



Senatsverwaltung für Bildung, Jugend und Familie
Integrierte Software Berliner Jugendhilfe -ISBJ-

Installationsanleitung für Zertifikate zur Nutzung der ISBJ-Portale

Autor: V E 21
Datum: 27.02.2024
Version: 3.0



1 Inhaltsverzeichnis

1	Einleitung	3
2	Mozilla Firefox.....	4
3	Google Chrome	10
4	Microsoft Edge.....	15
5	Apple Safari	19

1 Einleitung

Dieses Dokument beschreibt die Installation eines Zertifikats zur Nutzung der ISBJ Portale für Träger und Einrichtungen. Die Installationsanleitung gilt für die Browser Mozilla Firefox, Google Chrome, Microsoft Edge und Safari.

Von der Nutzung des Internet Explorers raten wir aus Sicherheitsgründen ab.

Um sich in einem der Portale anmelden zu können, muss jeder Benutzer einen Benutzernamen und ein Kennwort besitzen. Der Benutzername und das Kennwort werden nach Einrichtung durch den Administrator über das BNV-Portal an die hinterlegte E-Mailadresse des Benutzers versendet.

Außerdem benötigt der Benutzer ein Zertifikat, das ihm sein Administrator zusammen mit dem Kennwort für die Installation zur Verfügung stellt. Das Zertifikat gehört zum Administrator und ist für alle ihm zugeordneten Benutzer gleich.

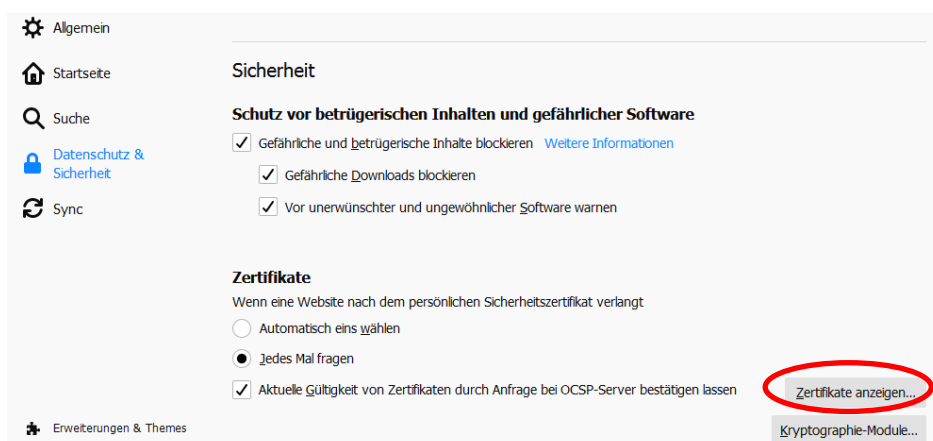
Jeder Benutzer, der ein gültiges Zertifikat verwendet, hat einen - seinen Rechten entsprechenden - Zugriff auf alle ISBJ-Portale.

2 Mozilla Firefox

Das ISBJ Trägerportal unterstützt generell den Mozilla Firefox ab der Version 25. Im Folgenden wird die Installation des Zertifikats exemplarisch anhand des Mozilla Firefox Version 102.14.0esr dargestellt.

1. Speichern Sie die Zertifikatsdatei aus der Email (Betreff: Zertifikat fuer Zugang zum ISBJ Portal) zunächst lokal auf Ihrem Rechner ab.

2. Starten Sie Mozilla Firefox und wählen Sie im Menü „Extras“ den Punkt „Einstellungen“ aus. Alternativ können Sie auch über die Menüschildfläche am rechten Rand die Einstellungen aufrufen. Wählen Sie nun links „Datenschutz und Sicherheit“ aus und klicken ganz unten auf „Zertifikate anzeigen“.

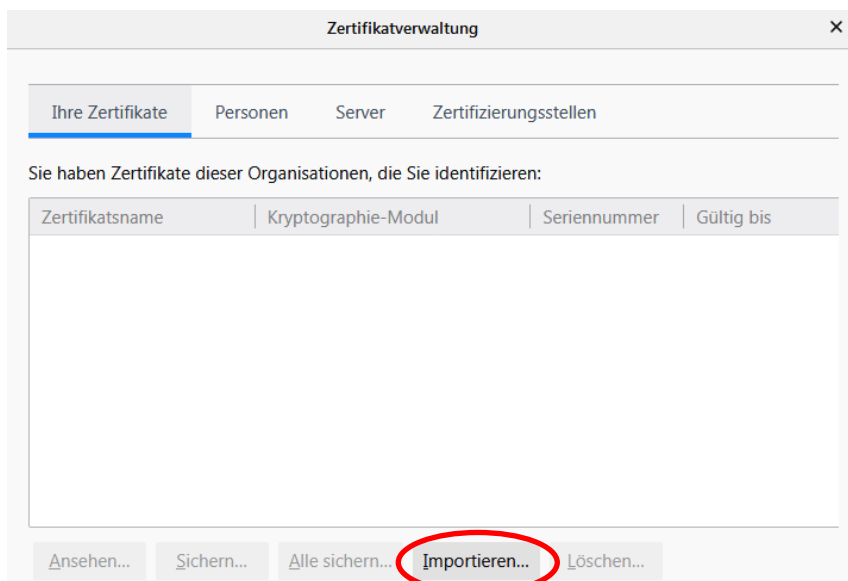


3. Der Assistent zur Organisation von Zertifikaten öffnet sich. Wechseln Sie in den Reiter „Ihre Zertifikate“.



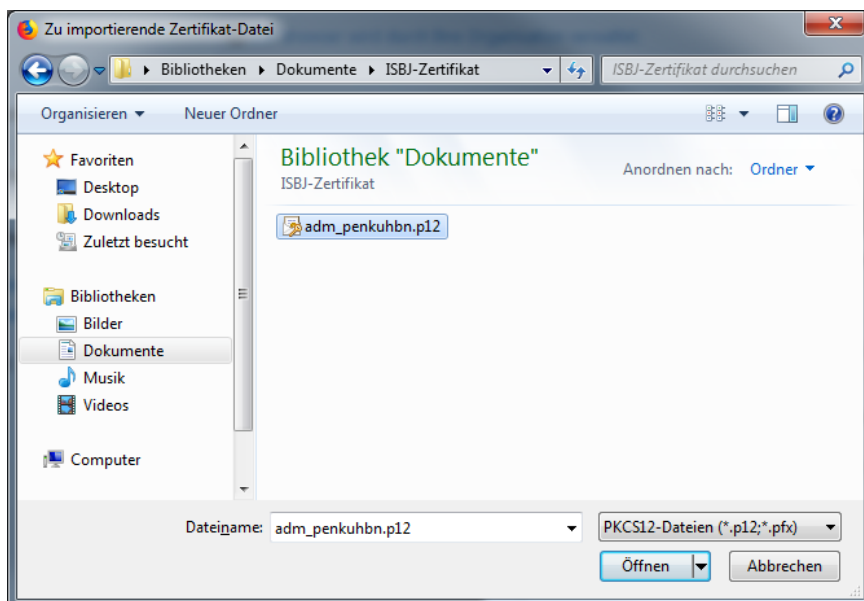
Wir empfehlen zunächst alle abgelaufenen ISBJ Zertifikate zu löschen. ISBJ Zertifikate erkennen Sie daran, dass in der Spalte „Ausgestellt von“ ISBJ Zertifizierungsinstanz angegeben ist.

4. Klicken Sie hier zunächst auf die Schaltfläche „Importieren“.



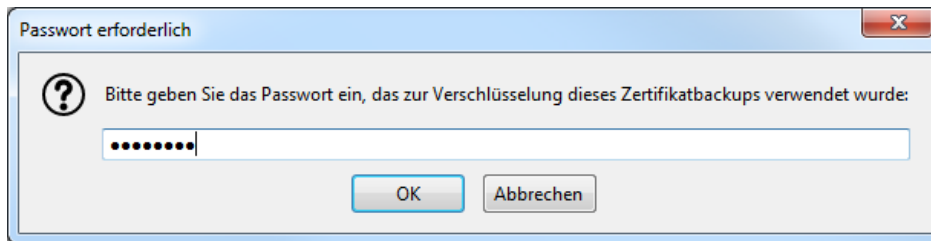
5. Es öffnet sich ein Fenster zur Auswahl der zu importierenden Zertifikatsdatei. Wählen Sie nun die zuvor heruntergeladene Zertifikatsdatei aus.

Bestätigen Sie die Auswahl über die Schaltfläche „Öffnen“.

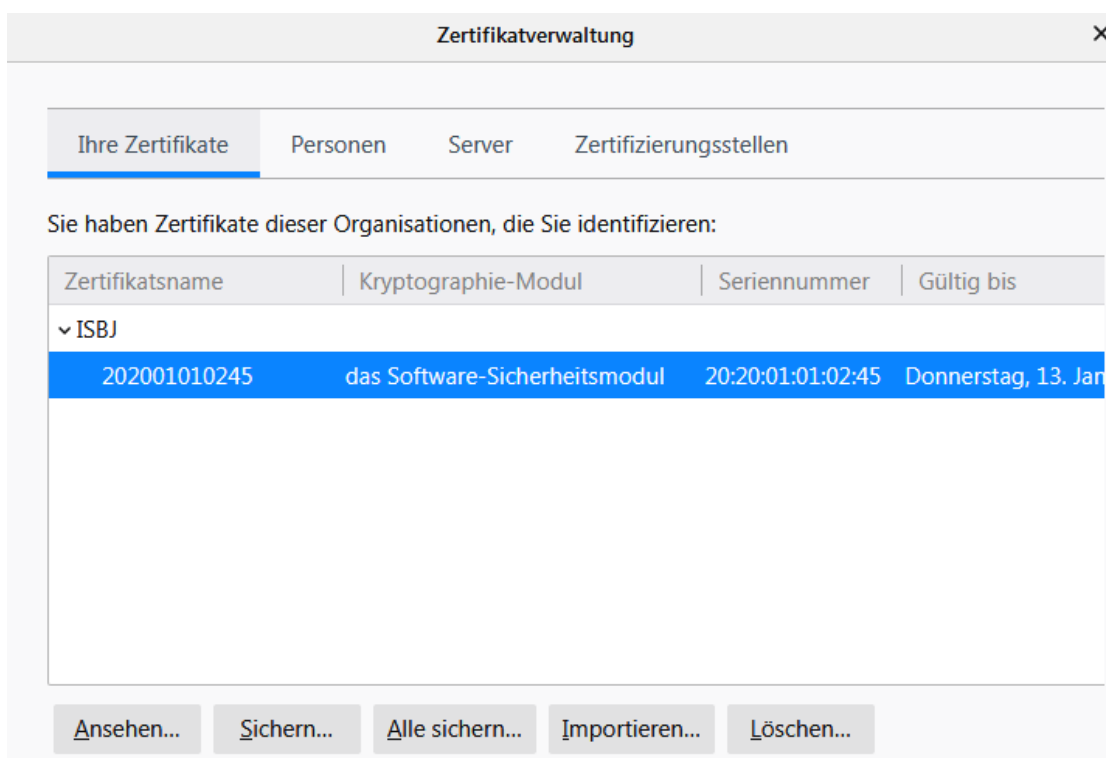


Hinweis: Im Beispiel wurde das Zertifikat zuvor unter „Dokumente“ in einem separat erstellten Ordner namens „ISBJ-Zertifikat“ gespeichert. Sofern Sie keinen anderen Ort ausgewählt haben, wird das Zertifikat standardmäßig unter „Downloads“ gespeichert.

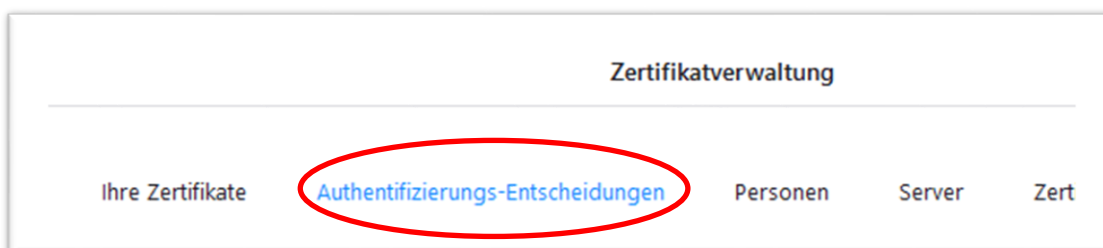
6. Geben Sie das Kennwort für die Installation des Zertifikats aus dem Brief im entsprechenden Feld ein. Klicken Sie auf „OK“.



7. Das Zertifikat erscheint jetzt in der Liste Ihrer Zertifikate.



7. Klicken Sie im Zertifikatsmanager auf den Reiter „Authentifizierungsentscheidungen“.



8. Falls hier bestehende Einträge vorhanden sind, die unter Host „verwalt-berlin.de“ enthalten, klicken Sie diese mit der linken Maustaste an und klicken unten auf „Löschen.“

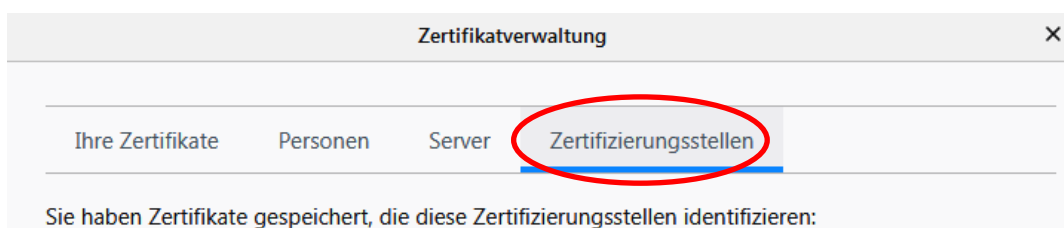
Beispiele:

portal.isbj.verwalt-berlin.de

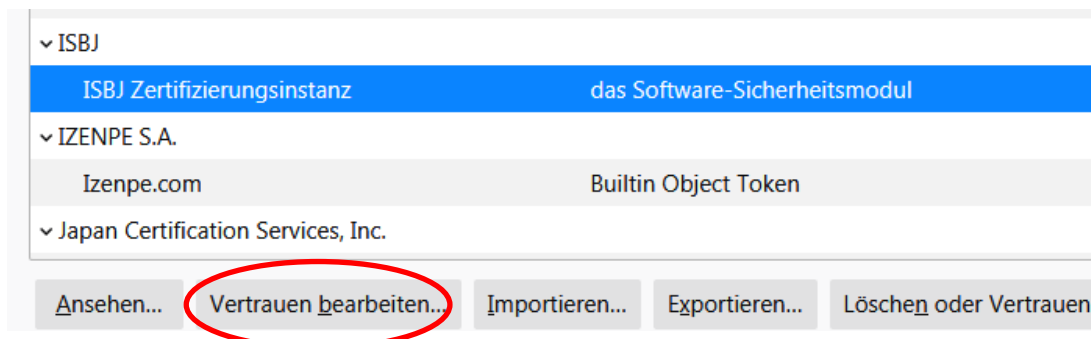
bnvportalp.isbj.verwalt-berlin.de

stportal.isbj.verwalt-berlin.de

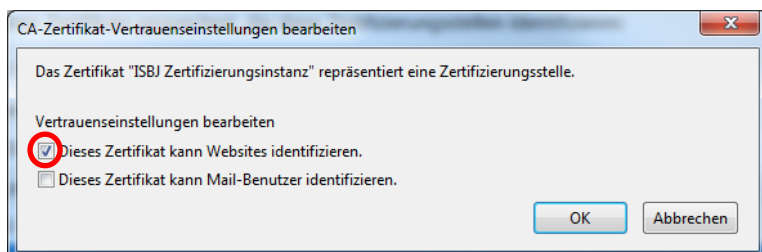
8. Wechseln Sie im Zertifikats-Manager auf den Reiter „Zertifizierungsstellen“.



9. Suchen Sie in der Liste nach ISBJ und markieren Sie den Eintrag „ISBJ Zertifizierungsinstanz“ mit der linken Maustaste. Klicken Sie danach auf „Vertrauen bearbeiten“.

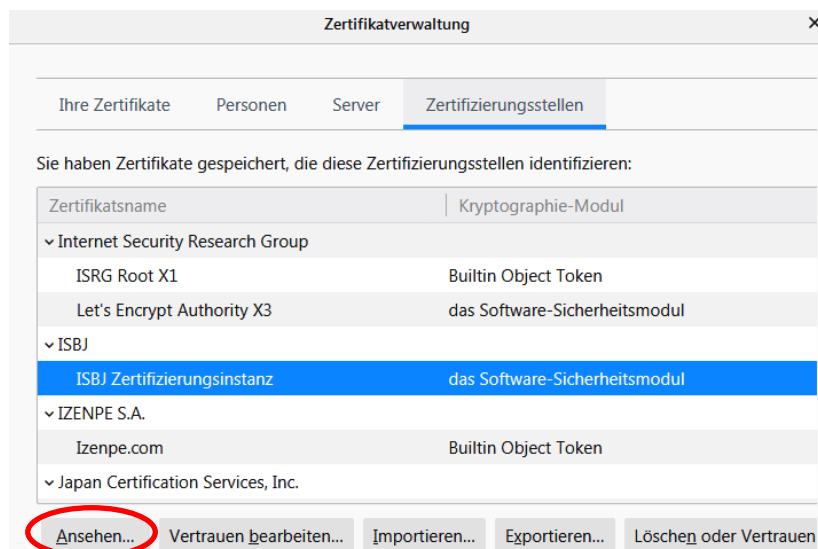


Es öffnet sich das Pop-Up „CA-Zertifikat-Vertrauenseinstellungen bearbeiten“. Markieren Sie bitte die Vertrauenseinstellung „Dieses Zertifikat kann Websites identifizieren“, und bestätigen Sie mit „OK“.



Kontrolle des Fingerabdrucks:

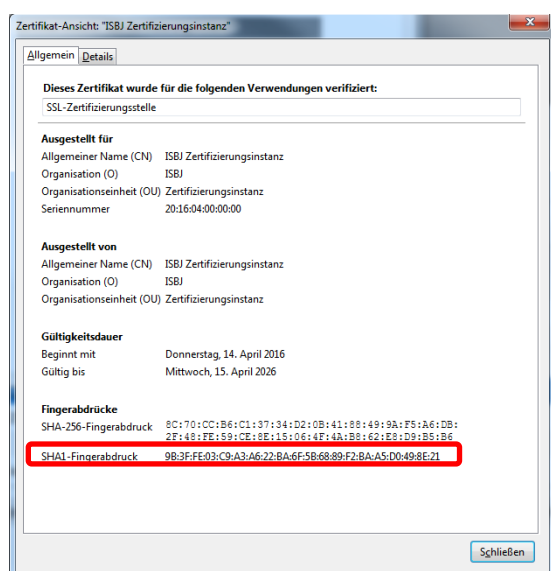
10. Wechseln Sie im Zertifikats-Manager auf den Reiter „Zertifizierungsstellen“. Suchen Sie in der Liste nach ISBJ und markieren Sie den Eintrag „ISBJ Zertifizierungsinstanz“. Klicken Sie anschließend auf die Schaltfläche „Ansehen...“



Hinweis: Alternativ kann unter „Kryptographie-Modul“ auch „OS Client Cert Token“ stehen.

11. Vergleichen Sie bitte in dieser Ansicht den SHA1-Fingerabdruck mit dem Fingerabdruck aus dem per Post geschickten Brief mit dem Installationskennwort für das Zertifikat.

Falls Sie mehrere ISBJ Zertifizierungsinstanzen haben, prüfen Sie bitte die jeweils aktuellste.



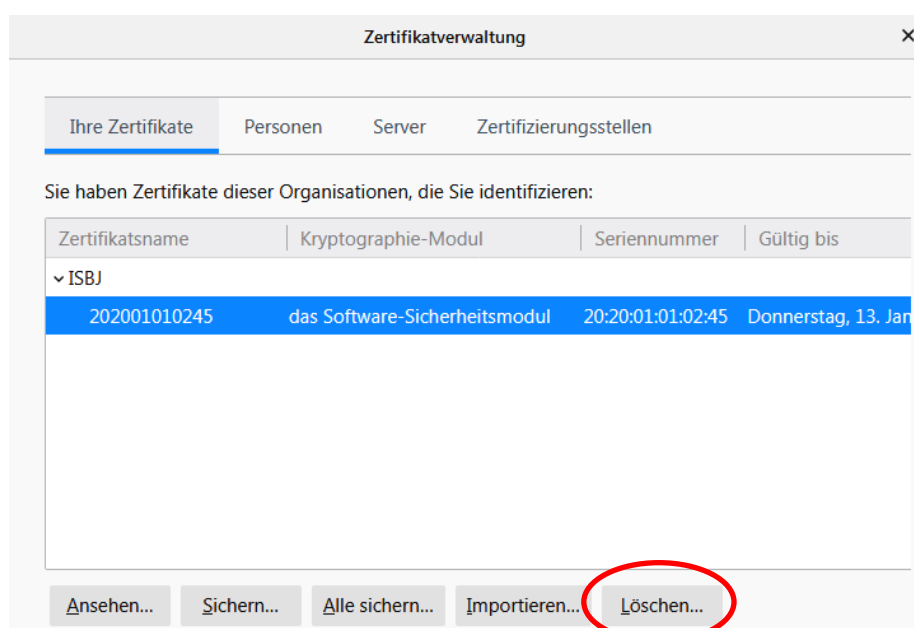
11.1 Stimmen die Daten überein, kann das installierte Zertifikat genutzt werden. Bitte klicken Sie auf „Schließen“

11.1.1 Klicken Sie im Anschluss im Fenster der Einstellungen auf „OK“, um die Installation des Zertifikats abzuschließen.

11.2 Stimmen die Fingerabdrücke **nicht** überein, muss das Zertifikat wieder deinstalliert werden. Bitte klicken Sie auf „Schließen“.

11.2.1 Wechseln Sie in den Reiter „Ihre Zertifikate“.

11.2.2 Wählen Sie das importierte Zertifikat aus der angezeigten Liste aus und klicken Sie auf „Löschen“.



11.2.4 Das Zertifikat wird aus der Liste entfernt. Klicken Sie im folgenden Fenster auf „OK“.

11.2.5 Sie können nun die Einstellungen schließen.

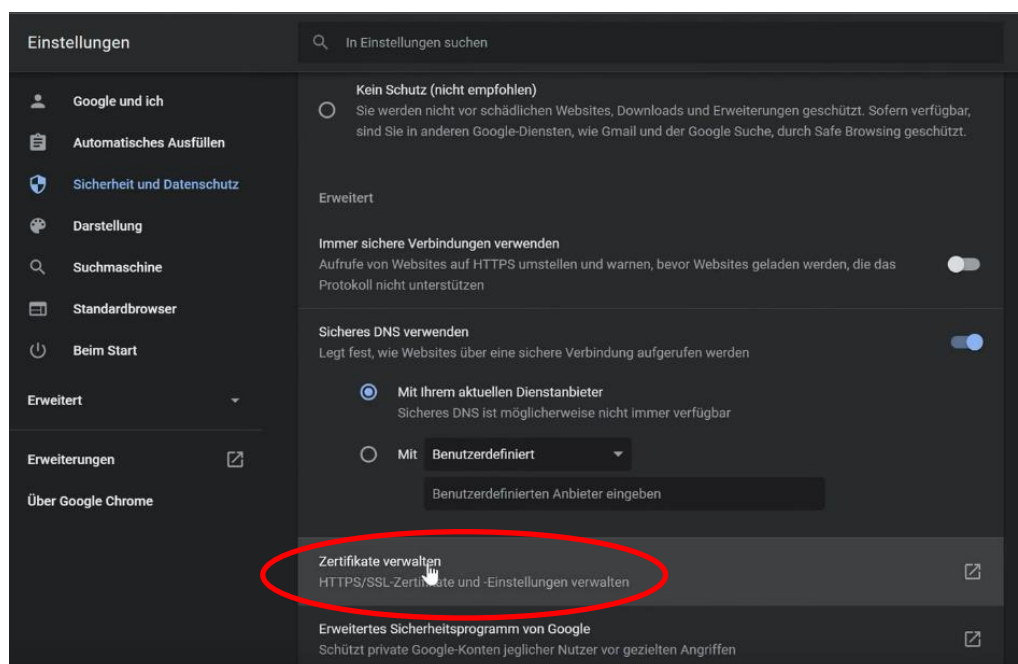
11.2.6 Bitte melden Sie nicht übereinstimmende Fingerabdrücke sofort an:
traeger-service@senbjf.berlin.de

3 Google Chrome

Das ISBJ Trägerportal unterstützt generell Google Chrome ab der Version 33. Im Folgenden wird die Installation des Zertifikats exemplarisch anhand der Google Chrome Version 97 dargestellt.

1. Speichern Sie die Zertifikatsdatei aus der Email (Betreff: Zertifikat fuer Zugang zum ISBJ Portal) zunächst lokal auf Ihrem Rechner ab.

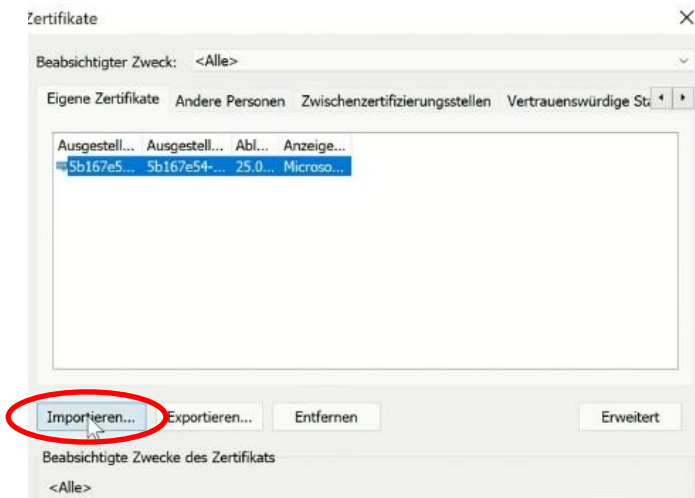
2. Starten Sie Google Chrome und wählen Sie über die Menüschaltfläche oben rechts den Punkt „Einstellungen“ aus. Auf der linken Seite klicken Sie nun auf die Kategorie „Sicherheit und Datenschutz“ und wählen dann „Sicherheit“ aus. Scrollen Sie hier etwas nach unten und wählen den Punkt „Zertifikate verwalten“.



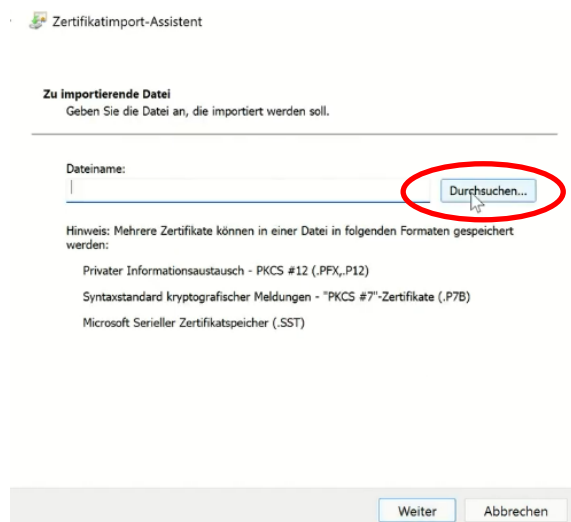
3. Der Assistent zur Organisation von Zertifikaten öffnet sich. Wechseln Sie in den Reiter „Eigene Zertifikate“.

Wir empfehlen zunächst alle abgelaufenen ISBJ Zertifikate zu löschen. ISBJ Zertifikate erkennen Sie daran, dass in der Spalte „Ausgestellt von“ ISBJ Zertifizierungsinstanz angegeben ist.

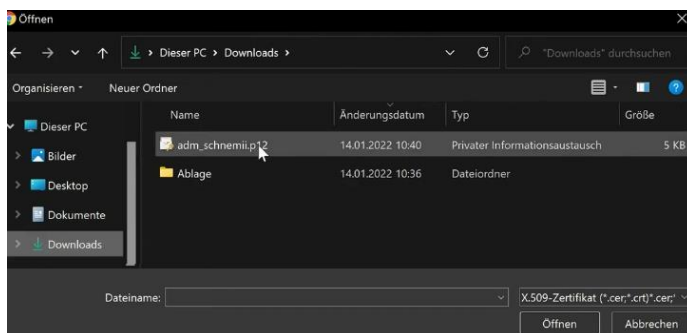
4. Um das neue Zertifikat zu installieren, klicken Sie nun auf die „Importieren“ Schaltfläche um den Zertifikatsimport-Assistenten zu öffnen.




5. Klicken Sie hier auf „Weiter“. Sie werden nun aufgefordert ein Zertifikat auszuwählen. Klicken Sie dazu auf die „Durchsuchen“ Schaltfläche.



6. Wählen Sie nun die zuvor heruntergeladene Zertifikatsdatei aus. Bestätigen Sie die Auswahl über die Schaltfläche „Öffnen“ und klicken Sie dann auf „Weiter“.



7. Geben Sie das Kennwort für die Installation des Zertifikats im entsprechenden Feld ein. Klicken Sie auf „Weiter“.

 Zertifikatimport-Assistent

Schutz für den privaten Schlüssel
Der private Schlüssel wurde mit einem Kennwort geschützt, um die Sicherheit zu gewährleisten.

Geben Sie das Kennwort für den privaten Schlüssel ein.


Kennwort:

Kennwort anzeigen

Importoptionen:

- Hohe Sicherheit für den privaten Schlüssel aktivieren. Wenn Sie diese Option aktivieren, werden Sie immer dann, wenn der private Schlüssel von einer Anwendung verwendet wird, zur Kennworteingabe aufgefordert.
- Schlüssel als exportierbar markieren. Dadurch können Sie Ihre Schlüssel zu einem späteren Zeitpunkt sichern bzw. überführen.
- Privaten Schlüssel mit virtualisierungsbasierter Sicherheit schützen (nicht exportierbar)
- Alle erweiterten Eigenschaften mit einbeziehen

8. Markieren Sie im Fenster „Zertifikatspeicher“ die Option „Zertifikatspeicher automatisch auswählen“. Bestätigen Sie mit „Weiter“.

 Zertifikatimport-Assistent

Zertifikatspeicher
Zertifikatspeicher sind Systembereiche, in denen Zertifikate gespeichert werden.

Windows kann automatisch einen Zertifikatspeicher auswählen, oder Sie können einen Speicherort für die Zertifikate angeben.

Zertifikatspeicher automatisch auswählen (auf dem Zertifikattyp basierend)

Alle Zertifikate in folgendem Speicher speichern

Zertifikatspeicher:

9. Klicken Sie auf „Fertig stellen“, um den Zertifikatimport abzuschließen.

Zertifikatimport-Assistent

Fertigstellen des Assistenten

Das Zertifikat wird importiert, nachdem Sie auf "Fertig stellen" geklickt haben.

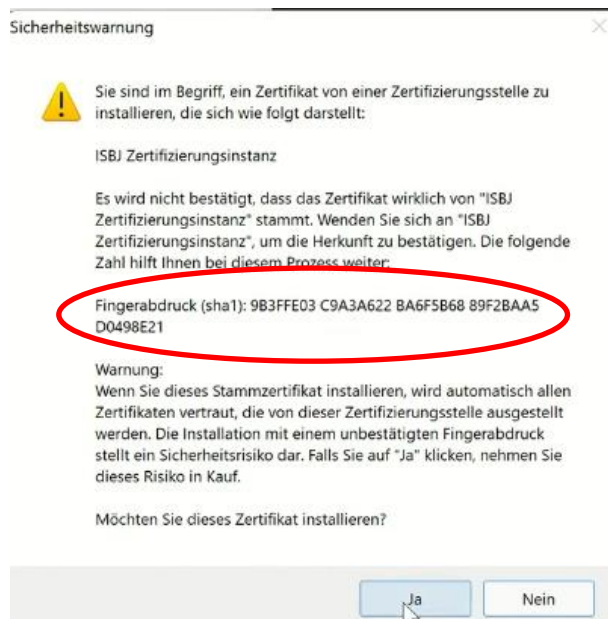
Sie haben folgende Einstellungen ausgewählt:

Gewählter Zertifikatspeicher	Auswahl wird vom Assistenten automatisch festgelegt
Inhalt	PFX
Dateiname	C:\Users\x360m\Downloads\adm_schnemii.p12



Kontrolle des Fingerabdrucks:

10. Eine Sicherheitswarnung mit Informationen zur Zertifizierungsinstanz und dem Hinweis zur Kontrolle des Fingerabdrucks erscheint. Überprüfen Sie den SHA1-Fingerabdruck mit dem Fingerabdruck aus dem per Post geschickten Brief mit dem Installationskennwort für das Zertifikat.



10.1 Stimmen die Daten überein, kann das installierte Zertifikat genutzt werden. Bitte klicken Sie auf „Ja“

10.2 Stimmen die Fingerabdrücke **nicht** überein, sollte das Zertifikat nicht installiert werden. Bitte klicken Sie dazu einfach auf „Nein“.

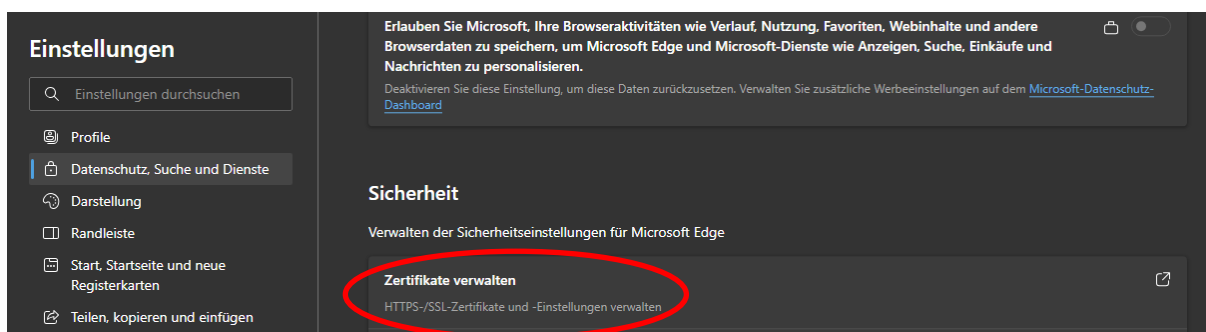
10.2.1 Bitte melden Sie nicht übereinstimmende Fingerabdrücke sofort an:
traeger-service@senbjf.berlin.de

4 Microsoft Edge

Das ISBJ Trägerportal unterstützt generell jede offizielle Version von Microsoft Edge. Im Folgenden wird die Installation des Zertifikats exemplarisch anhand der Microsoft Edge Version 117.0.2045.60 (64 Bit) dargestellt.

1. Speichern Sie die Zertifikatsdatei aus der Email (Betreff: Zertifikat fuer Zugang zum ISBJ Portal) zunächst lokal auf Ihrem Rechner ab.

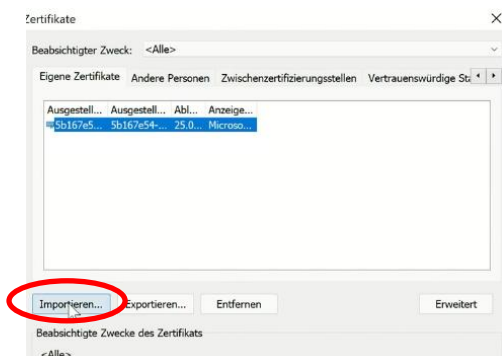
2. Starten Sie Microsoft Edge und wählen Sie über die Menüschaftfläche oben rechts den Punkt „Einstellungen“ aus. Auf der linken Seite klicken Sie nun auf die Kategorie „Datenschutz suche und Dienste“ und wählen dann unter der Überschrift „Sicherheit“ die Schaltfläche „Zertifikate verwalten“ aus.



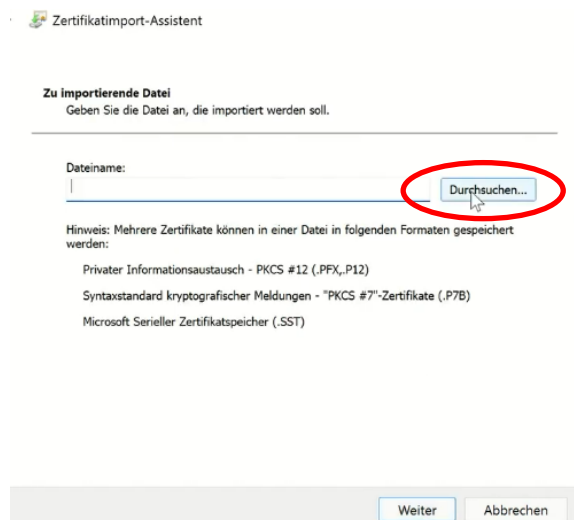
3. Der Assistent zur Organisation von Zertifikaten öffnet sich. Wechseln Sie in den Reiter „Eigene Zertifikate“.

Wir empfehlen zunächst alle abgelaufenen ISBJ Zertifikate zu löschen. ISBJ Zertifikate erkennen Sie daran, dass in der Spalte „Ausgestellt von“ ISBJ Zertifizierungsinstanz angegeben ist.

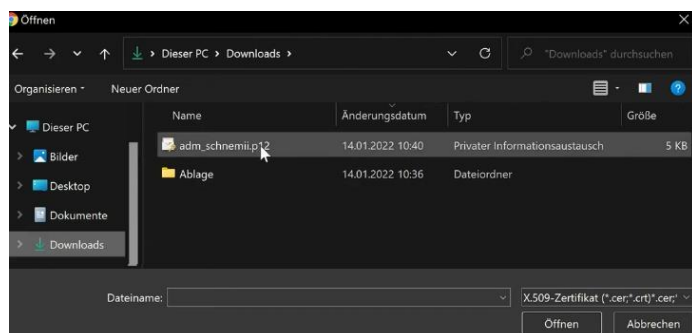
4. Um das neue Zertifikat zu installieren, klicken Sie nun auf die „Importieren“ Schaltfläche um den Zertifikatsimport-Assistenten zu öffnen.



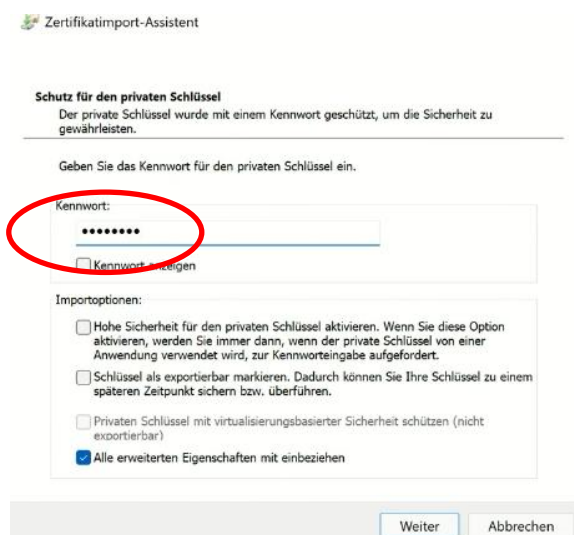
5. Klicken Sie hier auf „Weiter“. Sie werden nun aufgefordert ein Zertifikat auszuwählen. Klicken Sie dazu auf die „Durchsuchen“ Schaltfläche.



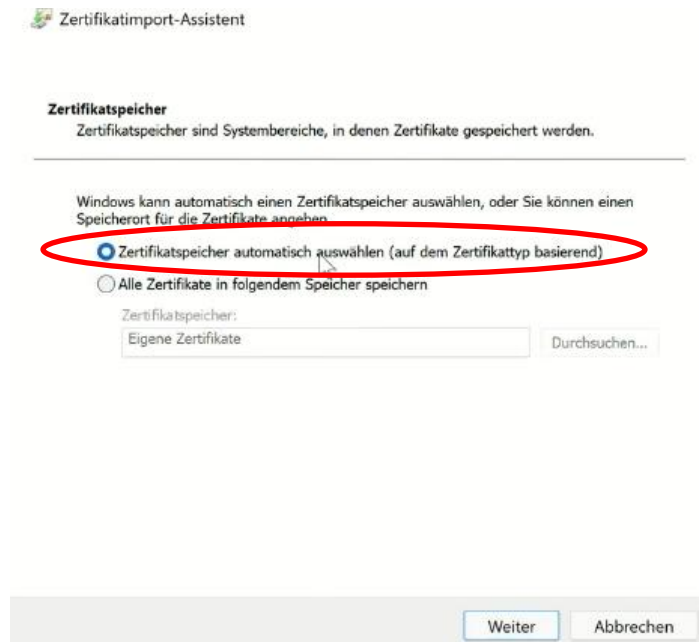
6. Wählen Sie nun die zuvor heruntergeladene Zertifikatsdatei aus. Bestätigen Sie die Auswahl über die Schaltfläche „Öffnen“ und klicken Sie dann auf „Weiter“.



7. Geben Sie das Kennwort für die Installation des Zertifikats im entsprechenden Feld ein. Klicken Sie auf „Weiter“.



8. Markieren Sie im Fenster „Zertifikatspeicher“ die Option „Zertifikatspeicher automatisch auswählen“. Bestätigen Sie mit „Weiter“.

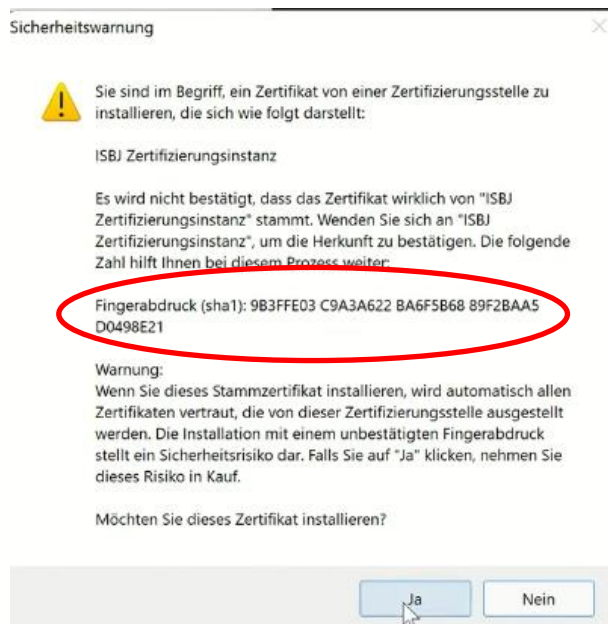


9. Klicken Sie auf „Fertig stellen“, um den Zertifikatimport abzuschließen.



Kontrolle des Fingerabdrucks:

10. Eine Sicherheitswarnung mit Informationen zur Zertifizierungsinstanz und dem Hinweis zur Kontrolle des Fingerabdrucks erscheint. Überprüfen Sie den SHA1-Fingerabdruck mit dem Fingerabdruck aus dem per Post geschickten Brief mit dem Installationskennwort für das Zertifikat.



10.1 Stimmen die Daten überein, kann das installierte Zertifikat genutzt werden. Bitte klicken Sie auf „Ja“

10.2 Stimmen die Fingerabdrücke **nicht** überein, sollte das Zertifikat nicht installiert werden. Bitte klicken Sie dazu einfach auf „Nein“.

10.2.1 Bitte melden Sie nicht übereinstimmende Fingerabdrücke sofort an:

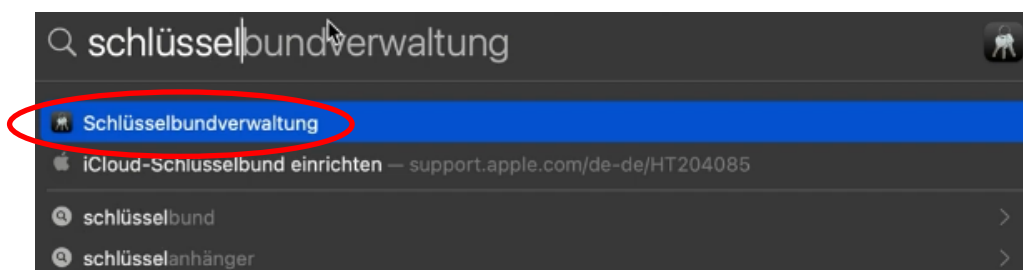
traeger-service@senbjf.berlin.de

5 Apple Safari

Das ISBJ Trägerportal unterstützt generell Safari ab der Version 5.1.10. Im Folgenden wird die Installation des Zertifikats exemplarisch anhand des Safari 16.5 dargestellt.

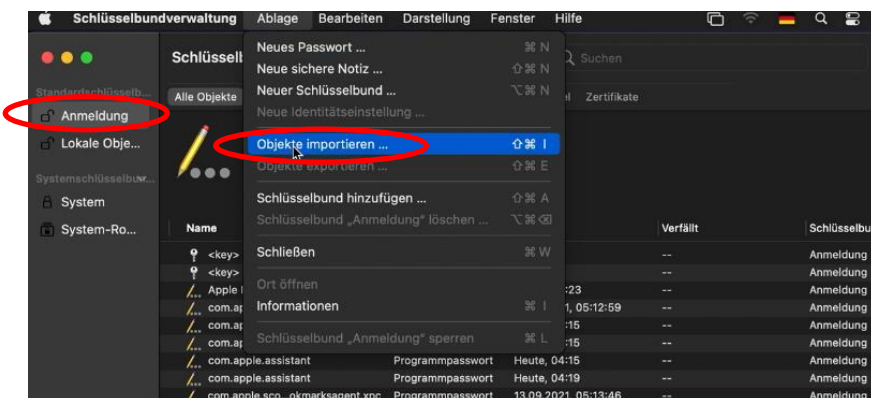
Safari verwaltet selbst keine Zertifikate, sondern greift (ab Mac OS X) auf den so genannten Schlüsselbund (Keychain) des Betriebssystems zurück. Sie Importieren Ihr Zertifikat also in den Schlüsselbund.

1. Speichern Sie die Zertifikatsdatei zunächst lokal auf Ihrem Rechner ab.
2. Öffnen Sie das Programm "Schlüsselbundverwaltung". Sie finden es z.B. per Spotlight-Suche oder im Finder unter Programme/Dienstprogramme (Shift-Command-U).

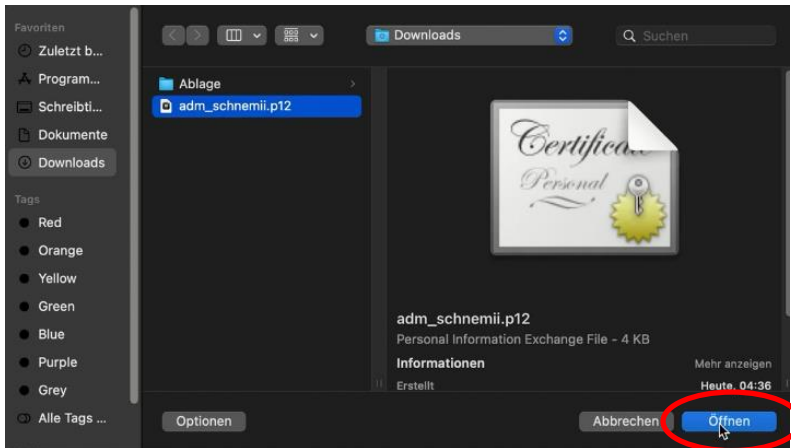


Sobald sich die Schlüsselbundverwaltung öffnet, sollten eventuell vorhandene alte Zertifikate gelöscht werden. Geben Sie dazu in die Suche der Schlüsselbundverwaltung „ISBJ“ ein und löschen Sie alle Einträge der Art „Zertifikat“ und „Identitätseinstellung“

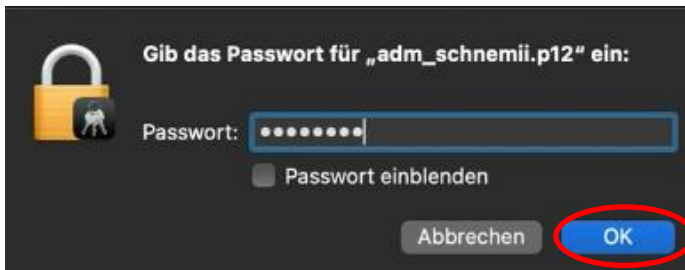
3. Um das Zertifikat zu installieren wählen Sie zunächst auf der rechten Seite den Schlüsselbund „Anmeldung“ aus und klicken Sie anschließend im Menü Ablage auf „Objekte importieren“. (Shift-Command-I)



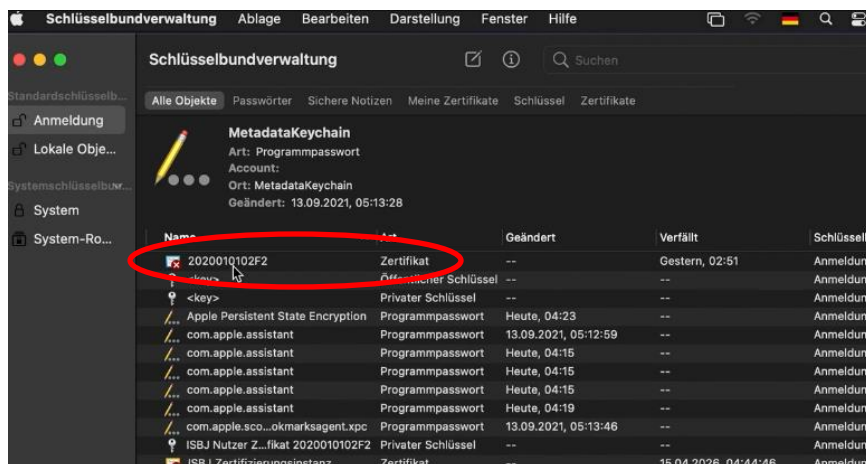
4. Wählen Sie nun die zuvor heruntergeladene Zertifikatsdatei aus und klicken Sie auf „Öffnen“



5. Geben Sie das Kennwort für die Installation des Zertifikats ein. Klicken Sie auf „OK“.

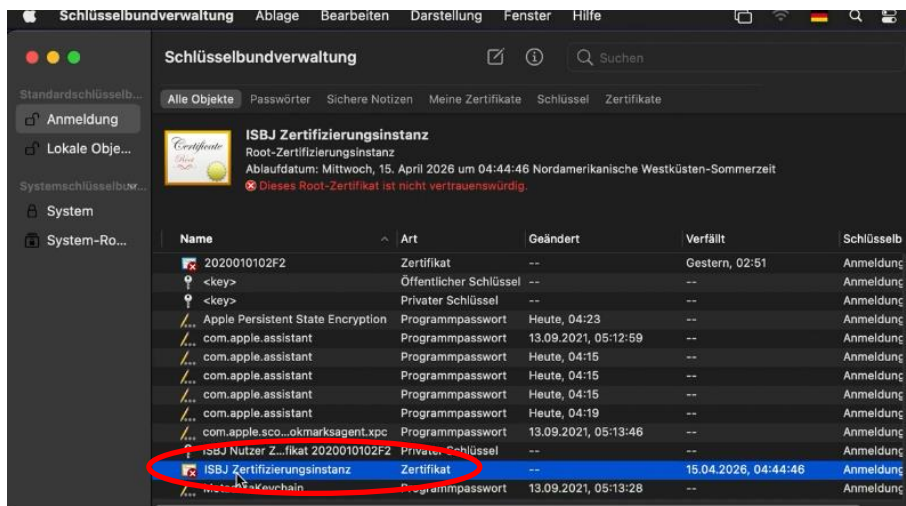


6. Nach dem Import sollte Ihr persönliches Zertifikat in der Liste der Kategorie "Meine Zertifikate" des Schlüsselbundes "Anmeldung" angezeigt werden.

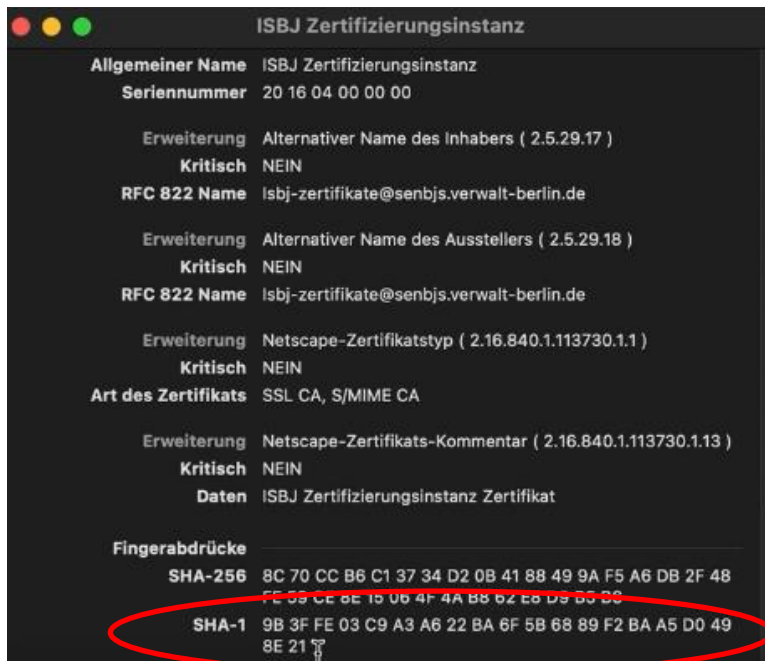


Kontrolle des Fingerabdrucks:

7. Klicken Sie nun im Schlüsselbund Anmeldung per Doppelklick auf den Eintrag „ISBJ-Zertifizierungsinstanz“.



8. Vergleichen Sie bitte in dieser Ansicht den SHA1-Fingerabdruck mit dem Fingerabdruck aus dem per Post geschickten Brief mit dem Installationskennwort für das Zertifikat.



9. Wenn die Fingerabdrücke übereinstimmen, scrollen Sie im geöffneten Fenster der Zertifizierungsinstanz nach oben und klicken auf den kleinen Pfeil neben „Vertrauen“, sodass sich das Menü ausklappt.

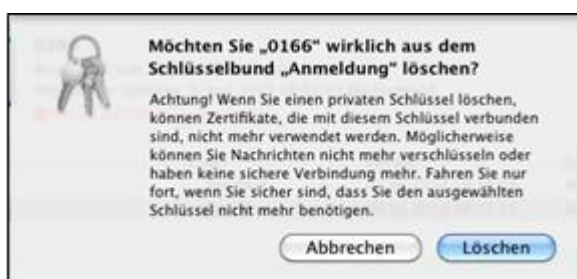


10. Wählen Sie nun unter „Bei Verwendung dieses Zertifikats“ die Option „Immer vertrauen“ aus und schließen Sie das Fenster. Das Zertifikat wurde erfolgreich installiert und Sie können die Schlüsselbundverwaltung schließen.

11. Stimmen die Fingerabdrücke nicht überein, muss das Zertifikat wieder deinstalliert werden. Klicken Sie hierzu das installierte Zertifikat an und wählen Sie über das Menü „Bearbeiten“ den Punkt „Löschen“ aus.



11.1 Bestätigen Sie den Löschvorgang mit „Löschen“. Das Zertifikat wird aus der Liste entfernt.



11.1.2 Bitte melden Sie die nicht übereinstimmenden Fingerabdrücke sofort an **traeger-service@senbjf.berlin.de**.