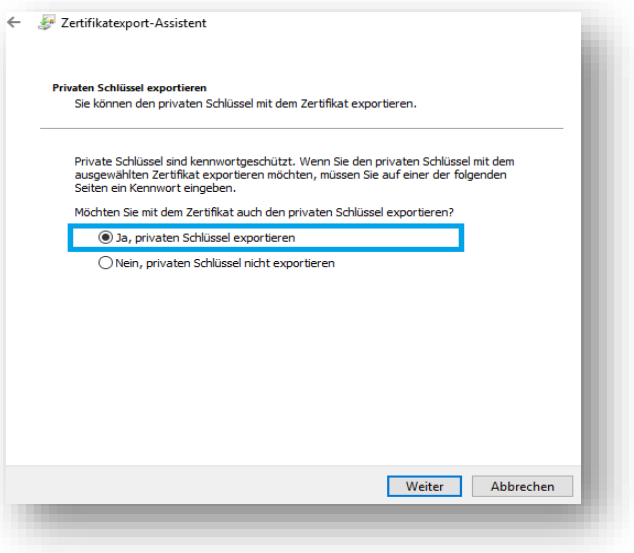
Achtung: Ist dies nicht der Fall, ist der Import nicht erfolgreich gewesen. Wenn das Zertifikat anstatt unter „Eigene Zertifikate“ im Reiter „Andere Personen“ gespeichert wurde, scheint es Probleme mit Ihrem privaten Schlüssel zu geben. Erste Ansätze zur Problembehebung beim Import finden Sie unter Punkt (3) der „FAQ, Abschnitt 4.2.

Hinweis: Nach Abschluss des Imports sollte eine Sicherungskopie des Zertifikates (öffentlicher **und** privater Schlüssel) erstellt werden. Die Schritte dazu sind identisch mit den ersten Schritten zur Verteilung des Zertifikates an die Mitarbeiterinnen und Mitarbeiter und werden im Folgenden erläutert.

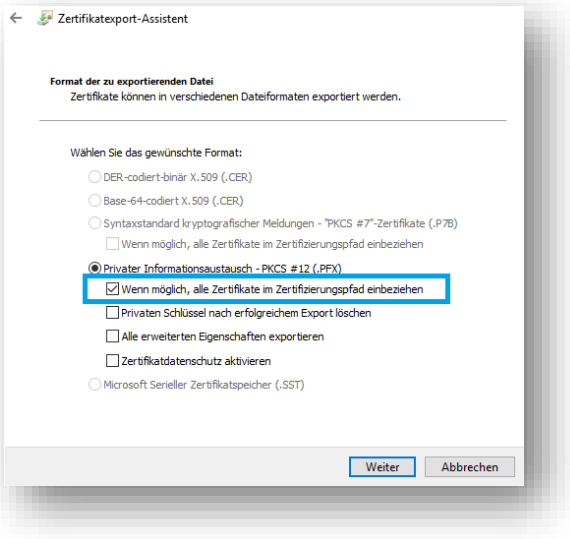
3.5.2 Sicherung / Export des Zertifikates (Internet Explorer)

Export /Sicherung des Zertifikates

1. Wählen Sie wie oben den Zertifikatspeicher des Internet Explorers: > Menü „Extras“ > „Internetoptionen“ > „Inhalte“ > „Zertifikate“ > „Eigene Zertifikate“.
2. Markieren Sie das zu exportierende Zertifikat und wählen „Exportieren“, ein Assistent führt Sie durch die einzelnen Schritte des Exports:



Stellen Sie sicher, dass Sie den **privaten Schlüssel** mit exportieren. **Ohne** den privaten Schlüssel funktioniert das Zertifikat auf anderen Rechnern **nicht!**



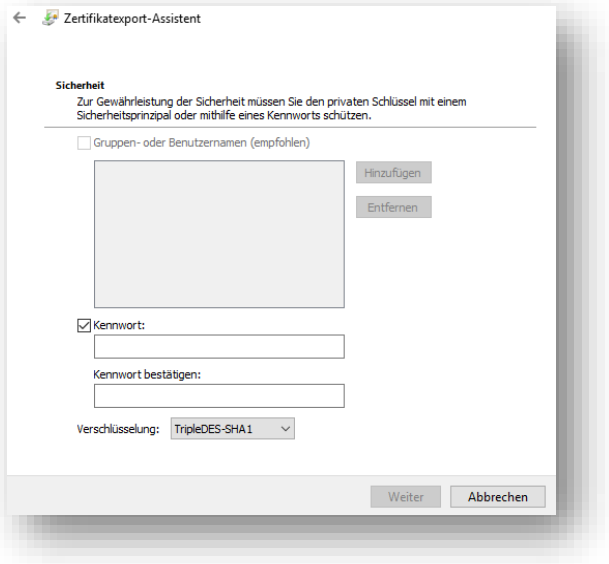
Für den Export ist das Format „PKCS #12“ vorgegeben. Wählen Sie ggf. die Option „Wenn möglich alle Zertifikate im Zertifizierungspfad einbeziehen“, um auf weiteren Rechnern nicht wieder die volle Zertifikatskette einzeln importieren zu müssen. Eine unvollständige Zertifikatskette muss gemäß den Schritten unter Abschnitt 3.5 „Herunterladen und Erst-Installation des Zertifikates

Herunterladen und Erst-Installation des Zertifikates“ ergänzt werden.

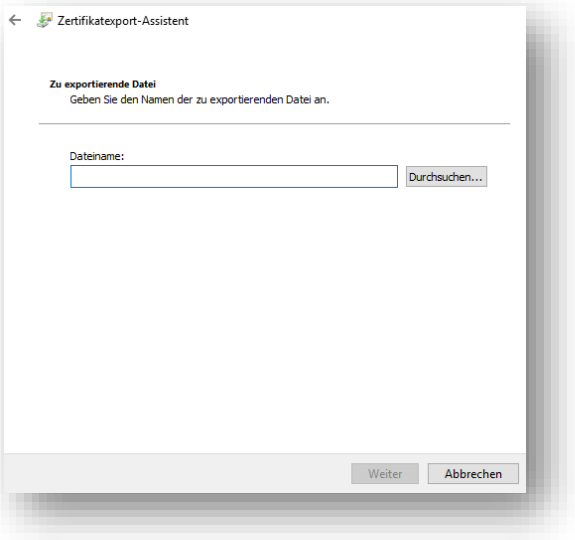
a. Stellen Sie sicher, dass der private Schlüssel nicht gelöscht wird, wenn Sie das Zertifikat auch auf diesem Rechner benutzen wollen!

b. Sie werden aufgefordert, den exportierten Schlüssel durch ein Kennwort zu schützen. Sie

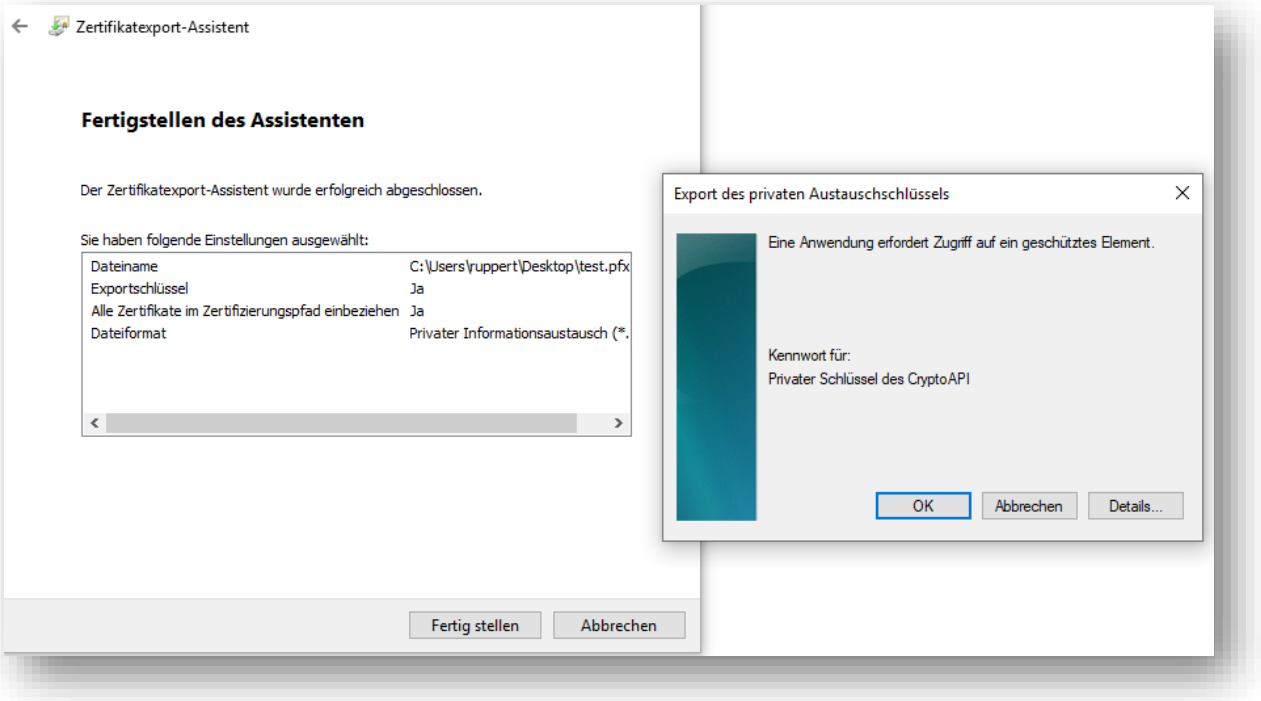
benötigen dieses Kennwort, um den Schlüssel und das Zertifikat auf einem anderen Rechner zu importieren.



c. Wählen Sie abschließend einen Dateinamen, unter dem der exportierte Schlüssel abgelegt werden soll. Erzeugt wird eine Datei mit der Endung .pfx. Aus dieser Sicherungsdatei kann das Zertifikat und der private Schlüssel jederzeit wiederhergestellt werden. Damit sind alle notwendigen Eingaben für den Assistenten getätigt.



3. Wählen Sie „Fertigstellen“, um nun das Zertifikat und den privaten Schlüssel zu exportieren.



Der private Schlüssel und das Gruppenzertifikat sind damit exportiert und befinden sich in einer Datei mit der typischen Endung .p12 bzw. .pfx

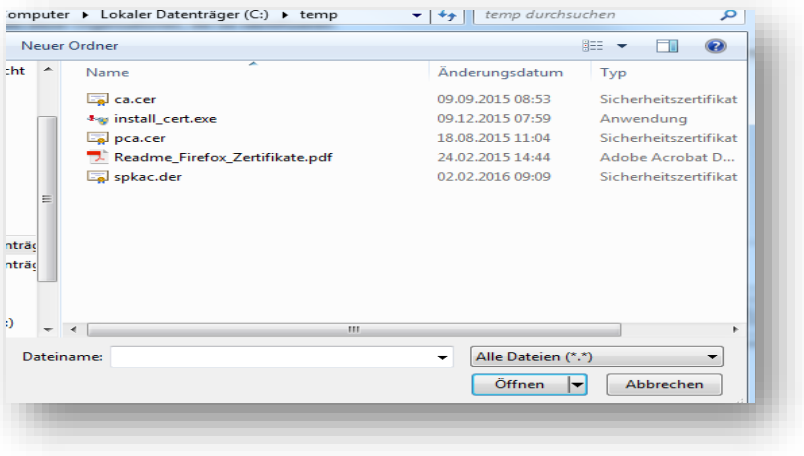
Achtung: Wir empfehlen die Daten auf einem einzigen Datenträger, z.B. einem USB-Stick, zu speichern, der zur Verteilung des Zertifikats und des privaten Schlüssels dient und abschließend als Datensicherung verwahrt werden kann. Stellen Sie dabei auch sicher, dass Sie sich an das Passwort der Exportdatei erinnern können. Wir raten von einem Versand der Exportdatei per E-Mail ab. Dies birgt ein Sicherheitsrisiko, da Unberechtigte unbemerkt eine Kopie der Exportdatei erlangen könnten und anschließend beliebig Zeit/Versuche haben, Ihr Passwort zu raten.

3.5.3 Herunterladen und Erst-Installation des Zertifikats (Mozilla Firefox)

Wenn Sie einen Zertifikatsantrag mit Mozilla Firefox gestellt haben, beachten Sie bitte folgende Hinweise zur Installation Ihres Zertifikats:

a. Sie haben von der Zertifizierungsstelle der SIT (Citkomm) einen Link erhalten. Über diesen Link laden Sie bitte eine **ZIP Datei** auf Ihren Computer, z.B. 10822.zip
b. Bitte stellen Sie sicher, dass im Laufwerk C der Ordner **temp** auf Ihrem Computer vorhanden ist, **ein anderer Ordner ist nicht zulässig**. Sollten Sie den Ordner **C:/temp** nicht vorfinden, erstellen Sie bitte einen entsprechenden Ordner. In manchen Fällen muss die IT temporär die Berechtigung dafür erteilen!

c. Entpacken (extrahieren) Sie bitte die ZIP-Datei in diesen Ordner. Es dürfen nur die 5 Dateien in dem Ordner sein. Achten Sie darauf, dass kein Unterordner vorhanden ist:



d. Bitte alle Webportale im Firefox schließen.

e. Bitte führen Sie die exe-Datei durch Doppelklick in C:/temp aus.

f. Wenn die Datei **install_cert.exe** ausgeführt wurde, erscheint in manchen Fällen der „Programmkompatibilitätsassistent“. In der Regel ist ihr Zertifikat aber dennoch richtig installiert. Den **Assistenten** bitte mit **„Das Programm wurde richtig installiert“** beenden.

g. Es werden nun in den Zertifikatsspeicher Ihres Firefox Browser drei Zertifikate installiert: Ihr eigenes Zertifikat, welches Sie beantragt haben, das Zertifikat der SIT (Citkomm) und das Zertifikat des BSI.

Sie können sich das Zertifikat anzeigen lassen und die Korrektheit anhand des Fingerabdrucks überprüfen (Groß-/Kleinschreibung und Füllzeichen wie Doppelpunkte sind dabei nicht relevant)

Fingerabdruck (SHA-1):

PCA-1-Verwaltung-17:

```
97 74 0f 27 83 b9 85 4d ad 72 4b 13 f3 d6 c7 52 f7 f4 6c c3
```

CA-7-SIT:

```
18 eb c7 c1 5e f9 df e7 da 25 78 36 72 65 ae ab 86 60 2f cb
```

- Stimmt der Fingerabdruck mit diesem Wert überein, so handelt es sich um das korrekte Zertifikat. Sie können dem Zertifikat vertrauen und es daher entsprechend weiter installieren.
- Stimmt der Fingerabdruck nicht überein, kontaktieren Sie bitte die Hotline der SIT (Citkomm).

Wichtig! Bitte überprüfen Sie den Fingerabdruck des Wurzelzertifikats immer an dieser Stelle.

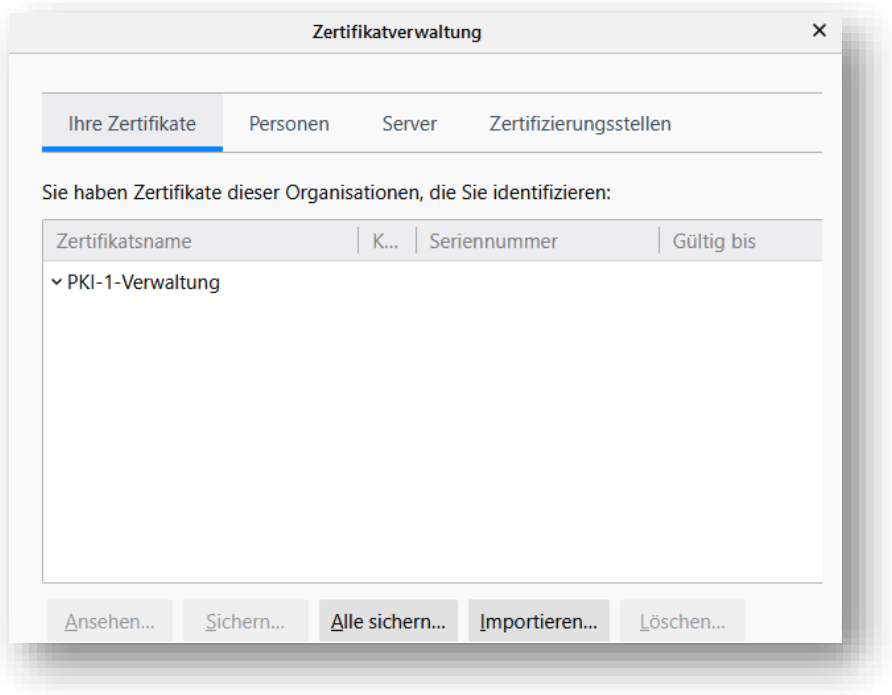
Damit ist die Installation abgeschlossen. Bitte fahren Sie anschließend damit fort, den Import zu überprüfen.

Import überprüfen

Der erfolgreiche Import sollte in jedem Fall überprüft werden. Insbesondere wenn Sie noch ein gültiges Zertifikat installiert haben und somit erst nach dessen Auslaufen feststellen, ob der Import tatsächlich erfolgreich war, ist dieser Schritt wichtig.

a. Öffnen Sie hierzu bitte den **Zertifikatsmanager des Mozilla Firefox:**

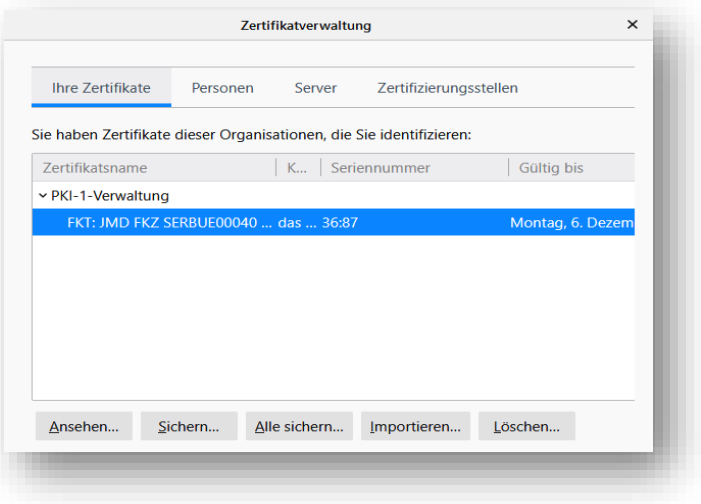
   Extras > Einstellungen > Erweitert > Zertifikate anzeigen > Ihre Zertifikate.



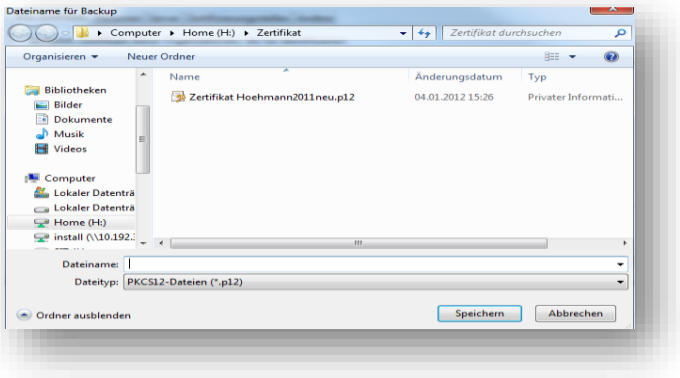
b. Sollte ihr Zertifikat nicht angezeigt werden, wenden Sie sich an die Support Hotline oder das Servicebüro Jugendmigrationsdienste.

3.5.4 Sicherung des Zertifikates / Export (Mozilla Firefox)

b. Lassen Sie sich zunächst Ihre Zertifikate anzeigen: Menü > Einstellungen > Inhalte > Dastenshutz und Sicherheit > Zertifikate anzeigen > Ihre Zertifikate

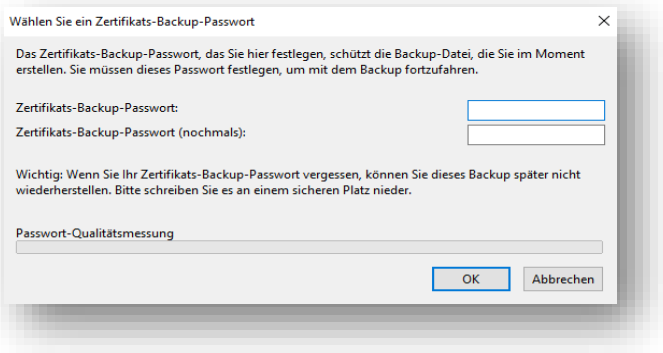


c. Klicken Sie das Zertifikat an und klicken dann auf **„Sichern“**



d. Wählen Sie bitte einen sicheren Speicherplatz und einen geeigneten Namen.

e. Klicken Sie auf „**Speichern**“



f. Wählen Sie abschließend ein Kennwort für die Sicherungsdatei.

Achtung: Wir empfehlen die Daten auf einem einzigen Datenträger, z.B. einem USB-Stick, zu speichern, der zur Verteilung des Zertifikats und des privaten Schlüssels dient und abschließend als Datensicherung verwahrt werden kann. Stellen Sie dabei auch sicher, dass Sie sich an das Passwort der Exportdatei erinnern können. Wir raten von einem Versand der Exportdatei per E-Mail ab. Dies birgt ein Sicherheitsrisiko, da Unberechtigte unbemerkt eine Kopie der Exportdatei erlangen könnten und anschließend beliebig Zeit/Versuche haben, Ihr Passwort zu raten.

3.6 Verteilung des Zertifikates

Das Sicherheitskonzept von JMD i-mpuls sieht vor, dass sich jeder Nutzer als Mitarbeiterin bzw. Mitarbeiter einer bestimmten Einrichtung authentisiert. Dazu wird das erstellte Zertifikat benutzt, das als Gruppenzertifikat fungiert. Das Zertifikat muss dafür an **jedem Arbeitsplatz mit Rechner** und für jede Benutzerin bzw. jeden Benutzer importiert werden, die bzw. der JMD i-mpuls benutzen soll.

Hinweis: Der Zugriff auf JMD i-mpuls sollte nur von vertrauenswürdigen Rechnern aus erfolgen, die hohen Sicherheitsanforderungen genügen. Rechnerpools in Schulen o. ä. erfüllen solche Anforderungen **NICHT**.

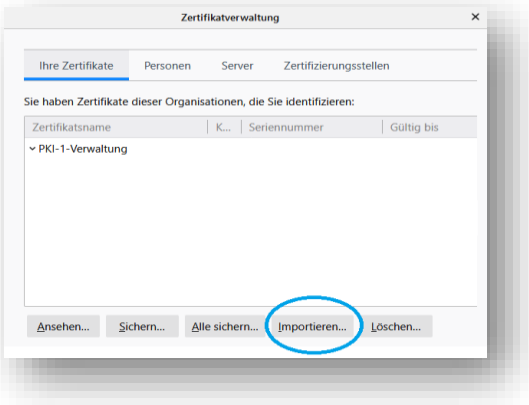
- Für die Verteilung wird das Zertifikat inklusive des privaten Schlüssels zunächst aus dem Browser exportiert und dann auf den entsprechenden Rechnern wieder importiert.
- Für den Import des Gruppenzertifikates und des Schlüssels benötigen Sie die Exportdatei (z.B. auf einer CD) und das Kennwort, das während des Exports vergeben wurde.

Internet Explorer:

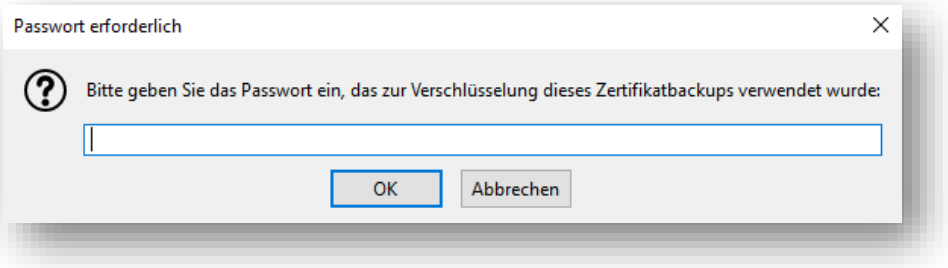
Der Import in den Internet Explorer ist den beschriebenen Vorgängen zur Erst-Installation sehr ähnlich: Mit einem Klick der rechten Maustaste auf das Datei-Icon einer Exportdatei öffnet sich ein Kontextmenü, hier können Sie die Option „Installieren“ wählen (siehe Punkt 3.5.1 Herunterladen und Erst-Installation (Internet Explorer)).

Mozilla Firefox:

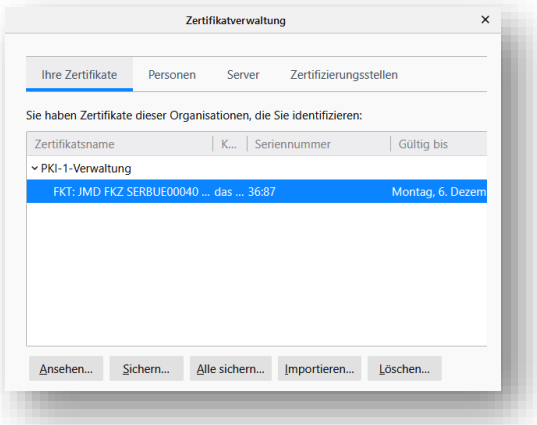
1. Starten Sie Firefox und wählen Sie den Zertifikat-Manager: Menü > Einstellungen > Inhalte > Dastenshutz und Sicherheit > Zertifikate anzeigen > Ihre Zertifikate
2. Klicken Sie im Zertifikat-Manager den Knopf „Importieren“, um den Import zu starten und die im vorherigen Schritt erstellte Exportdatei auszuwählen.



3. Für den Import wird nun das Passwort abgefragt, mit dem die erstellte Exportdatei geschützt wurde.



4. Bei korrekter Eingabe des Passwortes werden der Schlüssel und alle mit exportierten Zertifikate nun importiert und der erfolgreiche Import bestätigt.
5. Abschließend ist das Gruppenzertifikat im Zertifikat-Manager aufgeführt:



6. Nach dem erfolgreichen Import von privatem Schlüssel und Zertifikaten kann auch vom entsprechenden Nutzerkonto aus auf den Anwendungsbereich Ihrer Einrichtung zugegriffen werden.

Achtung: Bitte stellen Sie sicher, dass der Datenträger nach der Verteilung vernichtet oder sicher verwahrt wird. Ein unbemerkter Verlust des Datenträgers gibt Unberechtigten eine Möglichkeit, mit beliebiger Zeit/Anzahl von Versuchen Ihr Sicherungspasswort zu raten.

4 Support und Hilfen

4.1 Dokumentation

Die hier beschriebenen Arbeitsabläufe beziehen sich auf die Funktionen für die Antragstellung von Zertifikaten im System der Verwaltungs- Public-Key-Infrastruktur (V-PKI) der Südwestfalen-IT (SIT (Citkomm)). Die SIT (Citkomm) stellt die Dienstleistung eines Zertifizierungsdiensteanbieters der PKI-1-Verwaltung für Mitarbeiterinnen und Mitarbeiter von Behörden aus dem Bereich der öffentlichen Verwaltung zur Verfügung. Im Übrigen gelten die Ausführungen in der CP (**Sicherheitsleitlinie**) in der jeweils gültigen Fassung. Die Registrierungsstelle ist per E-Mail erreichbar unter pki@citkomm.de. Der Zugang zur V-PKI der SIT (Citkomm) geschieht über einen Browser über das Webportal:

http://cas.citkomm.de

Neben dieser Anleitung bietet das Trust-Center der SIT (Citkomm) weitere Dokumentationen an, die von der Web-Seite http://cas.citkomm.de heruntergeladen werden können:

- Antragstellerhandbuch: Das Dokument ist in der gültigen Fassung von der Webseite des Trust-Centers unter dem Stichwort „Bedienungsanleitung“ zu finden: (http://cas.citkomm.de/dokument/Antragstellerhandbuch.pdf)
- Sicherheitsleitlinien: Die Sicherheitsleitlinie (Certificate Policy, CP) ist das zentrale Dokument der PKI der SIT (Citkomm) und enthält die vertragsrelevanten Informationen zur Aufbau- und Ablauforganisation der PKI. Dieses ist unter http://cas.citkomm.de/dokument/CertificatePolicy_aktuell.pdf abrufbar.
- Tipps+Tricks: Bereits häufiger aufgetretene Probleme sind hier mit Lösungsansätzen dokumentiert: http://cas.citkomm.de/dokument/TippsundTricks.pdf

Im internen Bereich des JMD-Portals (www.jugendmigrationsdienste.de) finden Sie eine Sammlung von häufig gestellten Fragen (FAQ, Frequently Asked Questions) und entsprechende Antworten. Folgend einige FAQ, die sich auf das Zertifikat beziehen.

4.2 FAQ – die häufigsten Fragen

(1) Die Zuständigkeit für die Zertifikatsbeantragung hat sich geändert, was müssen wir tun?

Eine Zuständigkeitsänderung für die Zertifikatsbeantragung sollten Sie dem Servicebüro Jugendmigrationsdienste bekannt geben. Nennen Sie den vorherigen und den neuen Ansprechpartner inkl. E-Mail Adresse. Die Änderung der Zuständigkeit erfordert **keine Neubeantragung**! Das bestehende Zertifikat Ihrer Einrichtung bleibt weiterhin gültig.

(2) Wie oft muss das Zertifikat erneuert werden?

Das Sicherheitskonzept von JMD i-mpuls sieht vor, dass die Gruppenzertifikate, die Sie dazu berechtigen auf die entsprechenden Server und Datenbanken zuzugreifen, **alle drei Jahre erneuert** werden. Es ist notwendig den vollständigen Prozess zu durchlaufen, da es sich tatsächlich um eine NEU-Beantragung der Zertifikate handelt.

(3) Das importierte Zertifikat ist im Zertifikatsmanager nicht unter Eigene/Ihre Zertifikate gelistet – warum?

Wenn sich das importierte Zertifikat unter einem anderen Reiter befindet, können Sie davon ausgehen, dass der private Schlüssel die Ursache ist. Stellen Sie sicher, dass der Erstimport tatsächlich auf dem **Antragsrechner** durchgeführt wird, da hier der originale private Schlüssel liegt. Für die anschließende Verteilung an die Mitarbeiterinnen und Mitarbeiter muss beim Export des Zertifikates der **private Schlüssel** mit exportiert werden.

(4) Mit welchem Browser kann ich das Zertifikat nutzen?

Das Zertifikat können Sie für die Arbeit mit JMD i-mpuls mit jedem Browser mit SSL/TLS-Unterstützung benutzen. Wir empfehlen aktiv sicherheitsgepflegte Versionen. Lediglich die Beantragung und die Erstinstallation sind auf den Internet-Explorer bzw. Mozilla Firefox beschränkt.

(5) Kann JMD i-mpuls an einem Computer mit mehreren Browsern verwendet werden?

Ja, Sie müssen nur das Gruppenzertifikat in jedem verwendeten Browser extra importieren.

(6) Das neue Zertifikat ist installiert. Beim Aufrufen von JMD i-mpuls wird aber weiterhin eine Fehlermeldung angezeigt – warum?

Vermutlich ist die Vertrauenskette nicht vollständig. Mit einem manuellen Import von Wurzel- und/oder Serverzertifikat können Sie die Vertrauenskette wiederherstellen.

(7) Muss ich das Zertifikat auch auf meinem Laptop installieren?

Das Zertifikat dient der Authentifizierung vor dem Server und muss somit an jedem Arbeitsplatz installiert werden, an dem Sie mit JMD i-mpuls die Akten der jungen Menschen pflegen möchten. Wenn Ihr Laptop dazugehört, muss auch hier ein Zertifikat installiert werden.

(8) Ich erhalte eine Warnmeldung „Das Objekt unterstützt diese Eigenschaft oder Methode nicht“. Was kann ich tun?

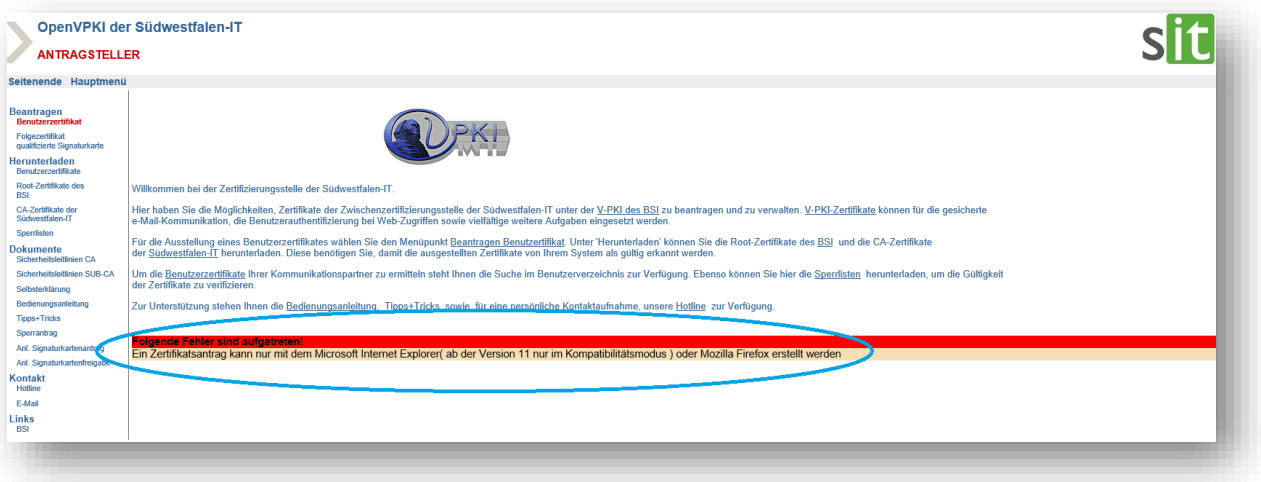
Dies ist vermutlich geschehen, als Sie den „Bestätigen“ Knopf während der Beantragung gedrückt haben. Vermutlich wurde ein ActiveX Steuerelement nicht ausgeführt. Das entsprechende Add-On muss aktiviert werden. Dafür können Sie wie folgt vorgehen:

Oberhalb der Webseite der OpenVPKI wird Ihnen eine gelbliche Leiste angezeigt: Diese Webseite möchte das folgende Add-On ausführen: "Microsoft Certficate Enrollment Control" von "Microsoft Corporation".

- Klicken Sie hier, wenn Sie der Website vertrauen und die Ausführung zulassen möchten.
- Klicken Sie auf das gelbe Banner und erlauben Sie die Ausführung. Nach erfolgreichem Import können Sie dieses Steuerelement wieder deaktivieren.

(9) Windows Internet Explorer 11, Kompatibilitätsmodus aktivieren

Ab der Version 11 des Microsoft Windows Internet Explorers ist die Aktivierung des „Kompatibilitätsmodus“ für die Seite *citkomm.de* notwendig.



Dieser Fehler wird wie folgt behoben:

- Öffnen Sie das Menü „Extras“ Je nach Darstellung ein Menüpunkt „Extras“ oder ein Zahnrad oben rechts, erreichbar auch über die Tastenkombination Alt-X

- Wählen Sie den Menüpunkt „Einstellungen der Kompatibilitätsansicht“
- Webseite *„citkomm.de“* hinzufügen
- Im geöffneten Einstellungsdialog wird die aktuelle Website vorgeschlagen. Stellen Sie sicher, dass unter „Folgende Website hinzufügen“ die Seite *citkomm.de* angegeben ist und klicken Sie „Hinzufügen“.
- Anschließend wird die Seite citkomm.de unter „Zur Kompatibilitätsansicht hinzugefügte Websites“ aufgeführt.
- Bestätigen Sie die Einstellungen mit einem Klick auf die Schaltfläche „Schließen“
- Wählen Sie anschließend erneut aus dem linken Menü der Webseite „Beantragen Benutzerzertifikat“ aus.

(10) Windows 7, Einstellungen für den Internet Explorer

Für Windows Internet Explorer ist unabhängig vom Kompatibilitätsmodus (s.o.) die Seite *„citkomm.de“* mit weiteren Einstellungen zu den „Vertrauenswürdigen Sites“ hinzuzufügen:

- Öffnen Sie das Menü „Extras“ Je nach Darstellung ein Menüpunkt „Extras“ oder ein Zahnrad oben rechts, erreichbar auch über die Tastenkombination Alt-X
- Wählen Sie den Menüpunkt „Internetoptionen“
- Wählen Sie im neu geöffneten Dialog den Reiter „Sicherheit“ und dort als Zone „Vertrauenswürdige Sites“ (symbolisiert durch einen grünen Haken).
- Klicken Sie anschließend auf die Schaltfläche „Sites“.
- Webseite der *„citkomm.de“* hinzufügen
- Im geöffneten Einstellungsdialog wird die aktuelle Website vorgeschlagen. Stellen Sie sicher, dass unter „Diese Website zur Zone hinzufügen“ die Seite *https://cas.citkomm.de* angegeben ist und klicken Sie „Hinzufügen“.
- Einstellungen bestätigen
- Anschließend wird die Seite https://cas.citkomm.de unter „Websites“ aufgeführt.
- Bestätigen Sie die Einstellungen mit einem Klick auf die Schaltfläche „Schließen“
- Anschließend muss die Sicherheitsstufe für die Zone „Vertrauenswürdige Sites“ angepasst werden. Klicken Sie dazu auf die Schaltfläche „Stufe anpassen“:

- Scrollen Sie bis zum Abschnitt „ActiveX-Steuerelemente und Plug-Ins“ und stellen Sie sicher, dass insbesondere im Abschnitt „ActiveX-Steuerelemente initialisieren und ausführen, die nicht als “sicher für Skripting” markiert sind“ *Aktivieren* ausgewählt ist.
- Beenden Sie den Dialog mit einem Klick auf „OK“.
- Bestätigen Sie die folgende Nachfrage „Möchten Sie die Einstellungen für diese Zone wirklich ändern?“ mit einem Klick auf „Ja“.
- Beenden Sie die Einstellungen mit einem Klick auf „OK“ im Dialog „Internetoptionen“.

(11) Warnmeldung: „Der Dialog wurde aus Sicherheitsgründen beendet, da Sie für den ausgewählten Verarbeitungszweig nicht berechtigt sind!“

Die Meldung tritt sporadisch unter Microsoft Windows Internet Explorer auf, wenn aufgrund der vielfältigen Konfigurationsoptionen die Sitzungsdaten nicht korrekt zwischen Browser und Server ausgetauscht werden konnten.

Klicken Sie in diesem Fall auf den Link „Hauptmenü“ und beginnen Sie die Antragstellung erneut. Andere Wege zurück zum Hauptmenü initialisieren ggf. die Sitzungsdaten nicht korrekt und führen nicht zu einer Lösung!

4.3 Individuelle Unterstützung

Sollten schwere Probleme auftreten, die sich mit der Dokumentation nicht lösen lassen, so wenden Sie sich bitte an das Servicebüro Jugendmigrationsdienste.