PWE Funktionszertifikat

Pilotbetrieb

Intevation GmbH

6. August 2021

Inhaltsverzeichnis

KAPITEL 1

Einleitung

PWE ist eine Webanwendung, die Anwender/innen kommunizieren verschlüsselt über das Internet mit der Anwendung. Um die Echtheit der Kommunikationspartner zu gewährleisten, werden an beiden Enden der Datenverbindung Zertifikate eingesetzt. Die Webanwendung akzeptiert nur Verbindungen von Stellen, die ihr als vertrauenswürdig bekannt sind. Im Gegenzug ist auch für Einrichtungen sichergestellt, dass sie direkt und über eine gesicherte Verbindung mit PWE kommunizieren. Zertifikate für einzelne Einrichtungen werden als Funktionszertifikate (X.509) vergeben. Die Zertifikatsverwaltung wird vom Trustcenter der SIT GmbH (SIT), Hemer, betrieben.

Dieses Dokument stellt die wichtigsten Punkte bei der Beschaffung und Benutzung der Zertifikate vor.

1.1 Wichtiges vorab

Bitte führen Sie den kompletten Antragsprozess zeitnah und ohne große Unterbrechungen durch! Der Prozess ist erst **nach dem erfolgreichen Import** des Zertifikates abgeschlossen, nicht schon nach dem Absenden des Antrages oder dem Herunterladen der Signaturdatei[1] vom Trustcenter. Bis zum **Abschluss** des Antragsprozesses dürfen am **Benutzerprofil auf dem Arbeitsplatzrechner des Antragstellers keine Veränderungen** vorgenommen werden. Dazu zählen z.B. auch Passwortänderungen und die Installation von Software, insbesondere Updates des Microsoft Internet Explorers bzw. EDGE oder Mozilla Firefox.

Hintergrund: Das Zertifikat besteht aus zwei verschiedenen Komponenten:

- **Öffentlicher Schlüssel**, der Ihnen vom Trustcenter signiert wird
- **Privater Schlüssel**, der beim Zertifikatsantrag durch den eingesetzen Browser erstellt und verborgen auf dem Antragsrechner verbleibt. Der private Schlüssel kann nicht explizit aufgerufen werden. Durch Veränderungen am Benutzerprofil unter Microsoft Windows auf Ihrem PC kann der private Schlüssel während der Antragsphase beschädigt werden bzw. verloren gehen.

Wichtig: Nur zusammen funktionieren beide Teile als Zertifikat. Daher ist es besonders wichtig, den Prozess zeitnah zu beenden und abschließend den erfolgreichen Import zu überprüfen.

[1] Die Signaturdatei heißt userCertifcate.p7b

Kurzportrait Funktionszertifikat	
Gültigkeitsdauer	3 Jahre - ein Wechsel der/des Zertifikatsverantwortlichen während der Gültigkeit erfordert **keine** Neubeantragung des Zertifikats
Aussteller	Trustcenter der SIT in Hemer
Verantwortlichkeit	Eine Person pro Einrichtung
Browser	Beantragung und Erst-Installation des Zertifikates sind nur mit dem Microsoft Internet Explorer[2], EDGE und dem Mozilla Firefox möglich, Verwendung ist später auch mit Opera, Safari u.a. Browsern möglich!
Speicherort	Import unter Eigene/Ihre Zertifikate im jeweiligen Zertifikatsmanager.

1.2 Allgemeines

Wie oben bereits angesprochen wird die Kommunikation zwischen dem Webbrowser der Anwender/innen und der zentralen Webanwendung verschlüsselt. Insgesamt wird ein dreistufiges Verfahren implementiert: Zunächst wird über das **Serverzertifikat** das System gegenüber der Anwenderin bzw. dem Anwender authentifiziert. Durch das **Funktionszertifikat** wird der Zugriff als Mitarbeiterin bzw. Mitarbeiter einer Einrichtung authentifiziert. Im letzten Schritt authentifiziert sich die Mitarbeiterin bzw. der Mitarbeiter durch **Benutzername und Passwort** persönlich.

Die Funktionszertifikate basieren auf einer Public-Key-Infrastruktur. Neben öffentlichen Schlüsseln (Public-Key), die vom Trustcenter 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**.

1.3 Dokumentation

Diese Anleitung beschreibt die **Antragsstellung** und **Installation** des Funktionszertifikates sowie den **Import** zugehöriger Zertifikate von Zertifizierungsstellen, um eine vollständige Vertrauenskette aufzubauen.

Für die **korrekte Anwendung** der Funktionszertifikate stellt die SIT außerdem folgende Dokumente bereit:

- Antragstellerhandbuch. Das Dokument ist in der gültigen Fassung von der Webseite des Trustcenters unter dem Stichwort „Bedienungsanleitung“ herunterladbar.
- Weitere Hinweise sind unter dem Stichwort **„Tipps+Tricks“** auf der gleichen Seite verfügbar.
- Certificate Policy (CP) für die zertifikatsbasierte Schlüsselinfrastruktur (Public Key Infrastructure – PKI) des Trustcenters der SIT.

[2] Abhängig von der installierten Version des IE können weitere Einstellungen notwendig sein. Schauen Sie hierzu im Anhang dieser Anleitung oder in die „Tipps+Tricks“ des Trustcenters (https://cas.citkomm.de).

KAPITEL 2

Der Zertifizierungsprozess

Die **Beantragung** eines Zertifikates ist aus technischen Gründen **nur** unter Microsoft Windows über einen Internet Explorer (IE), EDGE oder über Mozilla Firefox (FF) möglich. Andere Browser (z. B. Chrome, Opera usw.) werden bisher bei der Beantragung leider nicht unterstützt. Bereits erstellte Zertifikate können dann jedoch auch mit anderen Browsern benutzt werden.

Der Prozess für ein Funktionszertifikat teilt sich in mehrere Schritte:

1. Antragsstellung (nur mit IE oder FF unter Microsoft Windows möglich)
2. Authentifizierung durch Postident-Verfahren
3. Herunterladen und Erst-Installation des Zertifikates
4. Export/Import des Zertifikates (Verteilung an Anwender/innen, alle Browser)

Abb. 2.1: Zertifizierungsprozess

Für den Zertifizierungsprozess wird in jeder Einrichtung eine **Verantwortliche** bzw. ein **Verantwortlicher** im Vertrag zur Bereitstellung von PWE festgelegt. Die Schritte bis zum Verteilen des Zertifikates an die einzelnen Mitarbeiterinnen und Mitarbeiter der Einrichtung finden auf einem Rechner unter dem Nutzerkonto der verantwortlichen Person statt.

2.1 Notwendige Vorbereitungen und Hinweise

- **Windows Internet Explorer Version 11**

  Der Zertifizierungsprozess kann mit dem Microsoft Windows Internet Explorer 11 nur noch im Kompatibilitätsmodus durchgeführt werden. Folgen Sie dazu bei Bedarf der Anleitung unter *Windows Internet Explorer Version 11, Kompatibilitätsmodus aktivieren* (page 25).

- **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 *Microsoft Windows 7, Einstellungen für Windows Internet Explorer* (page 27).

- Vorgehen bei **Warnmeldung „Dialog wurde aus Sicherheitsgründen beendet“**

  Sporadisch kann die *Warnmeldung: „Der Dialog wurde aus Sicherheitsgründen beendet, da Sie für den ausgewälten Verarbeitungszweig nicht berechtigt sind!“* (page 30) auftreten, beachten Sie dazu bitte die *FAQ - Die häufigsten Fragen* (page 23) unten.

2.2 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 Trustcenter der SIT zur Signatur übermittelt. Zusammen fungiert das Schlüsselpaar später dann mit Signatur als „Funktionszertifikat“.

Gehen Sie bitte wie folgt bei der Antragstellung vor:

1. Öffnen Sie mit dem Internet Explorer bzw. mit dem EDGE oder Mozilla Firefox (andere Browser werden zur Zeit leider nicht unterstützt) die Seite https://cas.citkomm.de

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

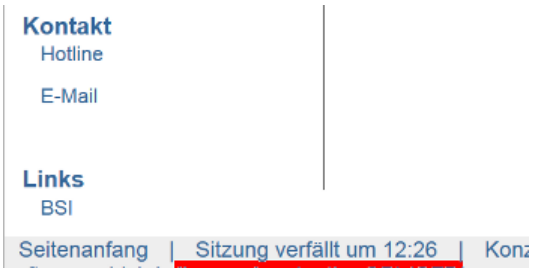


Abb. 2.2: Achten Sie bitte auf die zeitliche Begrenzung der Sitzung

2. Wählen Sie aus dem linken Menü „Beantragen Benutzerzertifikat” aus. Es werden nun schrittweise die notwendigen Angaben zum öffentlichen Schlüssel abgefragt:

   (a) Räumliche Ordnung: Wählen Sie „SIT”.

   (b) Organisationseinheit I: Diese haben wir Ihnen per Brief mitgeteilt.

   (c) Organisationseinheit II: Wählen Sie hier den Eintrag für Ihre Einrichtung aus. (Brief)

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

- **Kennung**: Geben Sie hier bitte den Schlüssel an, den wir Ihnen per Brief mitgeteilt haben. Über diese Angabe wird später Ihre Einrichtung identifiziert.
- **E-Mail Adresse**: Geben Sie hier bitte Ihre E-Mail Adresse ein, welche bei Ihrer Benennung zur verantwortlichen Person für das Funktionszertifikat angegeben wurde. Diese wird abgeglichen und ist für den weiteren Ablauf der Zertifikatsvergabe notwendig.
- Abschließend akzeptieren Sie bitte die Sicherheitsleitlinien. Diese sind verlinkt und können nachgelesen werden.
- Klicken Sie auf „beantragen".

3. Prüfen Sie die getroffenen Angaben im folgenden Dialog und bestätigen Sie diese - oder gehen Sie zurück, um die Angaben zu korrigieren.

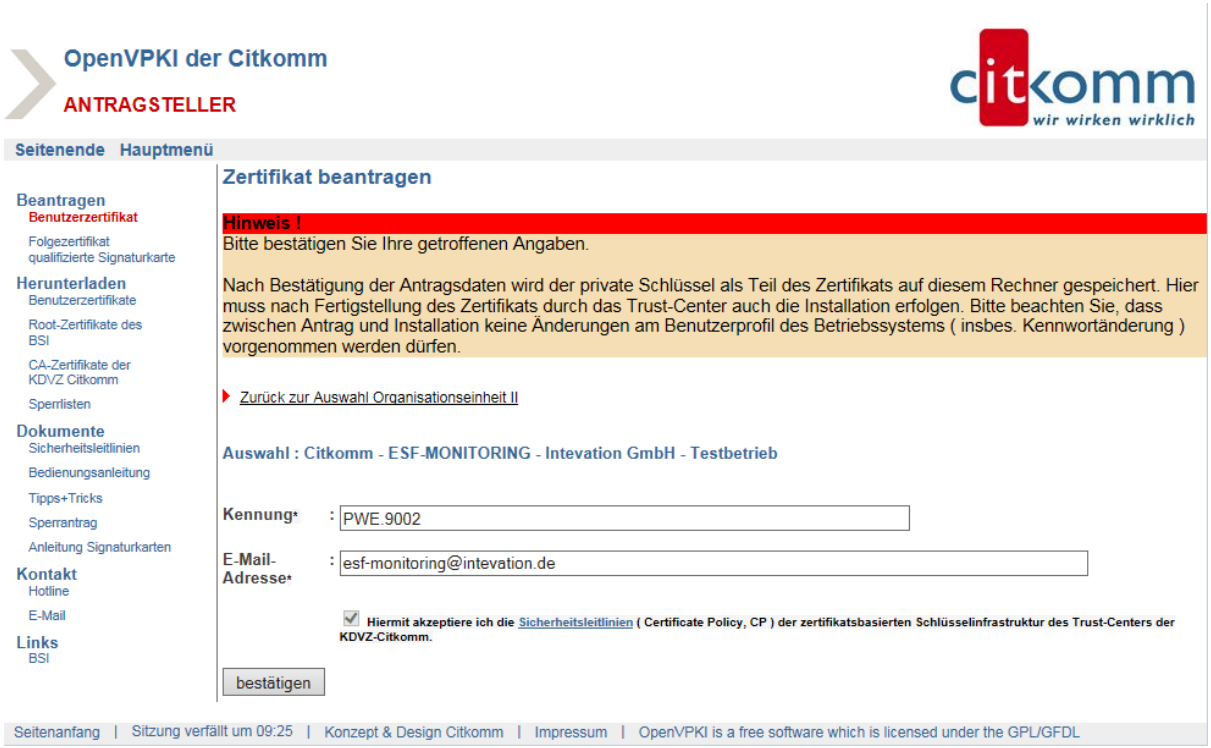


Abb. 2.3: Dialog zur Eingabe den Antragstellenden bekannter Daten am Beispiel PWE

4. Nach der Bestätigung kann es zu Warnmeldungen kommen:

   „Automatisierungsserver kann Objekt nicht erstellen". Hier müssen Sie die Seite https://cas.citkomm.de zu den vertrauenswürdigen Sites hinzufügen.

   „Objekt unterstützt diese Eigenschaft oder Methode nicht". Es fehlt meist eine für die Schlüsselerstellung notwendige Funktion die sich jedoch leicht aktivieren lässt.

   Zu diesen und ggf. anderen Warnmeldungen verweisen wir auf das Dokument „Tipps und Tricks", der SIT.

5. Es folgt eine Sicherheitsabfrage („Webzugriffsbestätigung“), die Sie bitte mit „Ja“ bestätigen.

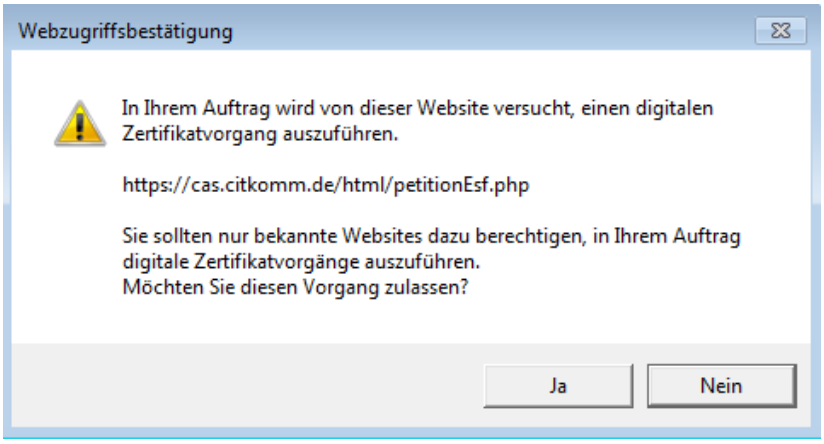


Abb. 2.4: Mögliche Sicherheitsabfrage im Internet Explorer

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

Wichtig: Vorgabe beim Schutz des (privaten) Schlüssels ist lediglich eine *mittlere Sicherheitsstufe*. Wir empfehlen die Einstellung *hohe Sicherheitsstufe*.

- Stellen Sie sicher, dass der private Schlüssel auf **hoher Sicherheitsstufe** geschützt ist (Ändern mit Klick auf „Sicherheitsstufe“)!

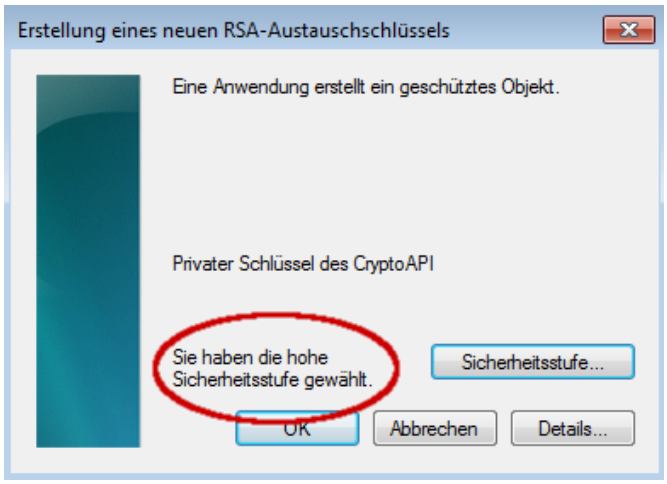


Abb. 2.5: Einstellung *hohe Sicherheitsstufe*

- Nach dem Bestätigen auf „OK“ werden Sie nach einem Passwort (**PW1** – vgl. *Zertifizierungsprozess im Überblick am Beispiel von mpuls_S* (page 33)) gefragt, das im Schritt 3 und 4 des Zertifizierungsprozesses bei jeder Verwendung des privaten Schlüssels erforderlich ist.

Wichtig: Stellen Sie sicher, dass Sie sich für diese späteren Schritte an das Passwort (**PW1**) erinnern können.

- Bestätigen Sie die folgenden Dialoge mit „OK“.

7. Das Schlüsselpaar wird erstellt und der öffentliche Teil an das Trustcenter übermittelt.

> **Achtung:** Durch eventuelle Veränderungen am Benutzerprofil auf dem Antragsrechner könnte der **private Schlüssel** vor Abschluss des Zertifizierungsprozess **unbenutzbar** werden. Daher sollten Sie den Prozess bis einschließlich *Verteilung des Zertifikates* (page 15) zeitnah abschließen.

8. Anschließend erfolgt eine Bestätigung und die Aufforderung, den Zertifikatsantrag (Namensvergabedokument) zu drucken.

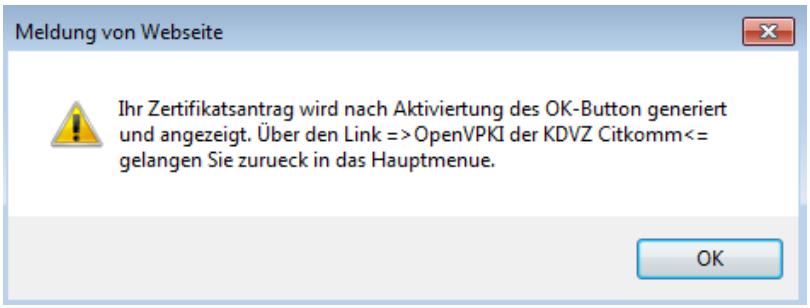


Abb. 2.6: Abschließende Meldung im Antragsprozess

> **Wichtig:** Drucken Sie den Zertifikatsantrag aus, er wird im weiteren Verfahren benötigt. Ohne diesen Ausdruck kann kein Zertifikat erstellt werden! Setzen Sie sich bei Problemen ggf. mit der SIT in Verbindung – der Antrag muss bei versäumten Ausdruck nicht erneut gestellt werden.

9. Damit ist der erste Schritt der Antragsstellung 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 Trustcenters der SIT. Drucken Sie ihn aus und schneiden Sie den Coupon ab. Diesen Coupon brauchen Sie für das Postident-Verfahren:

2.3 Postident-Verfahren

Die Prüfung eines Antrags und das damit verbundene persönliche Erscheinen der/des Antragstellenden (Authentisierung) sind in jedem Fall notwendig. Diese kann in einer Filiale der Deutschen Post AG (nicht Postagentur!) vorgenommen werden. Das Trustcenter der SIT nutzt dafür das Postident-Verfahren der Deutschen Post AG. Dieser zertifizierte Dienst übernimmt Teilaufgaben der Überprüfung.

> **Wichtig:** Vor dem Hintergrund der **persönlichen Authentisierung** ist es notwendig, **spätere Änderungen in der Zuständigkeit** für die Zertifikatsbeantragung mit einem formlosen Schreiben der Intevation GmbH als Vertragspartner der SIT in der Auftragsdatenverarbeitung schriftlich mitzuteilen.

Sie erhielten innerhalb der Antragsstellung via E-Mail ein Schreiben (PDF-Brief) des Trustcenter mit einem Coupon für das Postident-Verfahren, sowie ein Namensvergabedokument für Endbenutzerzertifikate.

Faxen Sie bitte das Namensvergabedokument an die angegebene Faxnummer und bewaren Sie es sorgfältig auf. Für das Postident-Verfahren wird es nicht weiter benötigt.

Um das Postident-Verfahren abzuschließen benötigen Sie die folgenden 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.

KAPITEL 3

Herunterladen und Erst-Installation

Nach erfolgreicher Durchführung des Postident-Verfahrens **signiert** das Trustcenter der SIT Ihren **öffentlichen Schlüssel** und stellt ein Zertifikat zur Verfügung. Die Antragsstellerin bzw. der Antragssteller erhält automatisch eine entsprechende E-Mail an die im Zertifikatsantrag angegebene Adresse.

Achtung: 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 zusammen gefügt, so dass diese als „Funktionszertifikat“ fungieren können.

3.1 Mozilla Firefox und EDGE

Bitte benutzen Sie für die Installation, die Überprüfung des Imports und die Sicherung des Zertifikates mit dem Mozilla Firefox oder EDGE die Anleitung der SIT unter:

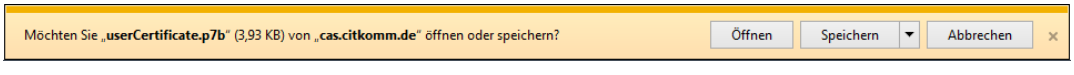
https://cas.citkomm.de/dokument/Antragstellerhandbuch.pdf

3.2 Internet Explorer

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

1. Benutzen Sie den in der E-Mail enthaltenen Link[1], 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 gespeichert werden.

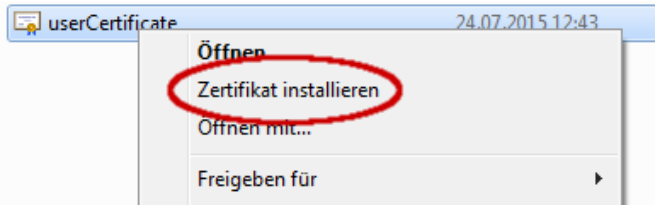
   (a) Speichern Sie die Transport-Datei „userCertifcate.p7b“ auf dem Desktop ab.

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

[1] Einige E-Mail-Programme haben Probleme mit dem enthaltenen Link, das Dokument „Tipps+Tricks“ enthält Hinweise zur Konfiguration. Alternativ können Sie das Zertifikat von der Webseite des Trustcenters im Abschnitt „Benutzerzertifikat“ suchen und herunterladen (Vgl. Abschnitt „Zentraler Verzeichnisdienst LDAP“ im Antragstellerhandbuch).

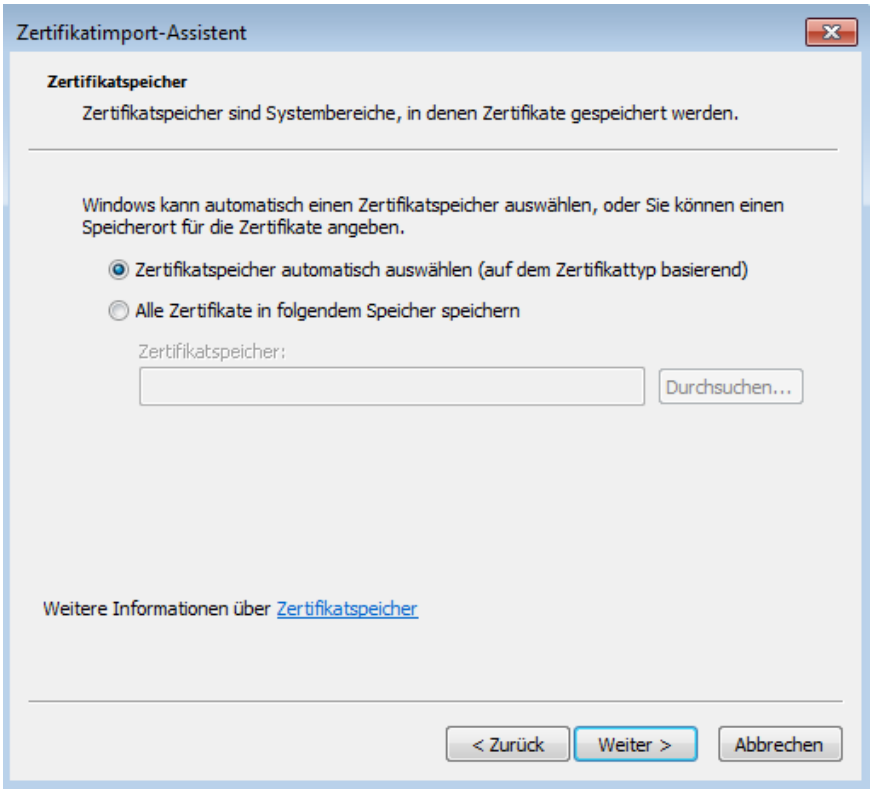
2. Klicken Sie anschließend die Datei mit der rechten Maustaste an und rufen Sie den Installationsassistenten mit einem Klick auf „Zertifikat installieren“ auf.



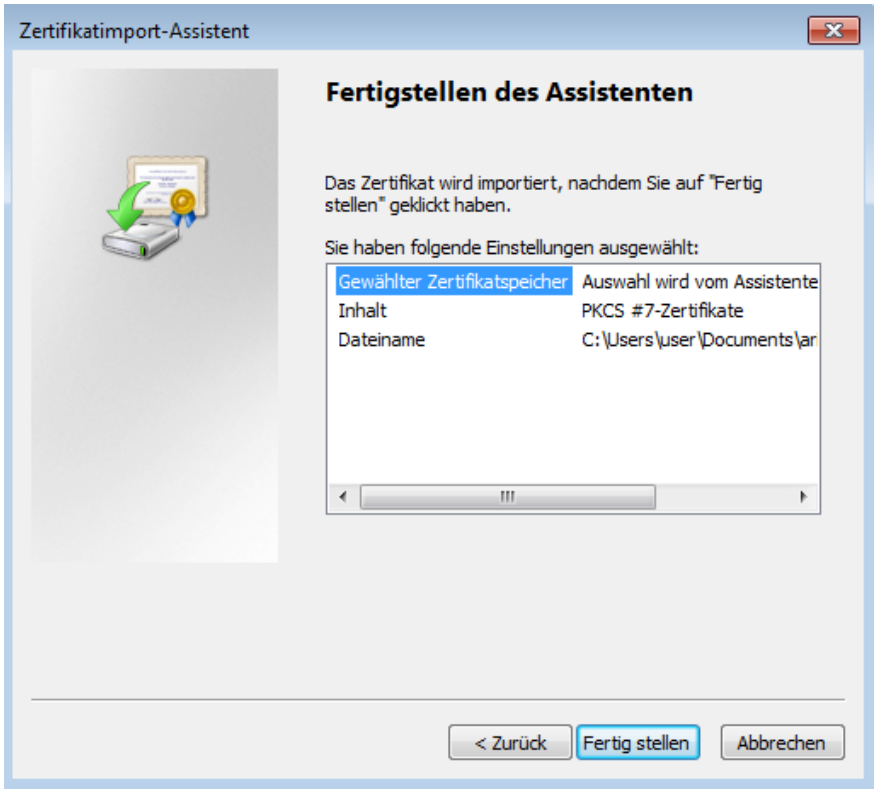
3. Der Assistent führt Sie durch die einzelnen Schritte des Importes, die Abfragen sind jeweils zu bestätigen. Sie benötigen zum Installieren das bei der Beantragung vergebene Passwort (**PW1** – vgl. *Zertifizierungsprozess im Überblick am Beispiel von mpuls_S* (page 33)).

   (a) Im Willkommen Dialog klicken Sie auf „Weiter“.

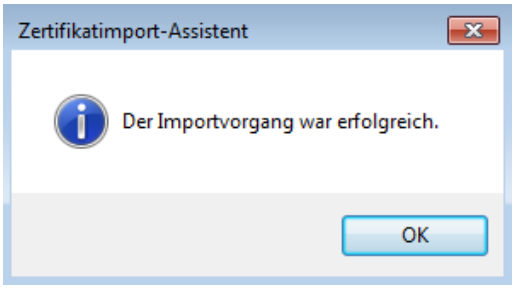
   (b) „Zertifikatsspeicher“: Ohne Änderung – bestätigen Sie mit „Weiter“



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



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



4. Es werden das eigene Zertifikat, das Zertifikat der SIT und das Zertifikat der Wurzelzertifizierungsstelle vom BSI (Bundesamt für Sicherheit in der IT) im Zertifikatspeicher in die verschiedenen Bereiche installiert. Dabei erfolgt ggf. eine Sicherheitsabfrage bezüglich des Wurzelzertifikates/Stammzertifikates “PCA-1-Verwaltung-xx”. Lassen Sie sich das Zertifikat anzeigen und überprüfen Sie die Korrektheit anhand des angezeigten Fingerabdruckes (Groß-/Kleinschreibung und Füllzeichen wie Doppelpunkte sind dabei nicht relevant).

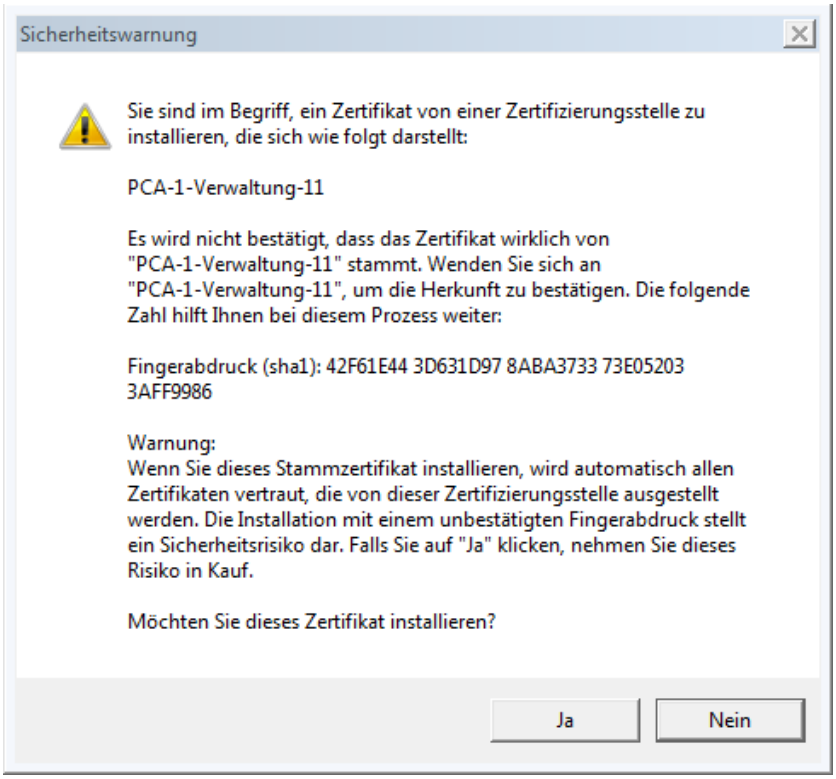


Abb. 3.1: Sicherheitswarnung

Fingerabdruck (SHA-1):

PCA-1-Verwaltung-11:

```
42 F6 1E 44 3D 63 1D 97 8A BA 37 33 73 E0 52 03 3A FF 99 86
```

CA-5-Citkomm:

```
F0 AA 34 88 39 CA 61 C7 AD 5F 0F 25 92 CE 7E 77 5E A2 7C B3
```

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

Wichtig: Bitte überprüfen Sie den Fingerabdruck des Wurzelzertifikates immer an dieser Stelle.

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

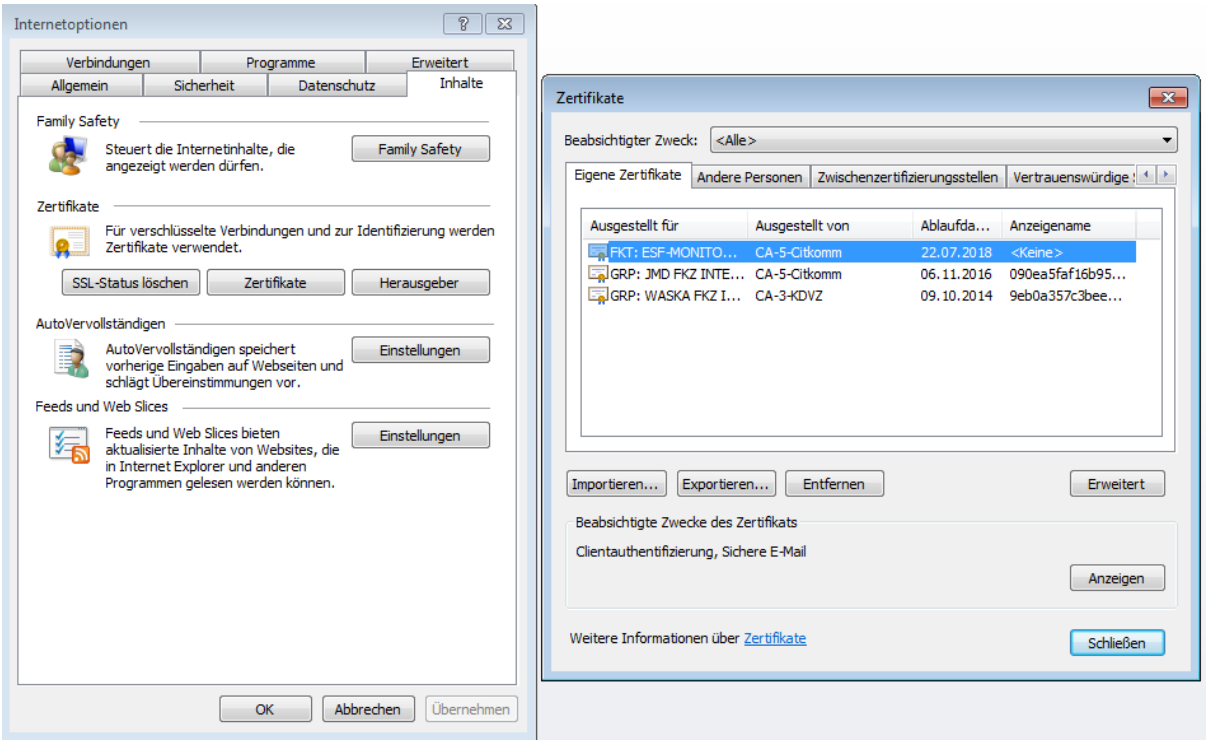
3.2.1 Import überprüfen

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

Öffnen Sie hierzu bitte den **Zertifikatsmanager des Internet Explorers**:

```
> Menü „Extras" > „Internetoptionen" > „Inhalte" > „Zertifikate" >
„Eigene Zertifikate"
```

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



Wichtig: 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 im Kapitel *FAQ - Die häufigsten Fragen* (page 23).

Wichtig: Nach Abschluss des Importes sollte eine Sicherungskopie des Zertifikates (öffentlicher **und** privater Schlüssel) erstellt werden. Die Schritte dazu sind identisch mit den ersten Schritten zur *Vertei-*

lung des Zertifikates (page 15) an die Mitarbeiterinnen und Mitarbeiter der Verwaltung.

KAPITEL 4

Verteilung des Zertifikates

Das Sicherheitskonzept von PWE sieht vor, dass sich jede Anmeldekennung als Mitarbeiterin bzw. Mitarbeiter einer bestimmten Einrichtung authentisiert. Dazu wird das erstellte Zertifikat benutzt, das als Funktionszertifikat fungiert. Das Zertifikat muss dafür an **jedem Arbeitsplatz mit Rechner** und für jede Mitarbeiterin bzw. jeden Mitarbeiter installiert werden, die bzw. der PWE benutzen soll.

Für die Verteilung wird das Zertifikat inklusive des privaten Schlüssels zunächst aus dem Browser exportiert und dann auf den entsprechenden Rechnern wieder importiert.

Wichtig: Der Zugriff auf PWE sollte nur von vertrauenswürdigen Rechnern aus erfolgen, die hohen Sicherheitsanforderungen genügen. Rechnerpools in Einrichtungen o. ä. erfüllen solche Anforderungen nicht.

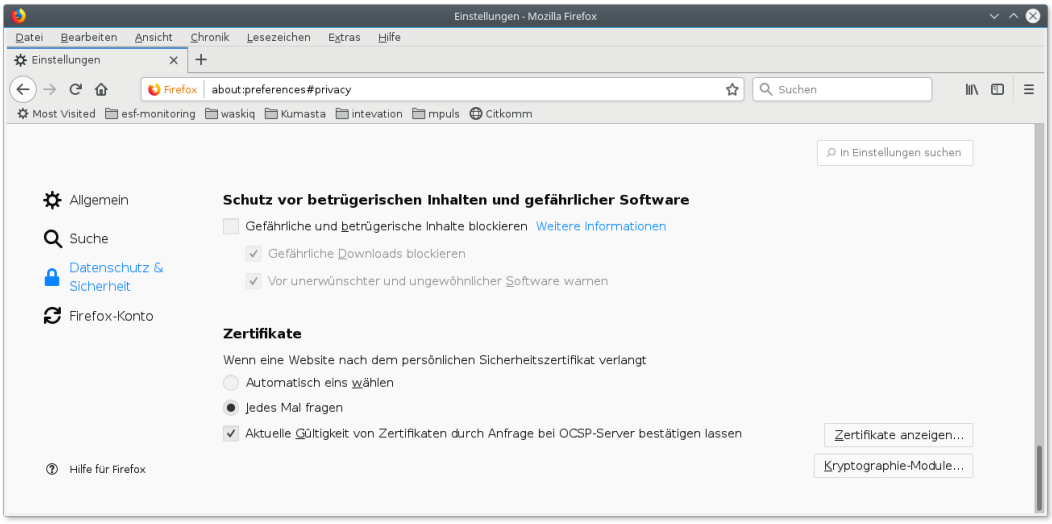
4.1 Mozilla Firefox

4.1.1 Sichern

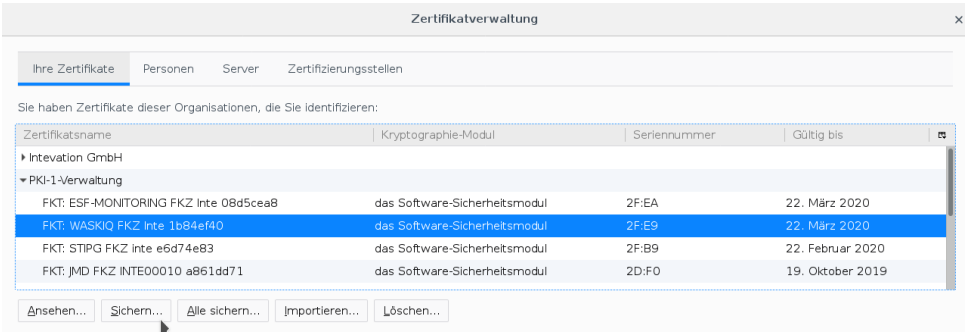
Wir beschreiben hier das Sichern des privaten Schlüssels und des Zertifikates über den Firefox.

1. Wählen Sie den Zertifikatspeicher im Firefox aus:

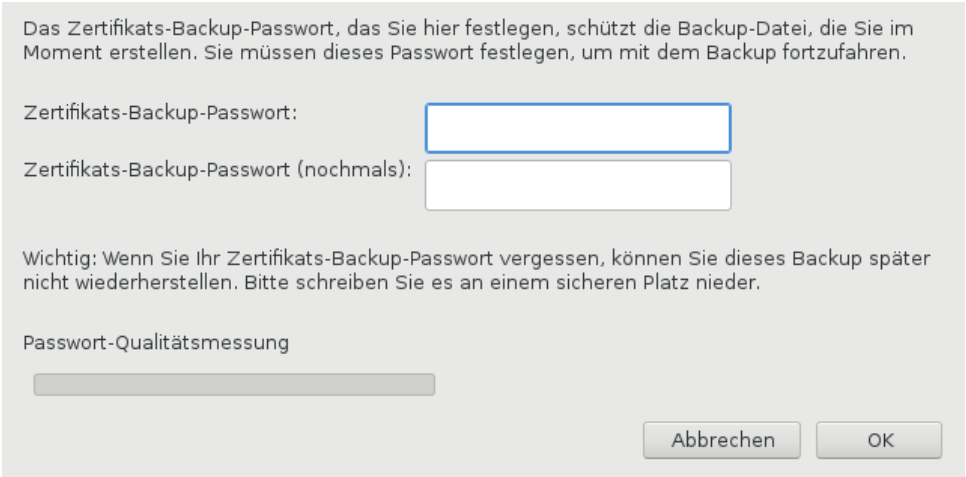
```
> Menü öffnen > "Einstellungen" > "Datenschutz & Sicherheit"
> "Zertifikate anzeigen" > "Ihre Zertifikate"
```



2. Markieren Sie das zu sichernde Zertifikat und wählen „Sichern...“, ein Assistent führt Sie durch die einzelnen Schritte des Exports:



- Wählen Sie bitte einen sicheren Speicherplatz, sowie einen geeigneten Namen und drücken Sie die Taste “Speichern”.
- Sie werden aufgefordert, den gesicherten Schlüssel durch ein Kennwort zu schützen. Sie benötigen dieses Kennwort, um den Schlüssel und das Zertifikat auf einem anderen Rechner zu importieren.



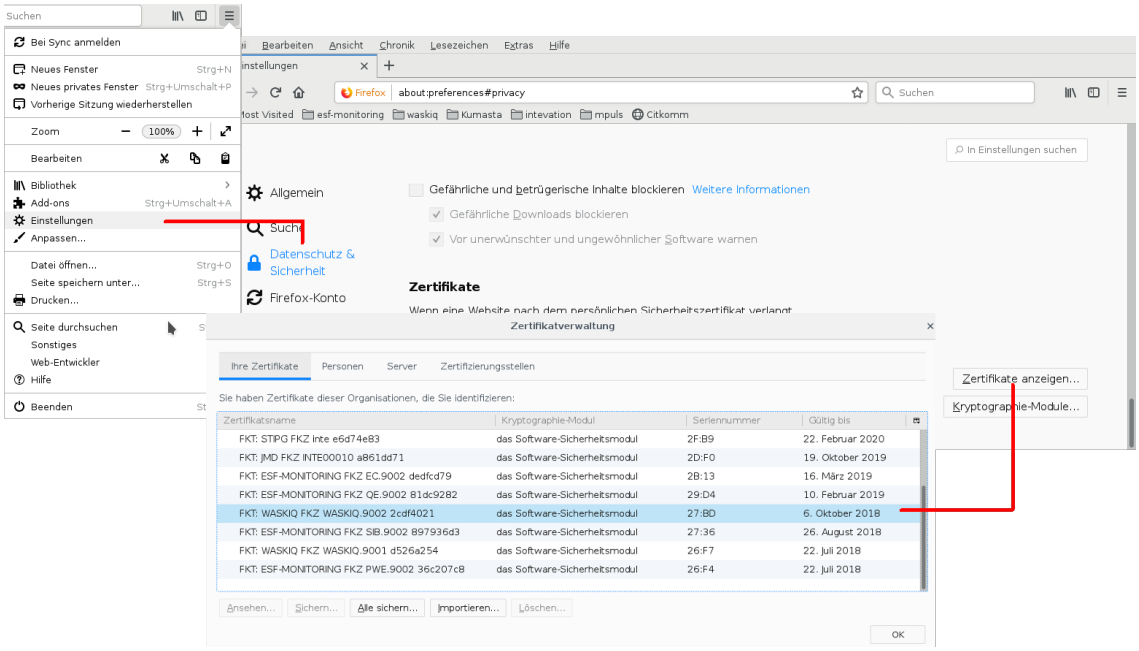
3. Das gesicherte Zertifikat können Sie nun auf einen Datenträger (USB-Stick, CD ..) speichern und zur Weiterverteilung/Importierung auf andere Rechner verwenden.

4.1.2 Import

Für den Import des Funktionszertifikates inkl. des privaten Schlüssels benötigen Sie die Sicherungsdatei (USB-Stick, CD ..) und das Kennwort, das während der Sicherung vergeben wurde.

1. Starten Sie den Mozilla Firefox und wählen Sie den Zertifikat-Manager:

```
> Menü „Öffnen" > "Einstellungen" > "Datenschutz & Sicherheit"
> "Zertifikate anzeigen" > "Ihre Zertifikate"
```



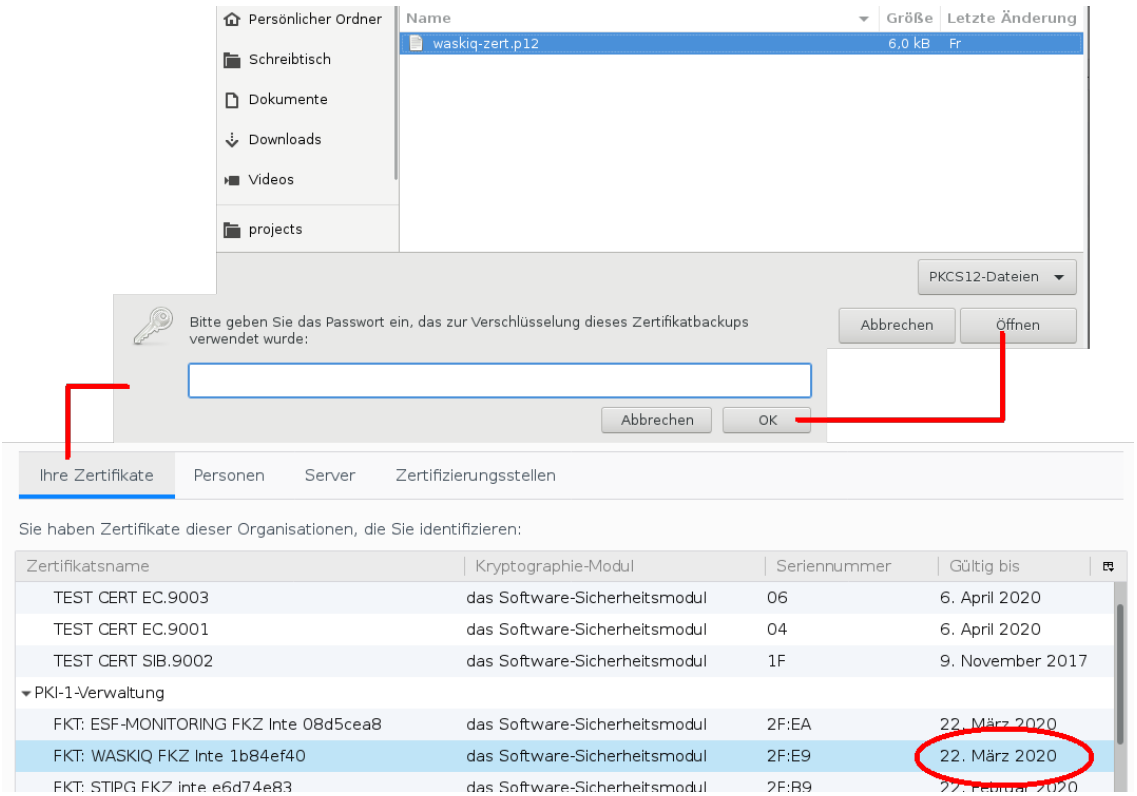
2. Klicken Sie im Zertifikat-Manager den Knopf „Importieren“, um den Import zu starten und die im vorherigen Schritt erstellte Sicherungsdatei auszuwählen.

3. Der Firefox speichert die Schlüssel in einem „Schlüsselbund“, der durch ein Master-Passwort geschützt ist. Wenn Sie noch kein Passwort für diesen Schlüsselbund vergeben haben, werden Sie aufgefordert, dies nun zu tun. Andernfalls werden Sie aufgefordert, Ihr bestehendes Passwort einzugeben.

4. Für den Import wird nun das Passwort abgefragt, mit dem die im vorherigen Schritt erstellte Sicherungsdatei geschützt wurde (**PW2** – vgl. *Zertifizierungsprozess im Überblick am Beispiel von mpuls_S* (page 33))

5. Bei korrekter Eingabe des Passwortes werden der private Schlüssel und alle mit exportierten Zertifikate nun importiert und der erfolgreiche Import bestätigt.

6. Abschließend ist das Funktionszertifikat im Zertifikat-Manager aufgeführt:



7. 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.

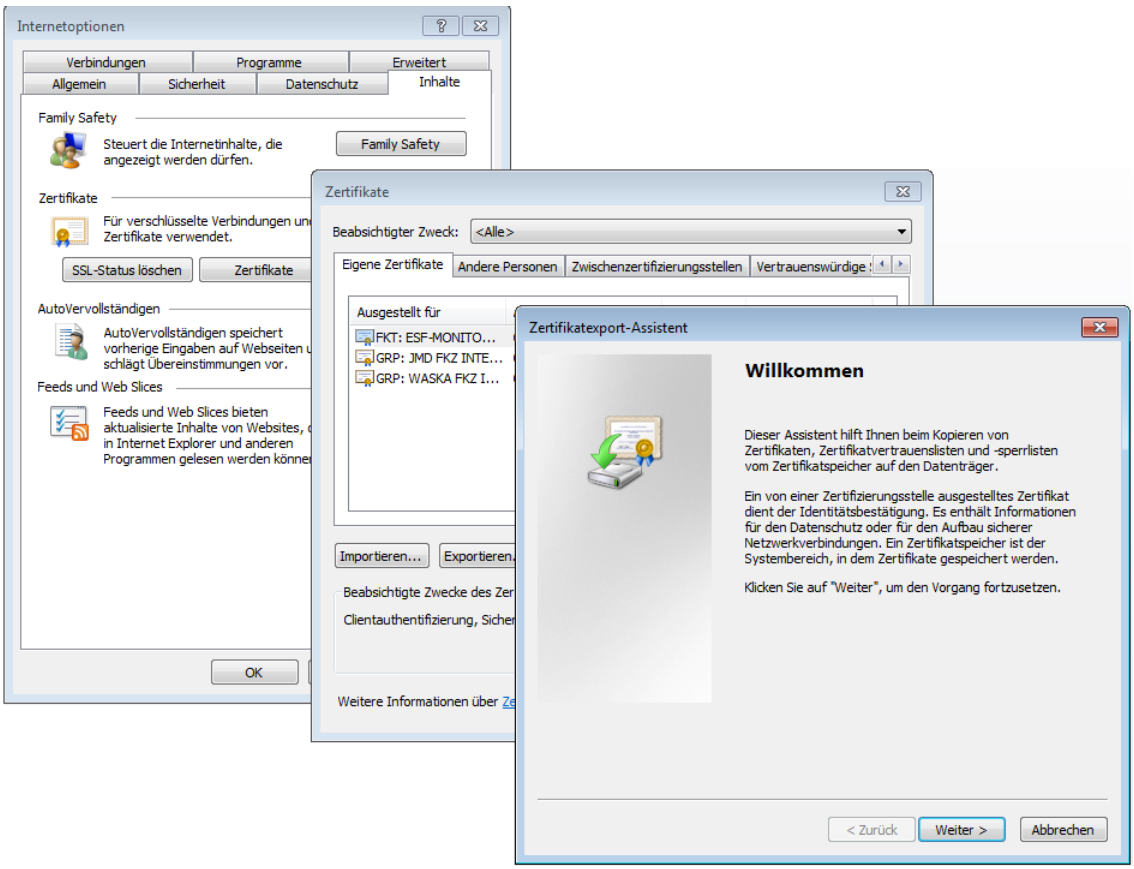
4.2 Internet Explorer

4.2.1 Sicherung

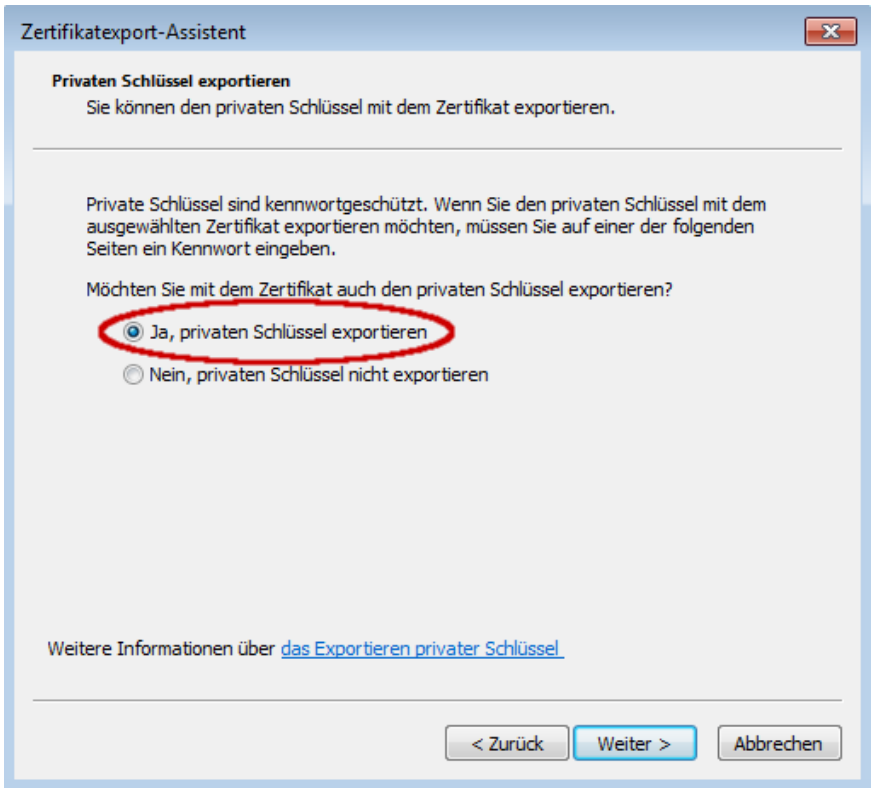
Wir beschreiben hier den Export des privaten Schlüssels und des Zertifikates über den Internet Explorer (IE).

1. Wählen Sie wie oben den Zertifikatspeicher des IE:

```
> Menü „Extras“ > „Internetoptionen“ > „Inhalte“ > „Zertifikate“
> „Eigene Zertifikate“
```

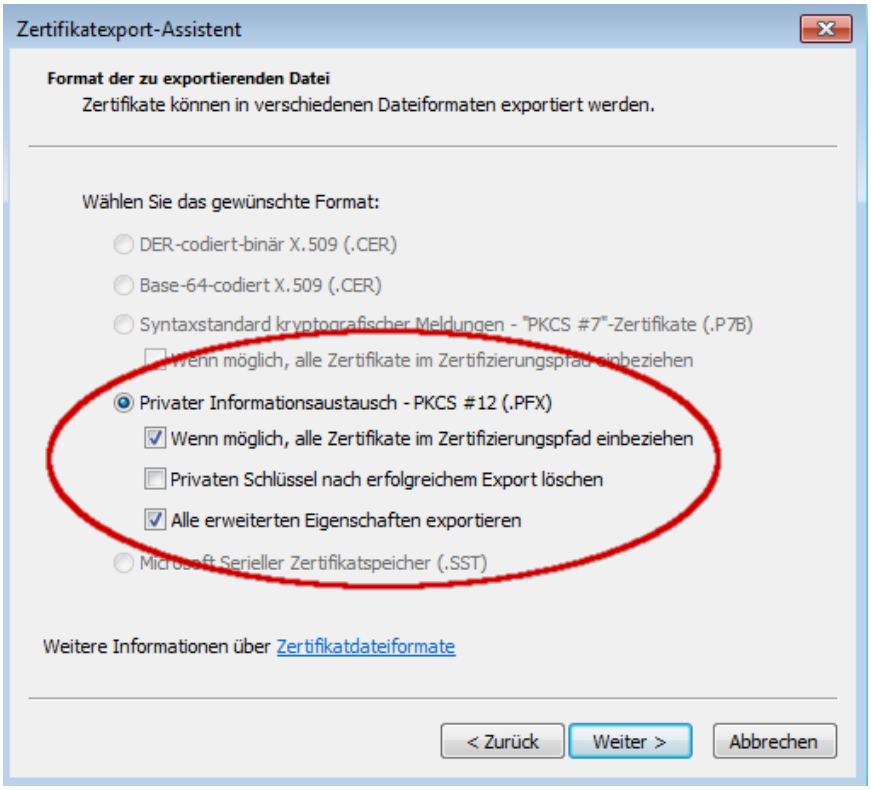


2. Markieren Sie das zu exportierende Zertifikat und wählen „Exportieren“, ein Assistent führt Sie durch die einzelnen Schritte des Exports:

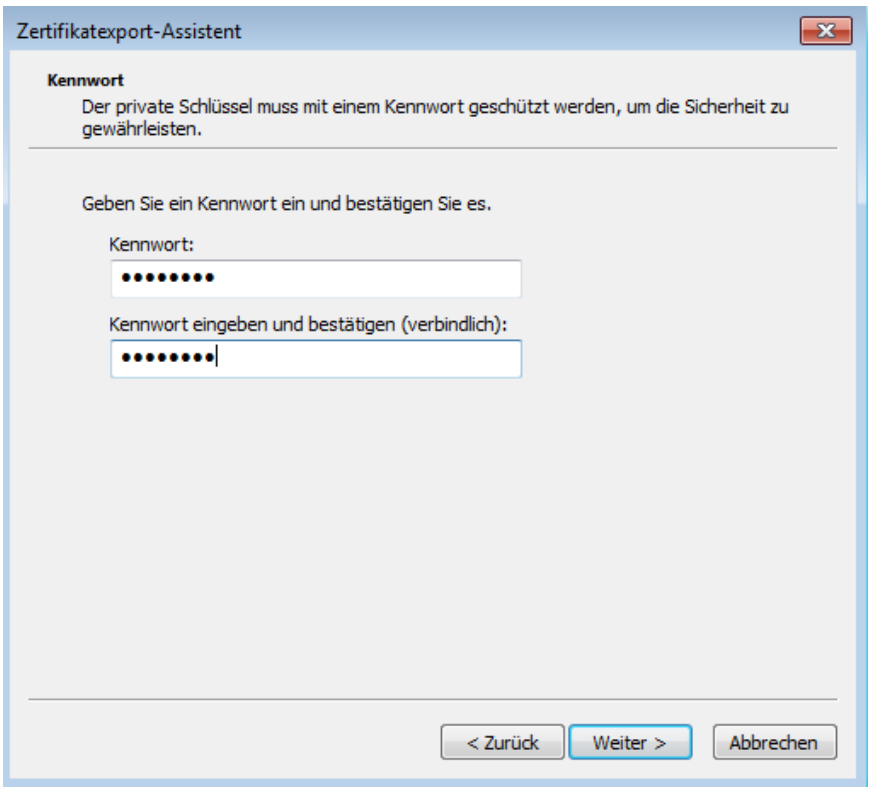


Achtung: Stellen Sie sicher, dass Sie den **privaten Schlüssel** mit exportieren. **Ohne** den privaten Schlüssel funktioniert das Zertifikat auf anderen Rechnern **nicht**!

- 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 *Herunterladen und Erst-Installation* (page 9) ergänzt werden.
- Unter Windows 10 gibt es noch die Möglichkeit, den Zertifikatdatenschutz zu aktivieren.
- Stellen Sie sicher, dass der private Schlüssel nicht gelöscht wird, wenn Sie das Zertifikat auch auf diesem Rechner benutzen wollen!

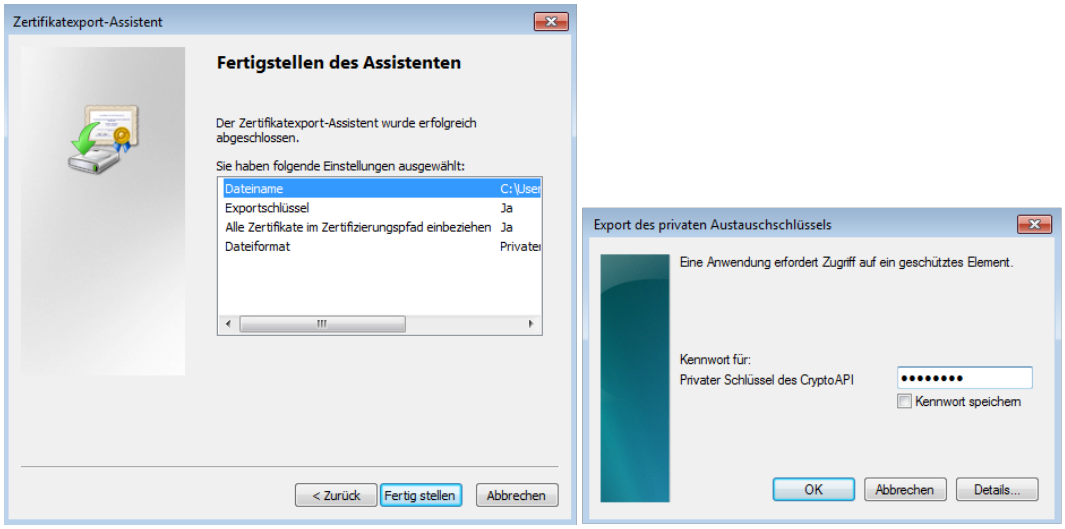


- Sie werden aufgefordert, den exportierten Schlüssel durch ein Kennwort (**PW2** – vgl. *Zertifizierungsprozess im Überblick am Beispiel von mpuls_S* (page 33)) zu schützen. Sie benötigen dieses Kennwort, um den Schlüssel und das Zertifikat auf einem anderen Rechner zu importieren.



- Wählen Sie abschließend einen Dateinamen, unter dem der exportierte Schlüssel abgelegt werden soll. Damit sind alle notwendigen Eingaben für den Assistenten getätigt.

3. Wählen Sie „Fertigstellen“, um nun das Zertifikat und den privaten Schlüssel zu exportieren. Dabei werden Sie aufgefordert, das Kennwort für den privaten Schlüssel einzugeben, das Sie während der Antragsstellung vergeben haben (**PW1** – vgl. *Zertifizierungsprozess im Überblick am Beispiel von mpuls_S* (page 33)):



Das Funktionszertifikat (Zertifikat inkl. privatem Schlüssel) sind damit exportiert und befinden sich in einer Datei mit der typischen Endung `.p12` bzw. `.pfx`.

Wichtig: Wir empfehlen, die Daten auf **einem** einzigen Datenträger, z.B. einer CD, zu speichern, der zur Verteilung des Zertifikates 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

(**PW2** – vgl. *Zertifizierungsprozess im Überblick am Beispiel von mpuls_S* (page 33)) 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.

4.2.2 Import

Für den Import des Funktionszertifikates inkl. des privaten Schlüssels benötigen Sie die Exportdatei (z.B. auf einer CD) und das Kennwort, das während des Exports vergeben wurde.

Der Import in den Internet Explorer ist den bisher beschriebenen Vorgängen 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.

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.

KAPITEL 5

Unterstützung und Hilfe

5.1 Dokumentation

Neben dieser Anleitung bietet das Trustcenter der SIT weitere Dokumentationen an, welche heruntergeladen werden können:

- **Bedienungsanleitung:** In dieser wird der Antragprozess und die Handhabung von Zertifikaten umfassend dargestellt.
- **Sicherheitsleitlinien:** Die Sicherheitsleitlinie (Certificate Policy, CP) ist das zentrale Dokument der PKI der SIT und enthält die vertragsrelevanten Informationen zur Aufbau- und Ablauforganisation der PKI.
- **Tipps + Tricks:** Bereits häufiger aufgetretene Probleme sind hier mit Lösungsansätzen dokumentiert.

5.2 FAQ - Die häufigsten Fragen

5.2.1 Die Zuständigkeit für die Zertifikatsbeantragung hat sich geändert, was müssen wir tun?

Eine Änderung der Zuständigkeit für die Beantragung eines Zertifikates sollten Sie mit einem formlosen Schreiben per Post an die Adresse:

```
Intevation GmbH
Neuer Graben 17
49074 Osnabrück
```

oder per Fax an:

```
+49-541-335083-99
```

bekannt geben.

Nennen Sie dabei die bisherige und die neue für das Zertifikat verantwortliche Person inkl. E-Mail Adresse.

5.2.2 Wie häufig muss das Zertifikat erneuert werden?

Das Sicherheitskonzept von PWE sieht vor, dass die Funktionszertifikate, die dazu berechtigen auf die entsprechenden Server und Datenbanken zuzugreifen, **alle drei Jahre** erneuert werden müssen. Es ist notwendig den vollständigen Prozess zu durchlaufen, da es sich tatsächlich um eine NEU-Beantragung der Zertifikate handelt und nicht um eine Verlängerung der Vorhandenen.

Das importierte Zertifikat ist im Zertifikatsmanager nicht unter Eigene/Ihre Zertifikate gelistet - warum?

Wenn sich das importierte Zertifikat unter einem anderen Reiter befindet, ist davon auszugehen, dass der fehlende private Schlüssel hier 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 Anwender muss beim Export des Zertifikates der **private Schlüssel** ebenfalls exportiert werden.

5.2.3 Mit welchem Browser kann ich das Zertifikat nutzen?

Das Zertifikat können Sie für die Arbeit mit PWE mit jedem Browser mit SSL/TLS-Unterstützung benutzen. Lediglich die Beantragung und die Erst-Installation sind auf den Internet Explorer, EDGE und Mozilla Firefox beschränkt.

5.2.4 Das neue Zertifikat ist installiert. Beim Aufrufen von PWE wird aber weiterhin eine Fehlermeldung angezeigt - warum?

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

5.2.5 Muss ich das Zertifikat auch auf meinem Laptop installieren?

Das Zertifikat dient der Authentifizierung und muss somit an jedem Arbeitsplatz installiert werden, von dem Sie mit PWE die Akten pflegen möchten. Wenn Ihr Laptop dazugehört, muss auch hier ein Zertifikat installiert werden.

5.2.6 Ich erhalte die 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 Certificate
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 erfolgreichen Import können Sie dieses Steuerelement wieder deaktivieren.

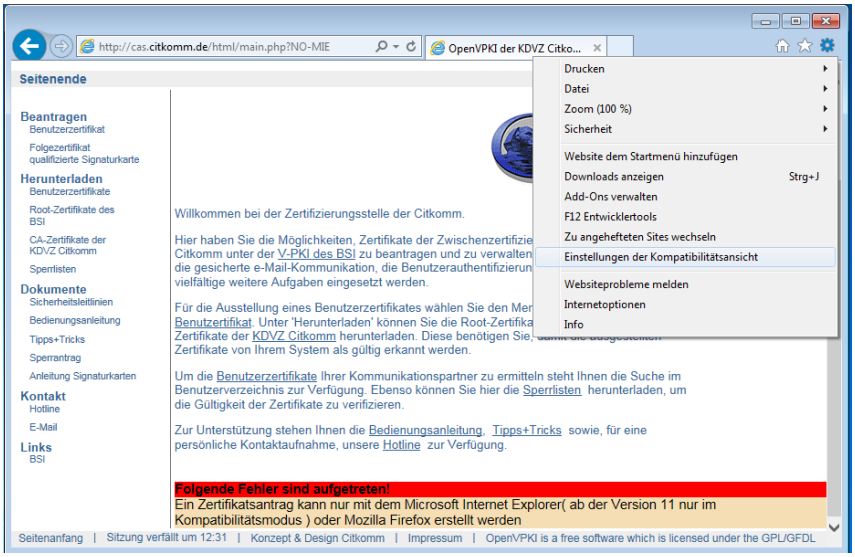
5.2.7 Windows Internet Explorer Version 11, Kompatibilitätsmodus aktivieren

Ab der Version 11 des Microsoft Windows Internet Explorers ist die Aktivierung des „Kompatibilitätsmodus“ für die Seite `citkomm.de` notwendig. Gehen Sie dazu wie folgt vor:

- Öffnen Sie das Menü „Extras“

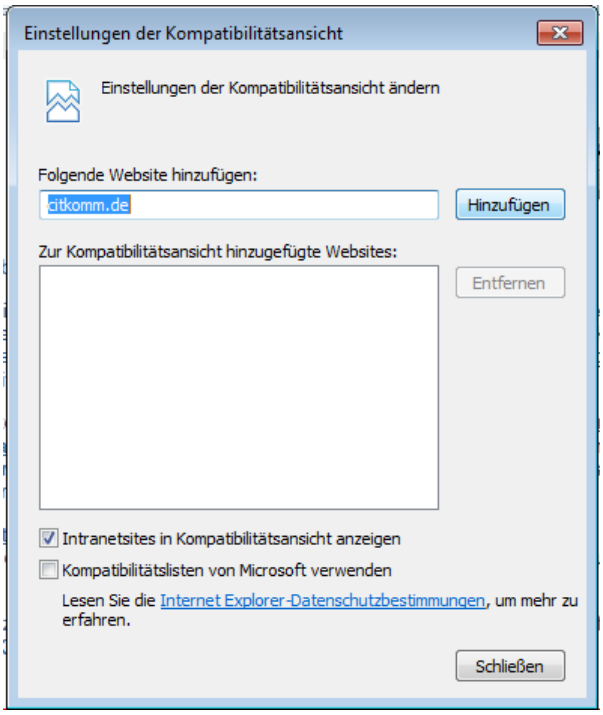
  Je nach Darstellung ein Menüpunkt „Extras“ oder ein Zahnrad oben rechts, erreichbar auch über die Tastenkombination `Alt-X`.

- Wählen Sie den Menüpunkt „Einstellungen der Kompatibilitätsansicht“



- Webseite der SIT hinzufügen

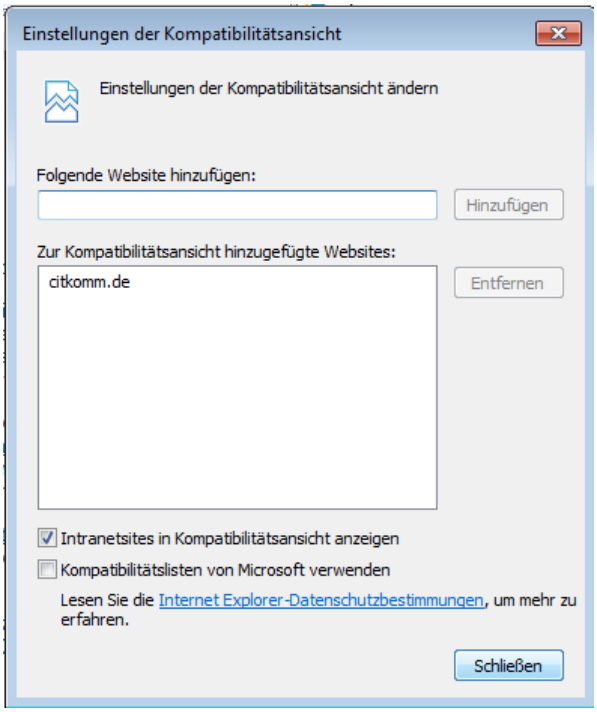
  Im geöffneten Einstellungsdialog wird die aktuelle Website vorgeschlagen. Stellen Sie sicher, dass unter „Folgende Website hinzufügen“ die Seite `citkomm.de` angegeben ist und klicken Sie „Hinzufügen“.



- Einstellung bestätigen

  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.

5.2.8 Microsoft Windows 7, Einstellungen für Windows Internet Explorer

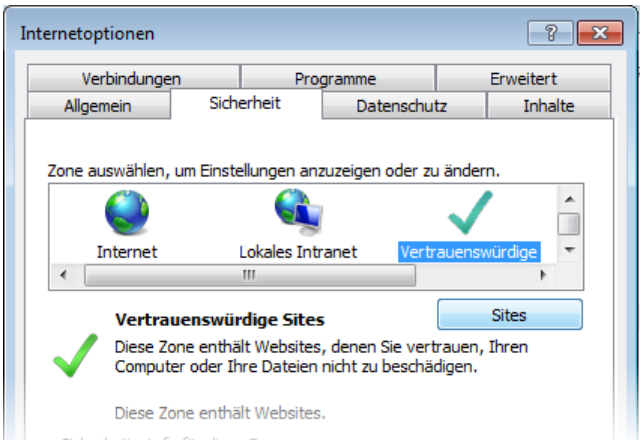
Für Windows Internet Explorer ist unabhängig vom Kompatibiltätsmodus (s.o.) die Seite der SIT mit weiteren Einstellungen zu den „Vertrauenswürdigen Sites“ hinzuzufügen:

- 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“

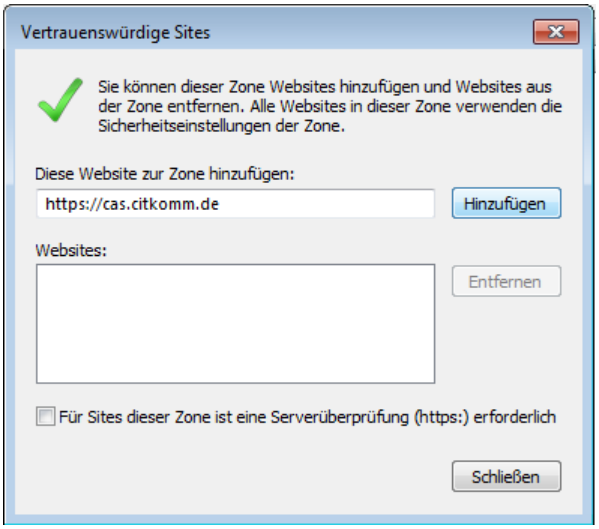
- Wählen Sie im neu geöffneten Dialog den Reiter „Sicherheit“ und dort als Zone „Vertrauenswürdige Sites“ (symbolisiert durch einen grünen Haken).



- Klicken Sie anschließend auf die Schaltfläche „Sites“

- Webseite der SIT hinzufügen

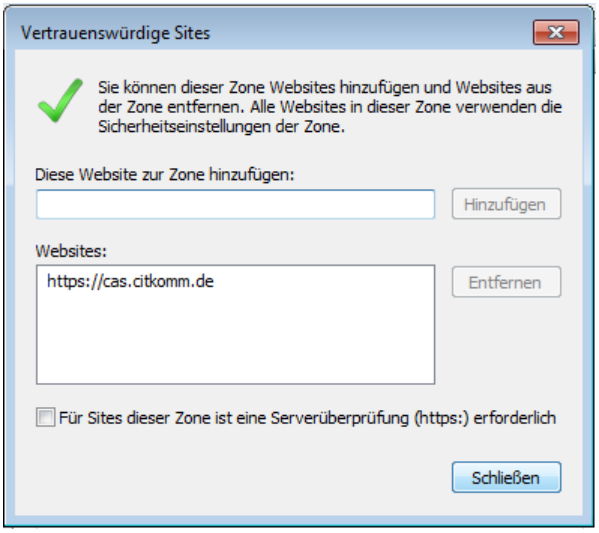
  Im geöffneten Einstellungsdialog wird die aktuelle Website vorgeschlagen. Stellen Sie sicher, dass unter „Diese Website zur Zone hinzufügen“ die Seite `https://cas.citkomm.de` angegeben ist und klicken Sie „Hinzufügen“.



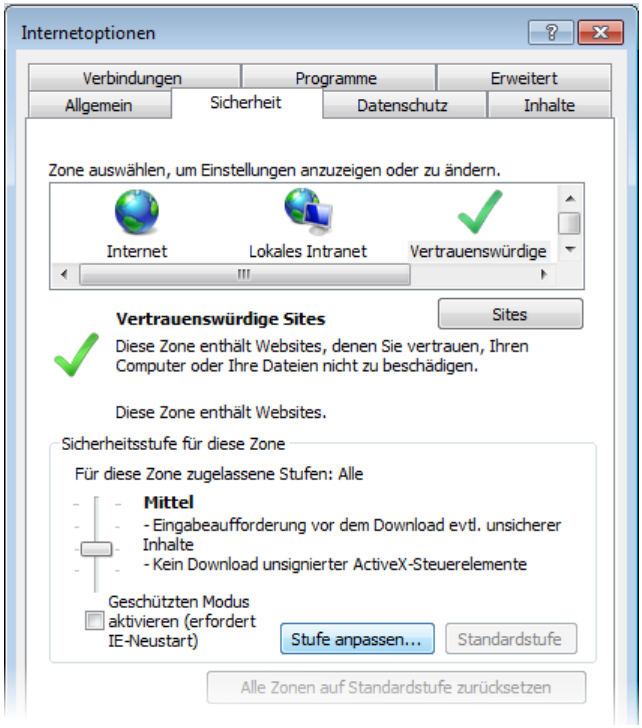
- Einstellung bestätigen

  Anschließend wird die Seite `https://cas.citkomm.de` unter „Websites“ aufgeführt.

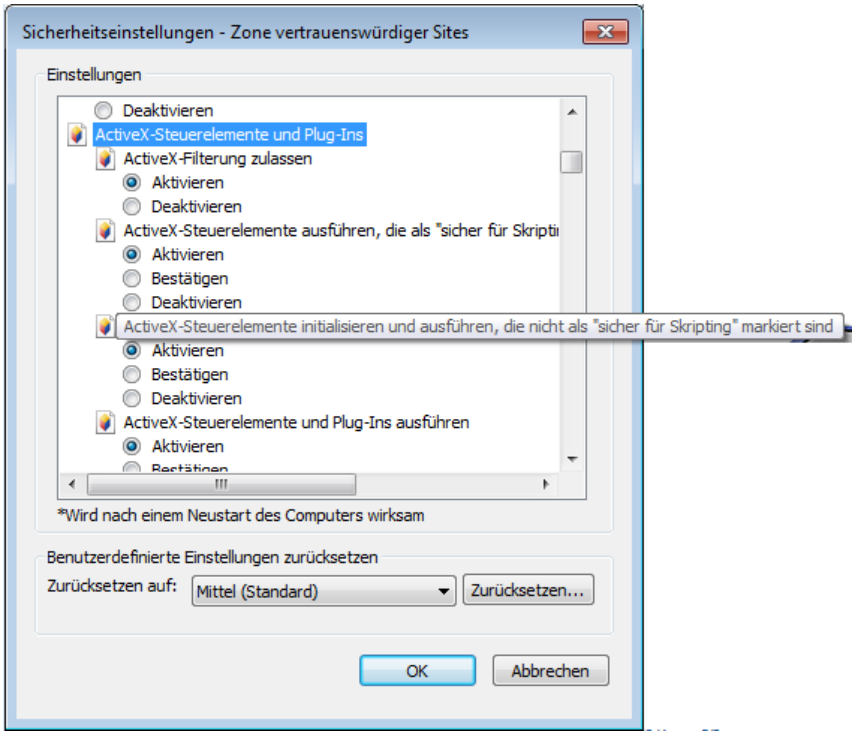
  Bestätigen Sie die Einstellungen mit einem Klick auf die Schaltfläche „Schließen“



- 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:



Darstellung aus dem Microsoft Internet Explorer 11, unter anderen Versionen kann die Auflistung der Konfigurationsoptionen abweichen.

- 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 auf „OK“ im Dialog „Internetoptionen“

5.2.9 Warnmeldung: „Der Dialog wurde aus Sicherheitsgründen beendet, da Sie für den ausgewälten 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“ (vgl. Screenshot) und beginnen Sie die Antragstellung erneut. Andere Wege zurück zum Hauptmenü initialisieren ggf. die Sitzungsdaten nicht korrekt und führen nicht zu einer Lösung!

Abb. 5.1: Warnmeldung, Link zum Hauptmenü hervorgehoben

5.3 Individuelle Unterstützung

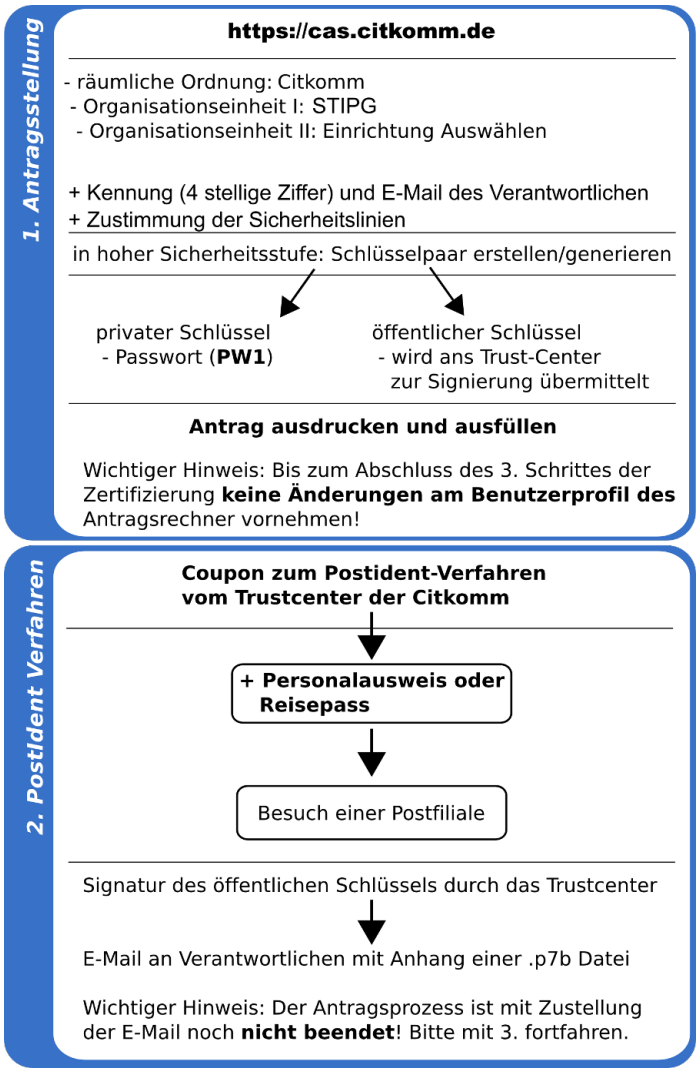
Sollten Probleme auftreten, die sich mit Hilfe dieser oder anderer Dokumentationen nicht lösen lassen, so können Sie beim Trustcenter unter der Rufnummer:

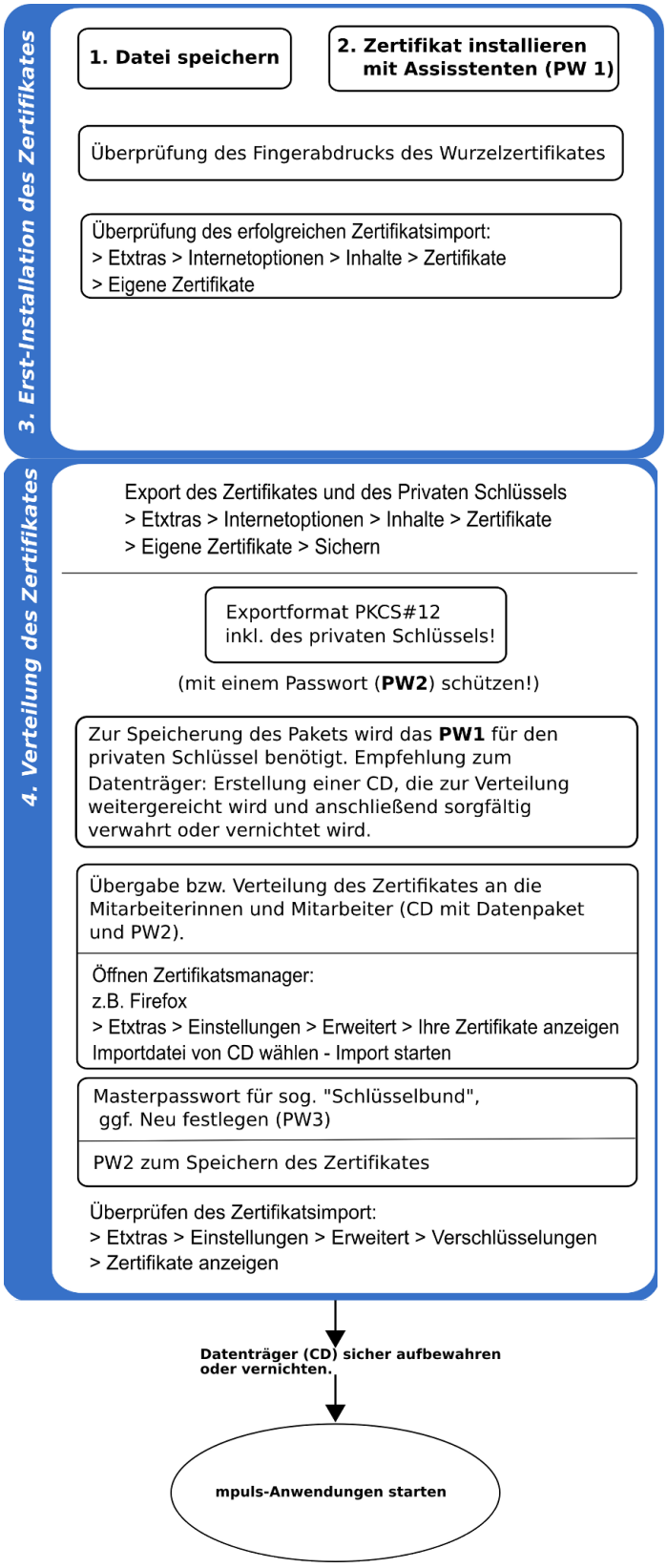
```
0049-2371-787 6 99 02
```

individuelle Unterstützung anfragen.

Sie erreichen unter dieser Rufnummer die Beraterinnen und Berater des Trustcenters, die Ihnen Mo. - Do. von 08:00 Uhr bis 16:00 Uhr sowie Fr. von 08:00 Uhr bis 13:00 Uhr (außer an Feiertagen in Nordrhein-Westfalen) zur Verfügung stehen.

Zertifizierungsprozess im Überblick am Beispiel von mpuls_S




3. Erst-Installation des Zertifikates
1. Datei speichern
2. Zertifikat installieren mit Assisstenten (PW 1)
Überprüfung des Fingerabdrucks des Wurzelzertifikates
Überprüfung des erfolgreichen Zertifikatsimport:
> Etxtras > Internetoptionen > Inhalte > Zertifikate
> Eigene Zertifikate
4. Verteilung des Zertifikates
Export des Zertifikates und des Privaten Schlüssels
> Etxtras > Internetoptionen > Inhalte > Zertifikate
> Eigene Zertifikate > Sichern
Exportformat PKCS#12
inkl. des privaten Schlüssels!
(mit einem Passwort (PW2) schützen!)
Zur Speicherung des Pakets wird das PW1 für den privaten Schlüssel benötigt. Empfehlung zum Datenträger: Erstellung einer CD, die zur Verteilung weitergereicht wird und anschließend sorgfältig verwahrt oder vernichtet wird.
Übergabe bzw. Verteilung des Zertifikates an die Mitarbeiterinnen und Mitarbeiter (CD mit Datenpaket und PW2).
Öffnen Zertifikatsmanager:
z.B. Firefox
> Etxtras > Einstellungen > Erweitert > Ihre Zertifikate anzeigen
Importdatei von CD wählen - Import starten
Masterpasswort für sog. "Schlüsselbund", ggf. Neu festlegen (PW3)
PW2 zum Speichern des Zertifikates
Überprüfen des Zertifikatsimport:
> Etxtras > Einstellungen > Erweitert > Verschlüsselungen
> Zertifikate anzeigen
Datenträger (CD) sicher aufbewahren oder vernichten.
mpuls-Anwendungen starten

KAPITEL 7

Dokumentinformation

Projekbezeichnung: PWE

Projektleiter AG: Dr. Jan Gregersen

Projektleiter AN: Frank Koormann

Verantwortlich: PWE Scrum Team

Erstellt am: 14.07.2015

Zuletzt bearbeitet: 29.01.2019

Bearbeitungszustand: fertig gestellt

7.1 Änderungen

Datum	Version	Kapitel	Beschreibung der Änderung	Autor	Zustand
14.07.2015	0.1	Alle	Initiale Produkterstellung	ab, dd, fk	freigegeben
27.08.2015		2 und 5.2	Hinweis Antragstellung Win7 und IE11	fk	
28.08.2015	1.0				freigegeben
29.01.2019	1.0	4	Sichern mit Firefox	ab	freigegeben
04.08.2021	1.0	Alle	Umbennung Citkomm zu SIT	ab	
04.08.2021			Verweis zur Hotline entfernt		
04.08.2021			EDGE als Möglichkeit hinzugefügt		