JUGEND
MIGRATIONS
DIENSTE

JMD i-mpuls JMD

Web-Anwendungs-Server für computergestützte Fallakten

Handbuch Funktionszertifikat

Stand: 9. September 2025

Projektbezeichnung	i-mpuls JMD	
Projektleiter (AG)	Ulrike Kiese (Servicebüro JMD)	
Projektleiter (AN)	Frank Koormann (Intevation)	
Verantwortlich	Katharina Schütze, Frank Koormann Intevation GmbH, Neuer Graben 17, 49074 Osnabrück	
Zuletzt geändert	9. September 2025	
Bearbeitungszustand		in Bearbeitung
		vorgelegt
	x	fertig gestellt

Inhaltsverzeichnis

1 Einleitung

Kurzportrait Funktionszertifikat	
Gültigkeits-dauer	**3 Jahre** Ein Wechsel in der Förderperiode (z.B. Adresse oder Verantwortlichkeiten) erfordern nicht, dass das Zertifikat neu beantragt werden muss.
Sicherheits-Hinweis	Wurde ein Rechner bzw. Laptop mit installiertem Zertifikat gestohlen oder ist verloren gegangen, stellen Sie bitte unverzüglich einen **Sperrantrag** (formlos per E-Mail) beim Servicebüro JMD, um die Daten vor Missbrauch zu schützen.
Aussteller	Vergabestelle i-mpuls JMD Funktionszertifikate, Intevation GmbH
Verantwortlichkeit	Eine Person pro Einrichtung, Name und E-Mail bitte an das Servicebüro JMD melden.
Dateiformat	Die Funktionszertifikate basieren auf einer Public-Key-Infrastruktur und bestehen aus öffentlichen Schlüsseln (Public-Key) und einem privaten Schlüssel. Beides wird durch die Vergabestelle erstellt und in einer verschlüsselten **p12-Datei** per E-Mail versendet.

i-mpuls JMD ist eine Web-Anwendung, bei der die Mitarbeitenden verschlüsselt über das Internet mit dem i-mpuls JMD 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 JMD kommunizieren. Zertifikate für einzelne Einrichtungen werden als Funktionszertifikate vergeben. Die Zertifikatverwaltung wird von der Intevation GmbH betrieben.

Insgesamt ist ein dreistufiges Verfahren implementiert:

1. Zunächst wird über das **Serverzertifikat** das JMD i-mpuls System gegenüber der Anwenderin bzw. dem Anwender authentifiziert.
2. Durch das **Funktionszertifikat** wird die Anwenderin bzw. der Anwender als Mitarbeiterin bzw. Mitarbeiter einer Einrichtung authentifiziert.
3. Im letzten Schritt authentifiziert sich die Mitarbeiterin bzw. der Mitarbeiter durch **Benutzername und Passwort** persönlich.

2 Der Vergabeprozess

Für den Vergabeprozess wird in jeder Einrichtung eine verantwortliche Person festgelegt.

- Name und die E-Mail Adresse müssen dem JMD Servicebüro in einem formlosen Schreiben mitgeteilt werden.
- Das Servicebüro JMD übermittelt den Bedarf an die Vergabestelle.
- Im Anschluss erstellt die Vergabestelle das Zertifikat.
- Die verantwortliche Person erhält:
  - eine entsprechende E-Mail an die angegebene E-Mail-Adresse sowie
  - parallel dazu einen Brief per Postversand mit dem Passwort.

2.1 Erst-Installation des Zertifikats

Zur Installation benötigen sie einen aktuellen und sicherheits-gepflegten Browser (Edge, Firefox oder Chrome).

1. **Datei lokal abspeichern**: Klicken Sie mit der rechten Maustaste auf den Anhang der E-Mail und wählen ▸ **Speichern unter**… in einem beliebigen Verzeichnis auf ihrem lokalen Rechner.
2. **Zertifikatverwaltung im Browser öffnen**:

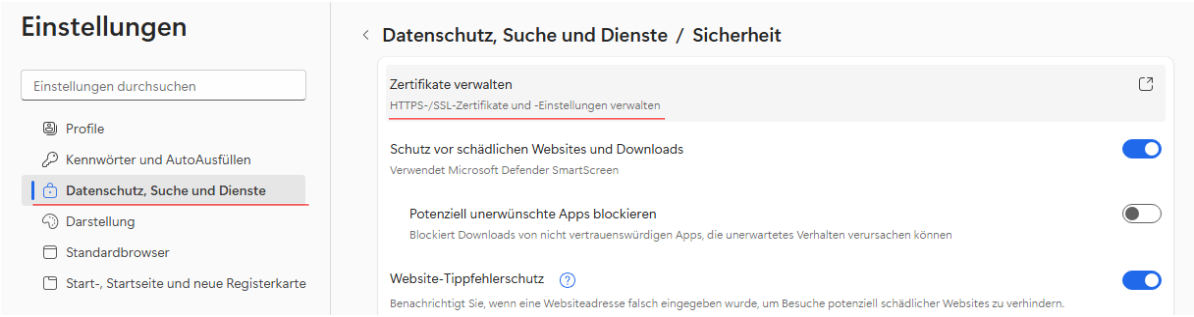
Edge	Siehe nachfolgendes Beispiel
Firefox	▸ „Burger-Menü“ ☰ oben rechts ▸ Einstellungen ▸ Datenschutz & Sicherheit ▸ Abschnitt: Sicherheit ▸ Zertifikate ▸ Zertifikate anzeigen ▸ Reiter „Ihre Zertifikate“ ▸ Importieren
Chrome	▸ „3-Punkt Menü“ … oben rechts ▸ Einstellungen ▸ Datenschutz und Sicherheit ▸ Abschnitt: Sicherheit ▸ Erweitert > Zertifikate verwalten ▸ „Meine Zertifikate“ (Menü links) ▸ Zertifikate ansehen ▸ Importieren

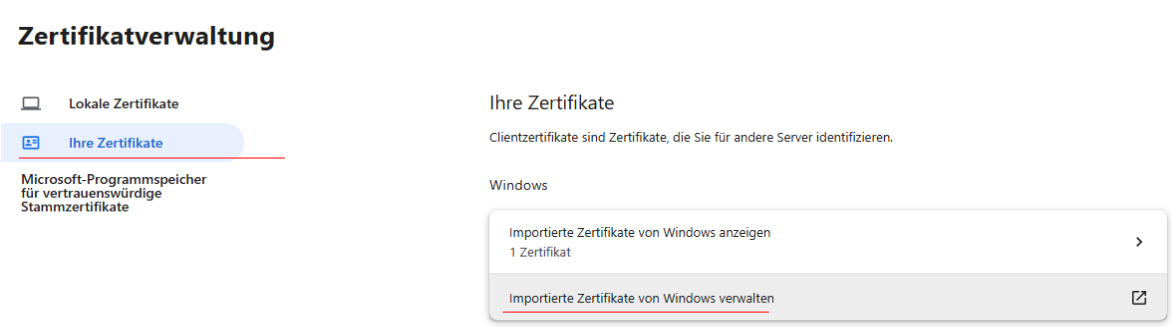
Die Importvorgänge ähneln sich in allen Browsern. Da unter Windows im Edge einige zusätzliche Optionen möglich sind (z.B. Exportierbarkeit des privaten Schlüssel) wird dieser Importvorgang detaillierter dargestellt.

Importvorgang am Beispiel des Edge:

a) Öffnen Sie die Zertifikatverwaltung im Edge

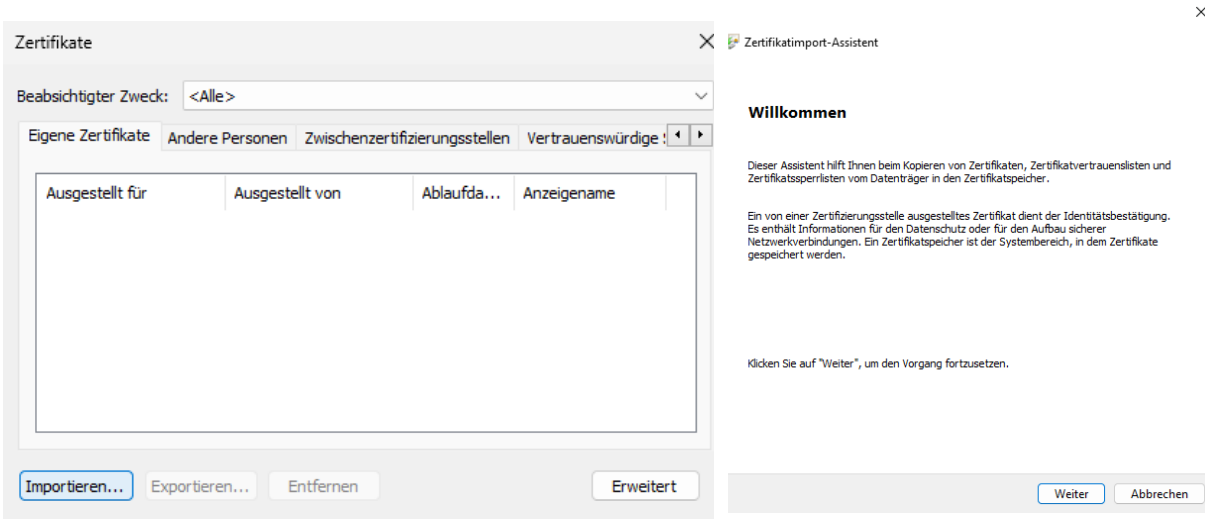
- ▸ 3-Punkt-Menü oben rechts
- ▸ Einstellungen
- ▸ Datenschutz, Suche und Dienste
- ▸ Sicherheit
- ▸ Zertifikate verwalten
- ▸ Ihre Zertifikate (linkes Menü)
- ▸ importierte Zertifikate von Windows **verwalten**



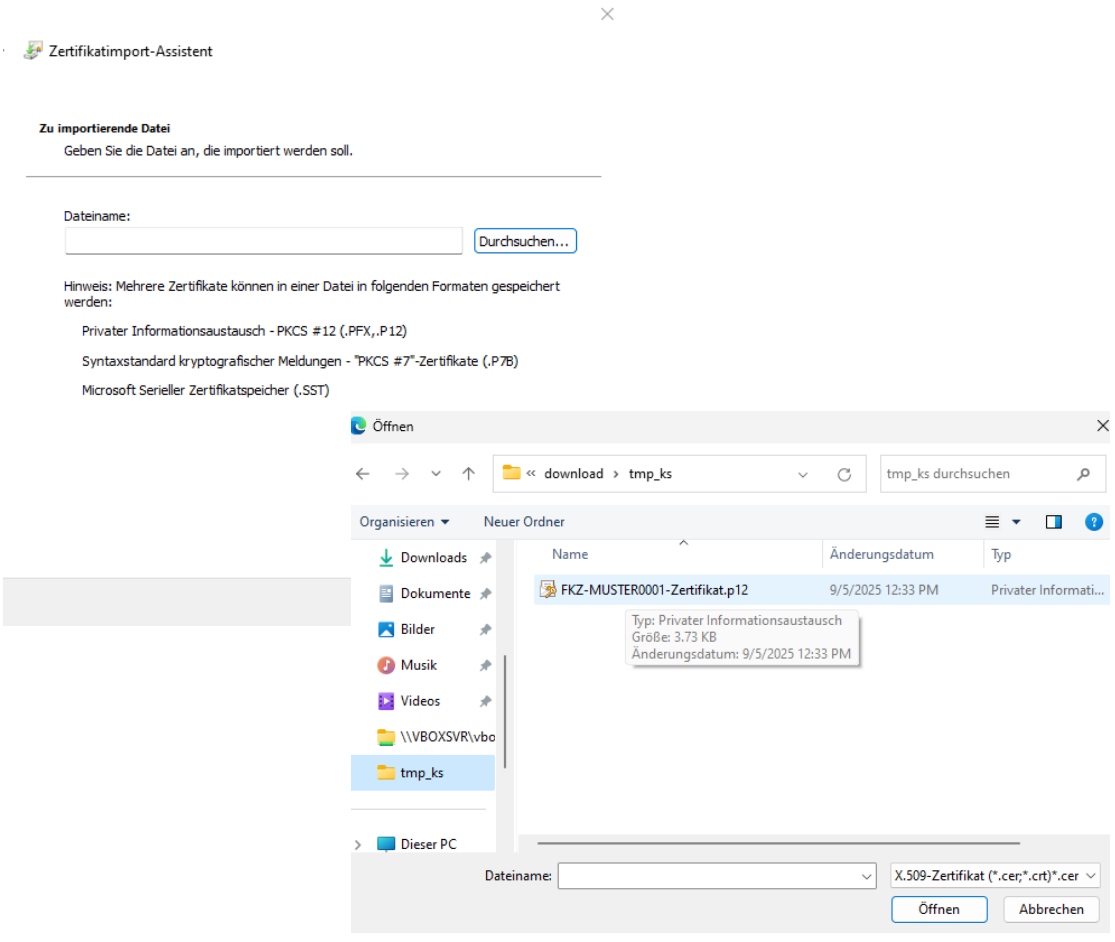


3. Datei importieren:

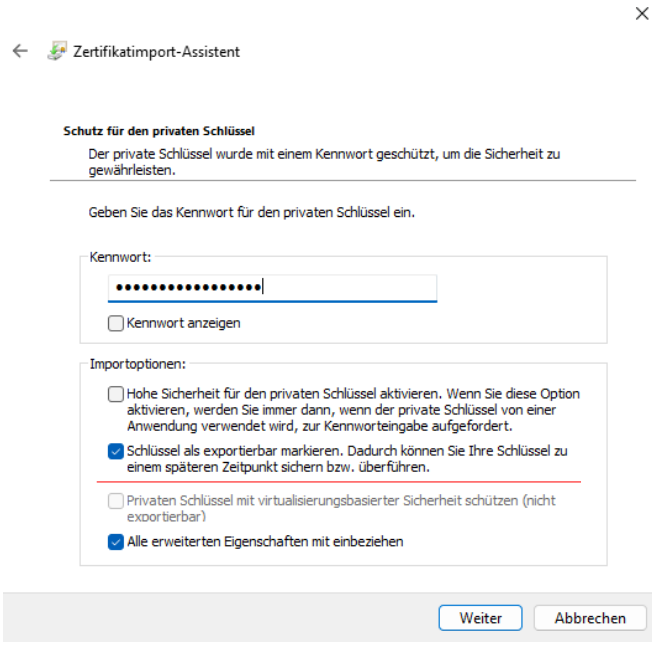
a) Klicken Sie auf ▸ Importieren und ▸ Weiter.



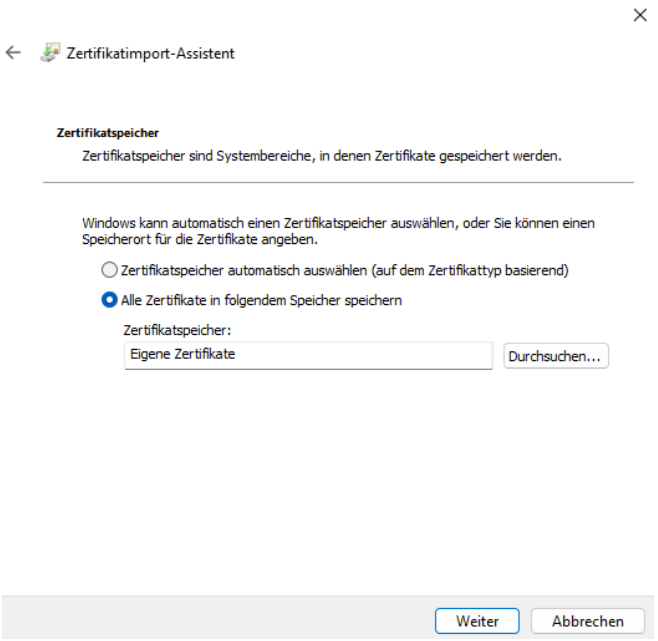
b) Klicken sie auf ▸ Durchsuchen und wählen die vorher gespeicherte Zertifikatsdatei von ihrem lokalen Rechner aus. Bestätigen Sie die Auswahl mit Klick auf ▸ Öffnen



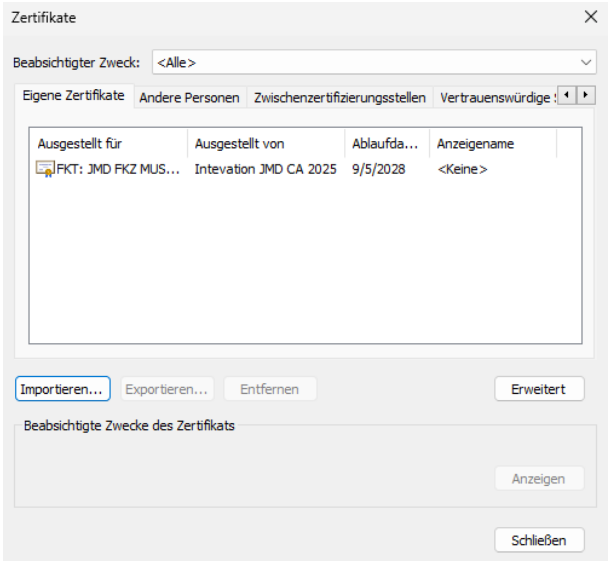
c) Geben Sie unter ▸ Kennwort das aus dem per Briefpost gesendete Passwort ein.
WICHTIG: Aktivieren sie **zusätzlich** die Option ▸ „**Schlüssel als exportierbar markieren**“ und bestätigen mit ▸ Weiter.



d) Wählen Sie den Zertifikatsspeicher „Eigene Zertifikate“ aus, der in der Regel voreingestellt ist und bestätigen mit ▸ Weiter.



4. **Import überprüfen**: Bitte überprüfen Sie abschließend den erfolgreichen Import des Zertifikats.



5. **Zugriff auf i-mpuls JMD:** Testen Sie nun den Zugriff auf den Anwendungsbereich ihrer Einrichtung auf dem Server.

2.2 Verteilen des Zertifikats

Das Sicherheitskonzept von JMD i-mpuls sieht vor, dass sich jede*r Nutzende als Mitarbeiterin bzw. Mitarbeiter einer Einrichtung authentisiert. Das Zertifikat muss dafür an **jedem Arbeitsplatz mit Rechner** und für jede Benutzerin bzw. jeden Benutzer installiert 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 gibt es 2 Optionen:

1. Befolgen Sie die oben beschriebenen Schritte zur Erst-Installation des Zertifikats auch an allen anderen Arbeitsplätzen.

   Wichtig: Geben Sie **niemals** die Zertifikatsdatei sowie das Passwort gemeinsam in einer E-Mail weiter. Das Passwort aus dem Brief geben sie idealerweise persönlich oder mündlich (z.B. per Telefon) weiter.

2. Fall die Original E-Mail/Datei oder das Passwort nicht mehr vorhanden sind, kann das Zertifikat auch aus dem Browser heraus **exportiert**, gesichert und im Anschluss an weiteren Arbeitsplätzen importiert werden. Dieses Verfahren wird im Anhang dargestellt.

3 Support und Hilfen

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

3.1 FAQ – die häufigsten Fragen

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

  Eine Zuständigkeitsänderung für die Zertifikatsbeantragung sollten Sie mit einem formlosen Schreiben dem Servicebüro bekannt geben. Nennen Sie die vorherige und die neue Ansprechperson inkl. E-Mail Adresse. Die Änderung der Zuständigkeit erfordert **keine Neubeantragung**! Das bestehende Zertifikat Ihrer Einrichtung bleibt weiterhin gültig.

- **Wie oft muss das Zertifikat erneuert werden?**

  Das Sicherheitskonzept von JMD i-mpuls sieht vor, dass die Funktionszertifikate, die Sie dazu berechtigen auf die entsprechenden Server und Datenbanken zuzugreifen, **alle drei Jahre** erneuert werden.

- **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.

- **Kann JMD i-mpuls an einem Computer mit mehreren Browsern verwendet werden?**

  Ja, Sie müssen das Funktionszertifikat in **jedem** verwendeten Browser separat importieren.

- **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.

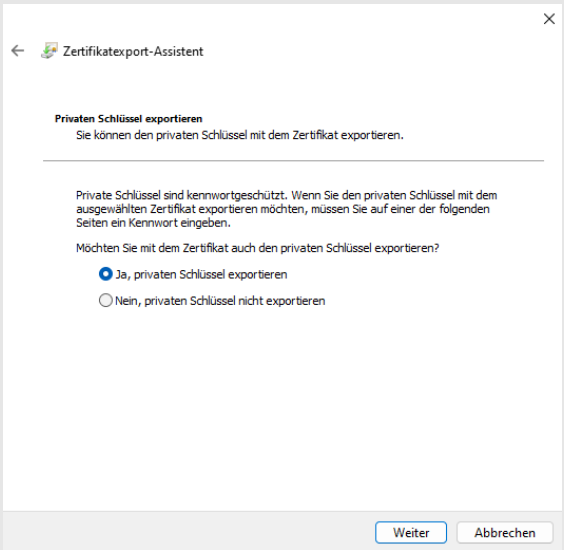
3.2 Anhang

Eine spätere Verteilung von Zertifikaten z.B. an neue Mitarbeitende des JMD kann auch mittels Export erfolgen, sofern die Original E-Mail und das Passwortschreiben nicht mehr zugänglich oder vorhanden sind. Das Vorgehen wird beispielhaft am Browser Edge erklärt.

3.2.1 Zertifikats-Export

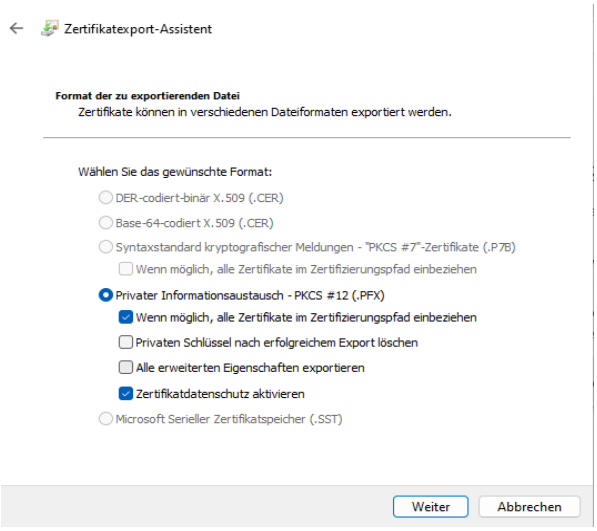
1. Öffnen Sie den Zertifikatspeicher des Edge :
   - ▸ 3-Punkt-Menü oben rechts ▸ Einstellungen ▸ Datenschutz, Suche und Dienste ▸ Sicherheit ▸ Zertifikate verwalten ▸ Ihre Zertifikate (linkes Menü) ▸ importierte Zertifikate von Windows **verwalten**
2. Markieren Sie das zu exportierende Zertifikat und 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!** Ist die Auswahl nicht möglich, wurde beim Import das entsprechende Häkchen nicht aktiviert. Prüfen Sie ob es anderer Stelle bzw. Arbeitsplätzen Zertifikate gibt, wo der private Schlüssel als exportierbar markiert wurde. (*Diese Option erlaubt ausschließlich der Edge*)

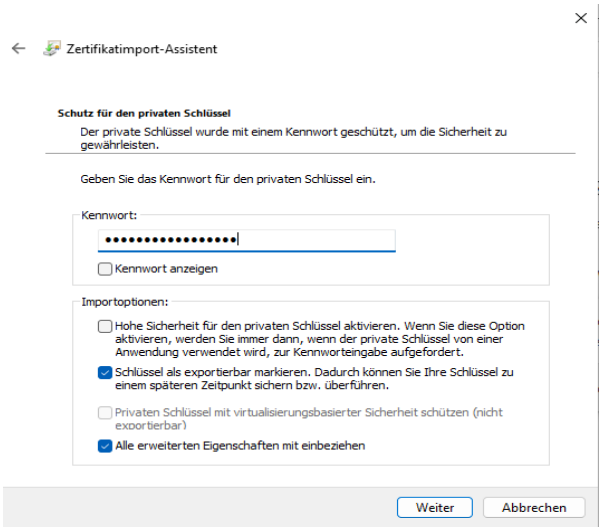


   - Für den Export ist das Format „PKCS #12“ vorgegeben. Wählen Sie ggf. die Option ▸ „Wenn möglich alle Zertifikate im Zertifizierungspfad einbeziehen“.

- Stellen Sie sicher, dass der **private Schlüssel nicht gelöscht** wird!



- Sie werden aufgefordert, den exportierten Schlüssel durch ein selbstgewähltes ▸ Kennwort (**PW2**) zu schützen. Sie benötigen dieses Kennwort, um Schlüssel und Zertifikat auf einem anderen Rechner zu importieren.



3. Wählen Sie abschließend einen ▸ Dateinamen für das Zertifikat und klicken abschließend auf ▸ „Fertigstellen“. Der private Schlüssel und das Funktionszertifikat sind damit exportiert und befinden sich in einer Datei mit der typischen Endung .p12 bzw. .pfx

4. 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 (**PW2**) der Exportdatei erinnern können.

3.2.2 Zertifikats-Import

Für den Import des Funktionszertifikats und des Schlüssels benötigen Sie die Exportdatei (z.B. auf einem USB-Stick) und das Kennwort (**PW2**), das während des Exports vergeben wurde.

Der Import ist den bisher beschriebenen Vorgängen auch in anderen Browsern ähnlich: Öffnen sie zuerst die Zertifikatsverwaltung (siehe 2.1 Erst-Installation des Zertifikats, S. 4) und importieren dann das gesicherte Zertifikat. Sie benötigen nun das **PW2** (und nicht mehr das Passwort aus dem postalisch gesendetem Brief).

Beispiel Firefox:

1. Klicken Sie im Zertifikat-Manager den Knopf ▸ „Importieren“ und wählen die im vorherigen Schritt erstellte Exportdatei aus.
2. Der Firefox speichert die Schlüssel in einem „Schlüsselbund“, der durch ein Master-Passwort geschützt werden kann. Haben Sie bereits ein Haupt- bzw. Master-Passwort im Firefox eingerichtet, werden Sie aufgefordert Ihr bestehendes Passwort einzugeben. (*Wir empfehlen zum Schutz der Zertifikate und privaten Schlüssel diese Sicherheitseinstellung im Browser zu aktivieren.*)
3. Bei korrekter Eingabe des Passwortes wird der erfolgreiche Import bestätigt und das Funktionszertifikat ist im Zertifikat-Manager aufgeführt.
4. Nach dem erfolgreichen Import von privatem Schlüssel und Zertifikaten kann vom entsprechenden Nutzerkonto aus auf den JMD i-mpuls-Anwendungsbereich Ihrer Einrichtung zugegriffen werden.
5. 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.