Zertifikat

Bundesinstitut
für Arzneimittel
und Medizinprodukte

Waisenhausgasse 36-38a
50676 Köln

Tel.: +49 228 99307-0
Fax +49 221 4724-444
www.dimdi.de

Ansprechpartner:
Helpdesk Technik
Tel: +49 228 99307-4949
helpdesk-technik@bfarm.de

Anleitung Zertifikate

Version 1.9

Inhalt

Im Geschäftsbereich des
Bundesministerium
für Gesundheit

1. Was ist ein digitales Zertifikat und wozu benötige ich es?

Ein Zertifikat ist eine Art elektronischer „Ausweis“. Verschlüsselungssysteme nutzen dieses Zertifikat zum Nachweis der Identität. Es enthält 2 Teile, ihren Private Key und den zugehörigen Public Key. Das Zertifikat wird bei Anwendungen mit hohem Schutzbedarf zur 2-Faktor-Authentifizierung (Benutzername/Passwort und Zertifikat) genutzt, um sich als berechtigter Nutzer des Single-Sign-On für PharmNet.Bund und BfArM zu authentifizieren. Nutzer, die kein Zertifikat besitzen, sich also nicht „ausweisen“ können, erhalten dabei keinen Zugriff auf Anwendungen mit hohem Schutzbedarf.

Das Zertifikat für den Zugang zu PharmNet.Bund und BfArM können Sie bei einer Zertifizierungsstelle (Certificate Authortiy – CA) oder bei einem Distributor erwerben. Es kann auch für andere Zwecke genutzt werden.

Das Zertifikat ist eine persönliche Identifikation des Benutzers, die die Funktion eines Ausweises hat. Aus den Angaben im Zertifikat sollte hervorgehen, welche Person es identifiziert.

Wir akzeptieren nur Zertifikate von CAs, die standardmäßig von der Programmiersprache Java unterstützt werden. Eine Liste mit möglichen Ausstellern finden Sie im Anhang.

2. Was benötige ich im Einzelnen?

Um ein Zertifikat zu erhalten und es für den Zugang zu PharmNet.Bund und BfArM zu nutzen, sind die folgenden drei Schritte notwendig:

- Beantragen Sie ein Zertifikat bei einer Zertifizierungsstelle oder einem Distributor. Es muss für eine TLS-WWW-Client-Authentifizierung ausgestellt und SHA-2 signiert sein.
  (Extended-Key-Usage für Client-Authentifizierung, siehe http://www.ietf.org/rfc/rfc3280.txt, Abschnitt 4.2.1.13).
- Holen Sie das für Sie ausgestellte persönliche Zertifikat ab und importieren Sie es in Ihren Browser. (Jeder Nutzer benötigt ein eigenes Zertifikat. Bitte achten Sie darauf, dass Ihr Name oder Ihre E-Mail-Adresse im Zertifikat vermerkt sind.)
- Sichern Sie Ihr Zertifikat

3. Wie erhalte ich ein Zertifikat?

Das Zertifikat beantragen Sie bei einer Zertifizierungsstelle oder einem Distributor. Angeben müssen Sie dabei üblicherweise Ihren Namen, Ihre Adresse, Ihre E-Mail-Adresse, das Land aus dem Sie kommen und eventuell einen Firmennamen oder ein Bundesland. Wie genau der Antrag erfolgt, erfahren Sie beim jeweiligen Anbieter. Den privaten Schlüssel (Private Key) sollten Sie gut aufbewahren. Zusätzlich müssen Sie sich noch identifizieren (z.B. Postident). Der Aussteller stellt Formulare für die Beantragung und Beschreibungen für das Eintragen des Zertifikats in den Browser zur Verfügung.

Die Beantragung und Abholung eines Zertifikats kann recht unterschiedlich sein. Der übliche Weg ist, die Webseite des Anbieters zu besuchen und dort Ihre Daten einzugeben. Dabei erstellt der Browser auf Ihrem Computer den Private Key und den Public Key.

Der Public Key wird an den Anbieter gesendet und dort signiert, während der Private Key in ihrem Browser verbleibt. In den meisten Fällen werden Sie anschließend per E-Mail aufgefordert, die Webseite erneut mit dem gleichen Browser zu besuchen. Dabei wird der signierte Public Key mit dem Private Key zusammengeführt und letztendlich das Zertifikat erstellt. Zugleich wird das Zertifikat auch in Ihrem Browser installiert. In diesem Fall sollten Sie Ihr Zertifikat im Anschluss unbedingt sichern.

Eine weitere Variante wird in Abschnitt 4 beschrieben. Dabei erhalten Sie das fertige Zertifikat entweder vom Aussteller oder von einem Kollegen Ihrer IT, der es für Sie beantragt hat.

4. Wie importiere ich mein persönliches Zertifikat?

Wenn Sie Ihr Zertifikat erhalten haben, muss es in den Browser importiert werden, bevor Sie es verwenden können. Durch den Import wird das Zertifikat im richtigen Zertifikatsspeicher platziert.

Im Folgenden wird das Importieren beispielhaft zuerst für den Browser Mozilla Firefox, dann für den Internet Explorer und abschließend für Google Chrome durchgeführt:

4.1. Mozilla Firefox

Wählen Sie zuerst im Menü am rechten oberen Bildrand den Punkt „Einstellungen“ aus.

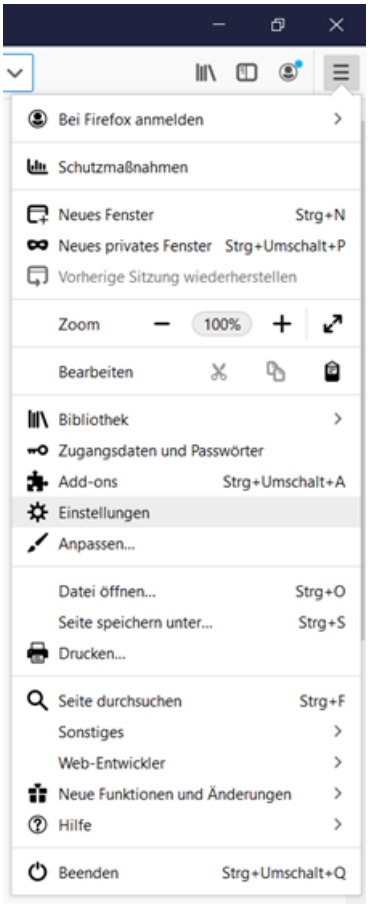

Abbildung 1: Einstellungen Erweitert

Wählen Sie nun „Datenschutz & Sicherheit“ aus und scrollen Sie hinunter bis der Menüpunkt „Zertifikate“ erscheint.

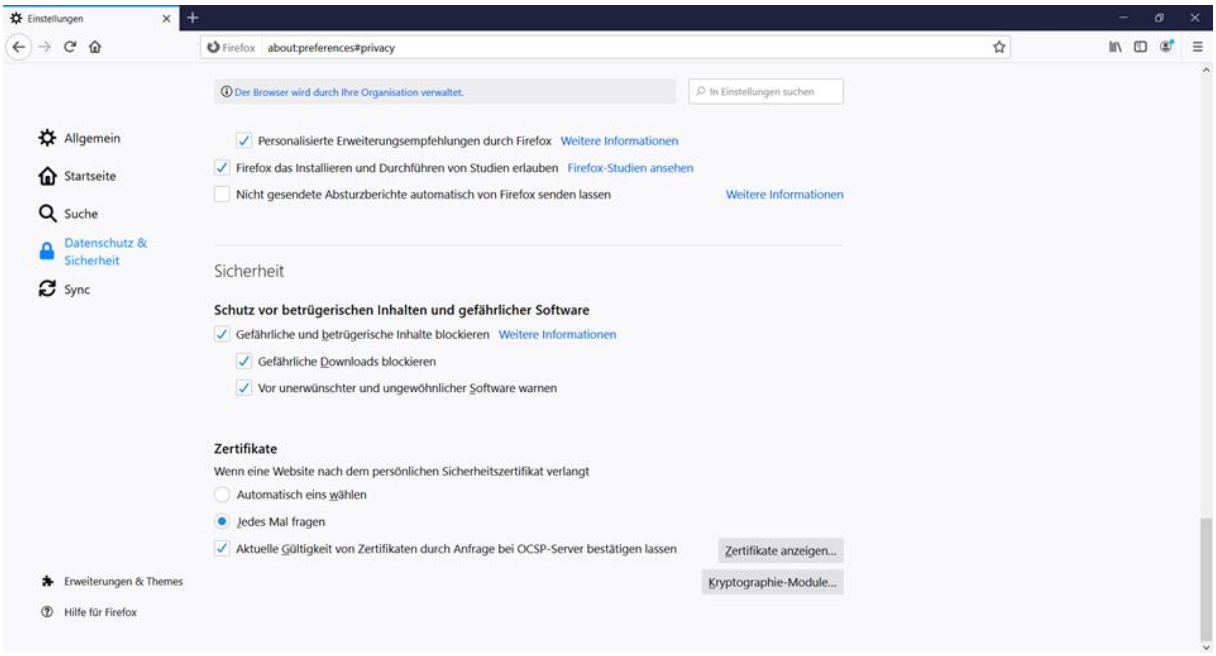

Abbildung 2: Übersicht Zertifikate

Wählen Sie „Zertifikate anzeigen“: Es öffnet sich ein weiteres Fenster, in dem Sie den Reiter „Ihre Zertifikate“ wählen. Sie sehen nun eine Übersicht der bereits installierten Zertifikate (im Beispiel sind keine Zertifikate vorhanden).

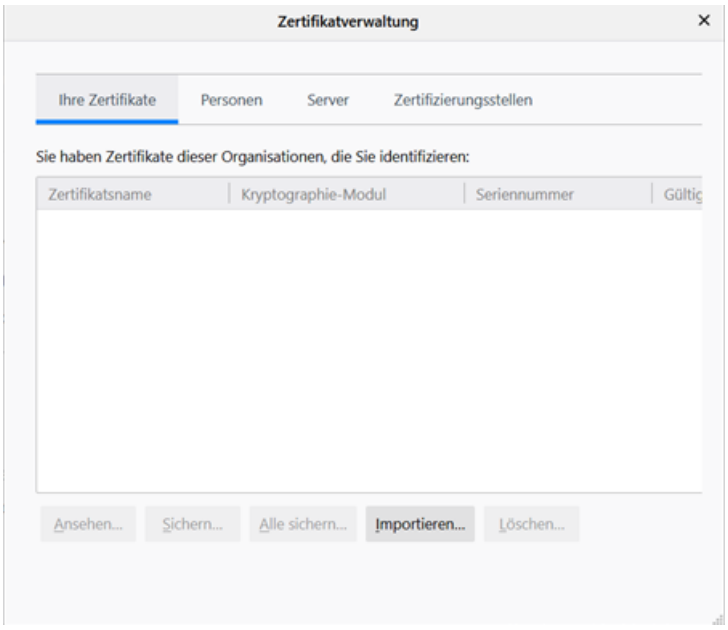

Abbildung 3: Zertifikatverwaltung

Nach Klick auf „Importieren“ erscheint eine Datenauswahlbox.

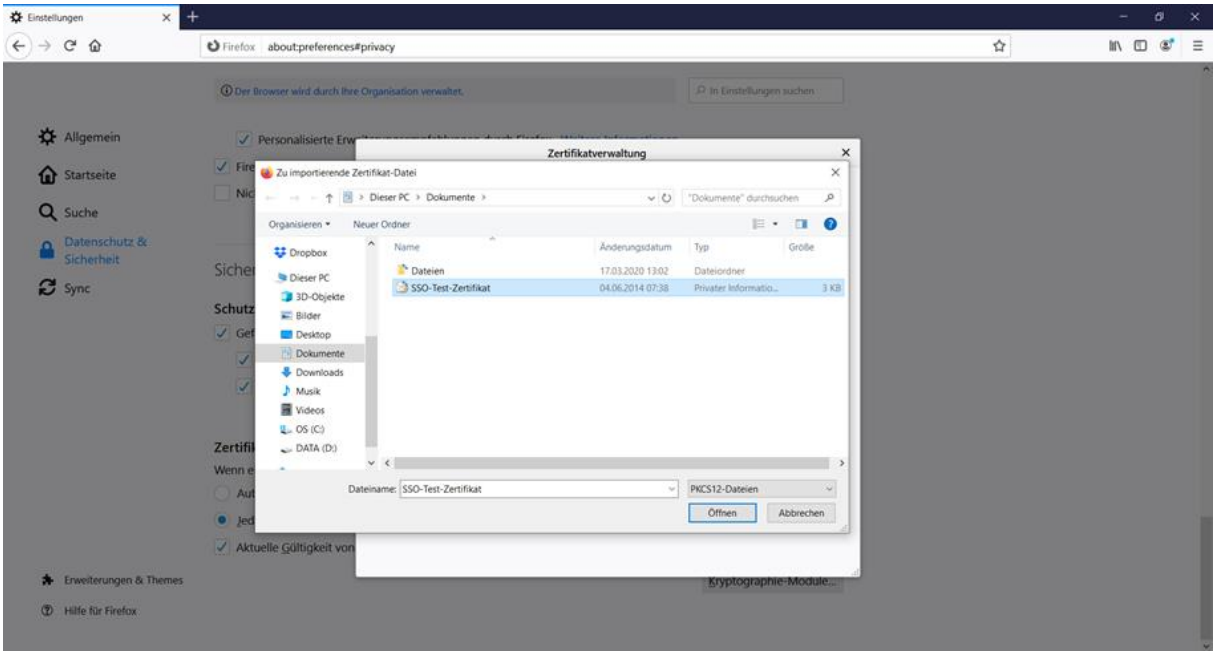

Abbildung 4: Importieren des Zertifikats

Wählen Sie Ihr Zertifikat aus und klicken Sie auf „Öffnen“. Sie werden nun aufgefordert, das Passwort für die Schlüsseldatei einzugeben.

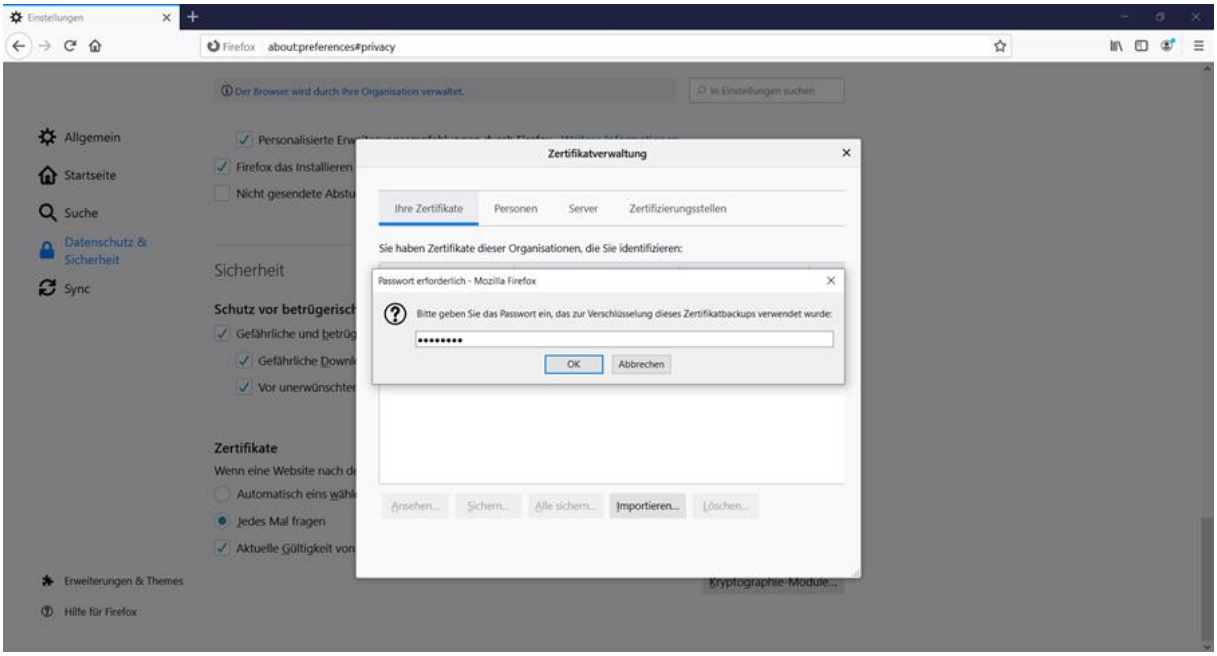

Abbildung 5: Passwort des Zertifikats

Nach erfolgreichem Import des Zertifikats ist es unter „Ihre Zertifikate“ eingetragen.

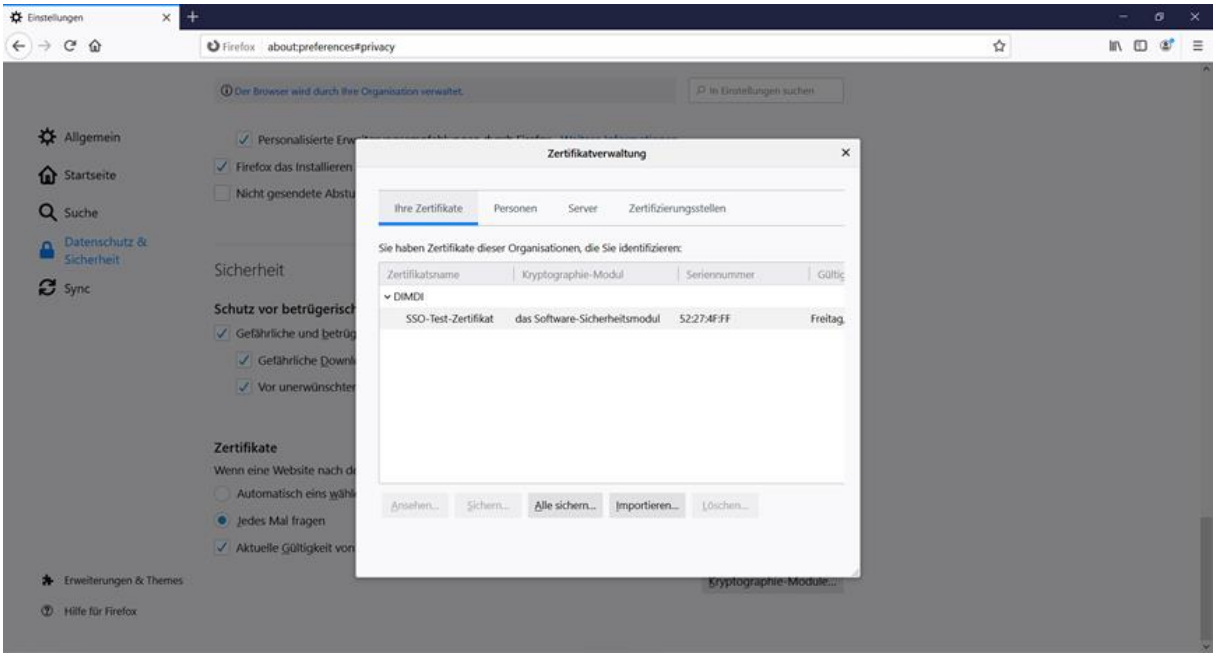

Abbildung 6: Übersicht mit hochgeladenem Zertifikat

4.2. Internet Explorer

Hier wählen Sie im Menü „Extras“ den Punkt „Internetoptionen“.

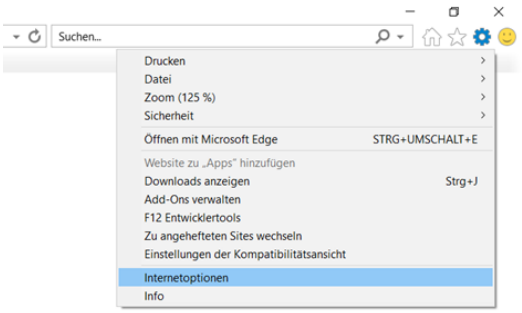

Abbildung 7: Öffnen der Internetoptionen

Dann wählen Sie den Reiter Inhalte aus und klicken auf den Knopf „Zertifikate“.

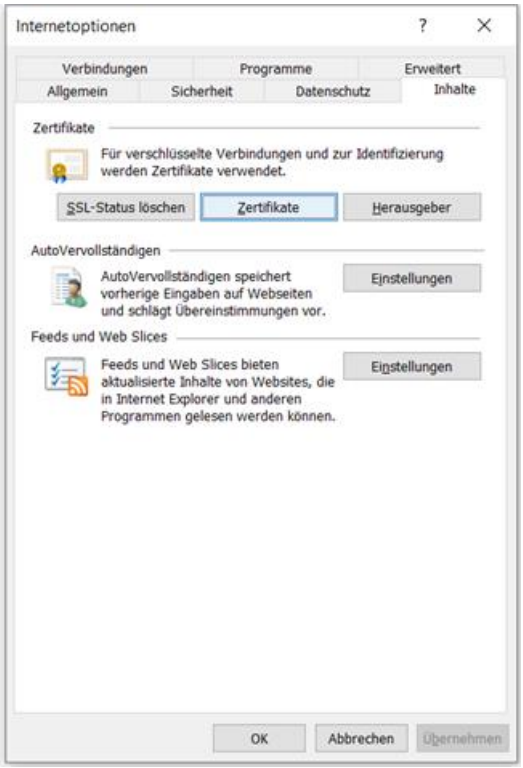

Abbildung 8: Aufruf Zertifikate

Sie sehen unter „Eigene Zertifikate“ eine Übersicht der bereits installierten Zertifikate. Nach Klick auf „Importieren“ erscheint der Zertifikatsimport-Assistent. Bei der ersten Ansicht klicken Sie auf „Weiter“. In der folgenden Ansicht wählen Sie das Zertifikat aus, bestätigen mit „Weiter“ und geben Ihr Passwort ein.

Nun erscheint die Auswahl des Zertifikatspeichers. Die Einstellungen sollten den unten angezeigten Einstellungen entsprechen.

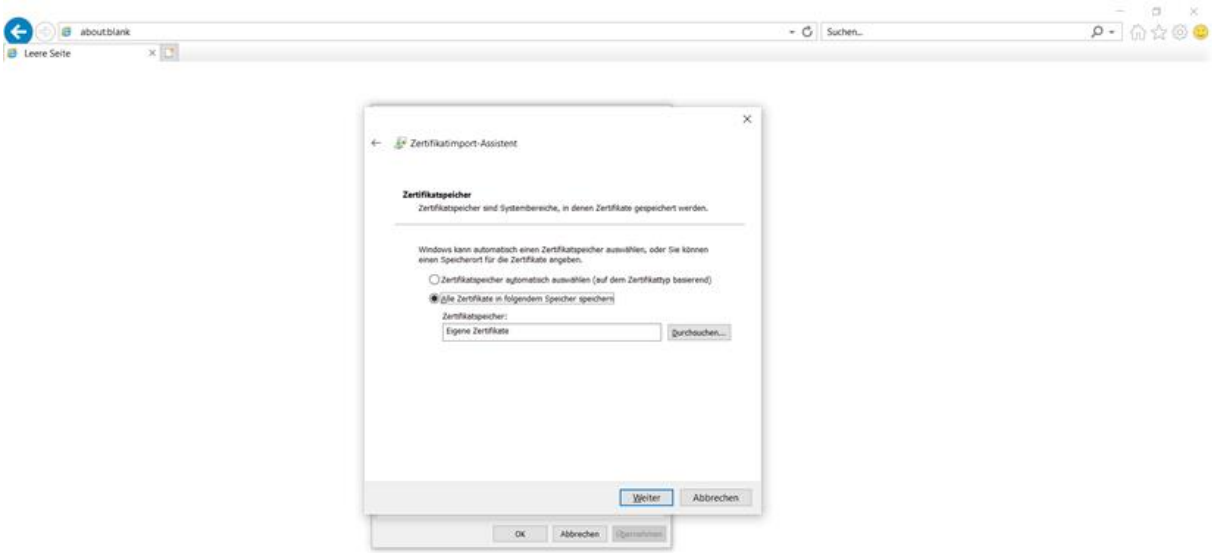

Abbildung 9: Auswahl des Zertifikatspeichers

Klicken Sie nun auf „Weiter“ und bestätigen Sie die folgende Ansicht mit „Fertig stellen“.

Ihr Zertifikat sollte nun unter der Ansicht „Eigene Zertifikate“ angezeigt werden.

4.3. Google Chrome

Wählen Sie unter „Google Chrome anpassen und einstellen“ den Punkt „Einstellungen“ aus.

Abbildung 10: Einstellungen öffnen

Wählen Sie nun „Datenschutz und Sicherheit“ aus und klicken Sie auf „Mehr“.

Es öffnen sich nun weitere Auswahlmöglichkeiten. Hier klicken Sie bitte auf den untersten Punkt „Zertifikate verwalten“.

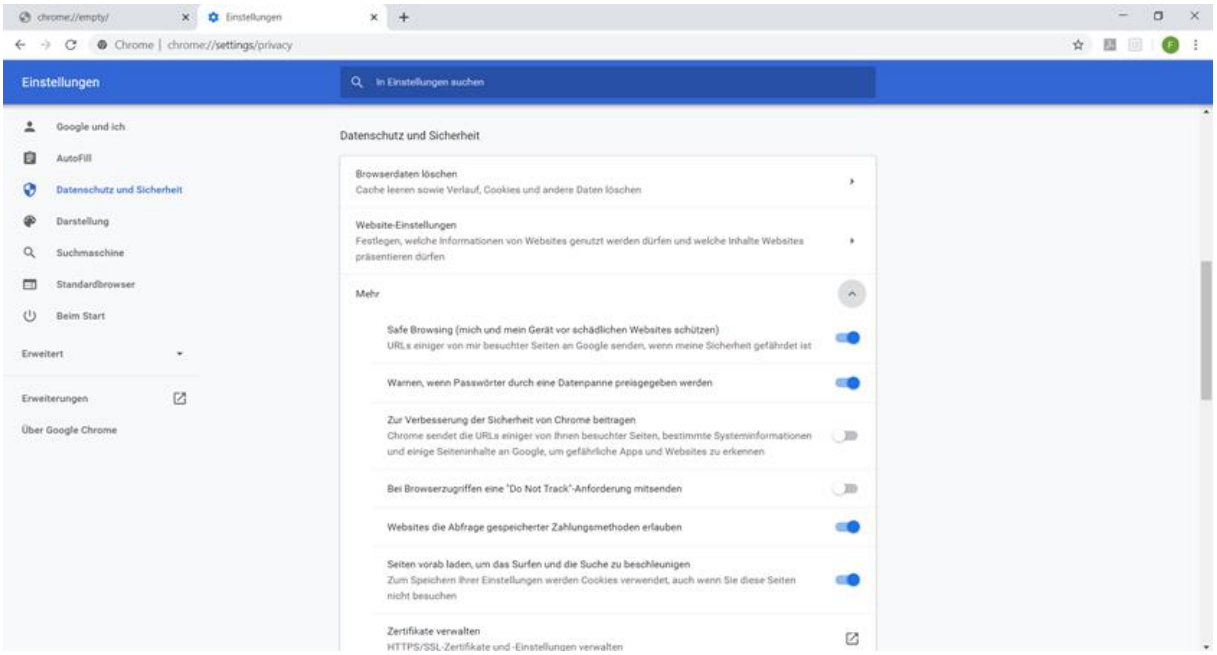

Abbildung 11: Zertifikate verwalten auswählen

Sie sehen unter „Eigene Zertifikate“ eine Übersicht der bereits installierten Zertifikate. Nach Klick auf „Importieren“ erscheint der Zertifikatsimport-Assistent. Bei der ersten Ansicht klicken Sie auf „Weiter“. In der folgenden Ansicht wählen Sie das Zertifikat aus, bestätigen mit „Weiter“ und geben Ihr Passwort ein.

Nun erscheint die Auswahl des Zertifikatspeichers. Die Einstellungen sollten den unten angezeigten Einstellungen entsprechen.

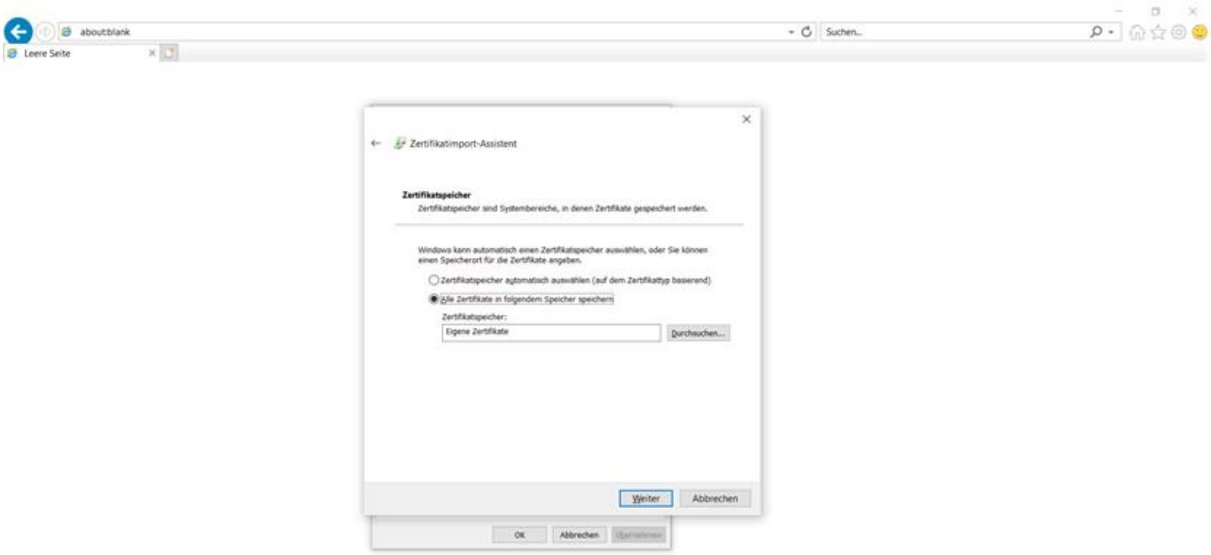

Abbildung 12: Auswahl des Zertifikatspeichers

Klicken Sie nun auf „Weiter“ und bestätigen Sie die folgende Ansicht mit „Fertig stellen“.

Ihr Zertifikat sollte nun unter der Ansicht „Eigene Zertifikate“ angezeigt werden.

5. Exportieren des öffentlichen Teils des Zertifikates

5.1. Mozilla Firefox (Version 70.X oder aktueller)

Um den öffentlichen Teil des Zertifikates für die Registrierung beim BfArM hochzuladen, extrahieren Sie diesen Teil Ihres Zertifikats. Hierzu öffnen Sie, wie in Abschnitt 4 beschrieben, den Zertifikat-manager, markieren unter „Meine Zertifikate“ das gewünschte Zertifikat und klicken dann auf „Ansehen…“.

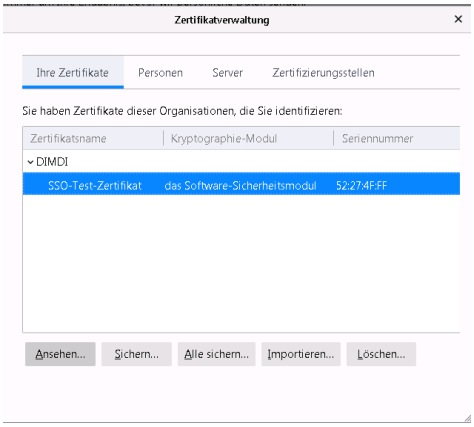

Abbildung 13: Exportieren des Zertifikats

Scrollen Sie dann hinunter bis Sie „Speichern“ sehen und klicken Sie auf „PEM (Zertifikat)“.

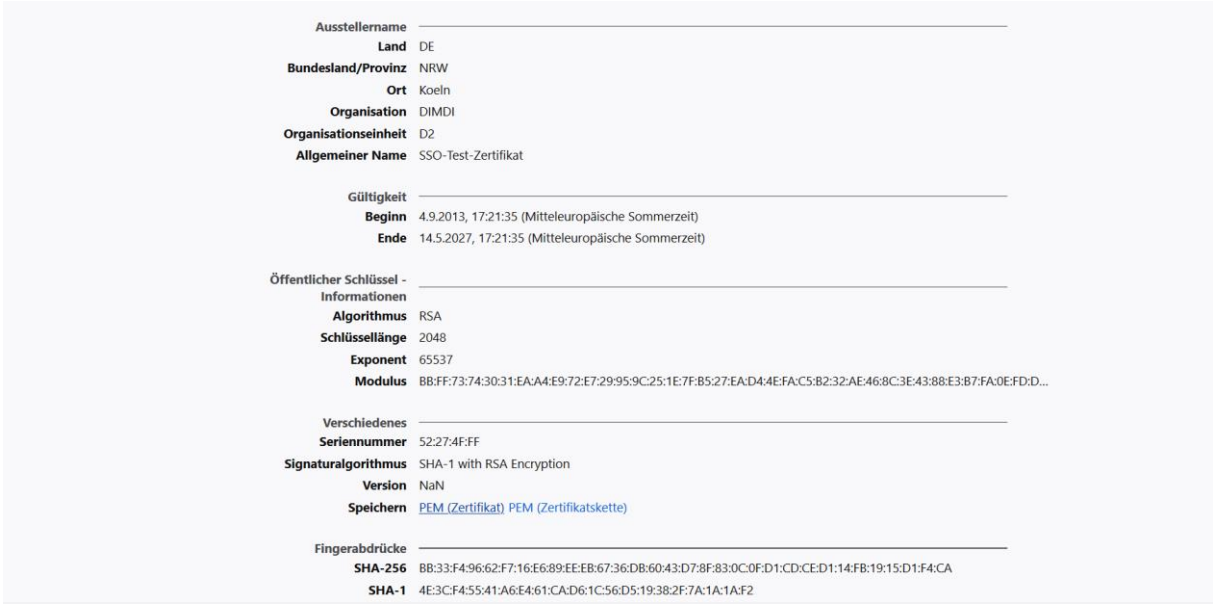

Abbildung 14: Extrahieren des öffentlichen Teils

Speichern Sie das Zertifikat lokal und sehen in Ihrem Download Ordner (falls nicht anders angegeben) nach, ob das Zertifikat heruntergeladen wurde.

5.2. Mozilla Firefox (Version 69.X oder älter)

Um den öffentlichen Teil des Zertifikates für die Registrierung beim BfArM hochzuladen, extrahieren Sie diesen Teil Ihres Zertifikats. Hierzu öffnen Sie, wie unter Abschnitt 4 beschrieben, den Zertifikat-manager, markieren unter „Meine Zertifikate“ das gewünschte Zertifikat und klicken dann auf „Ansehen…“.

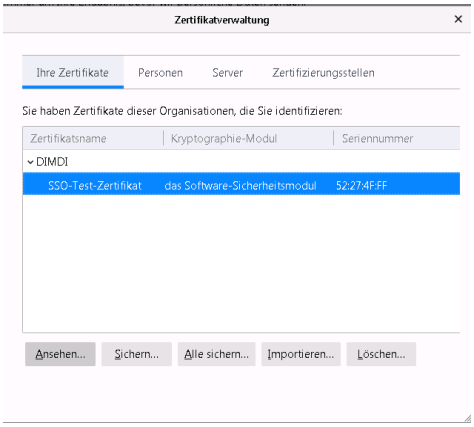

Abbildung 15: Exportieren des Zertifikats

Danach wählen Sie den Reiter „Details“.

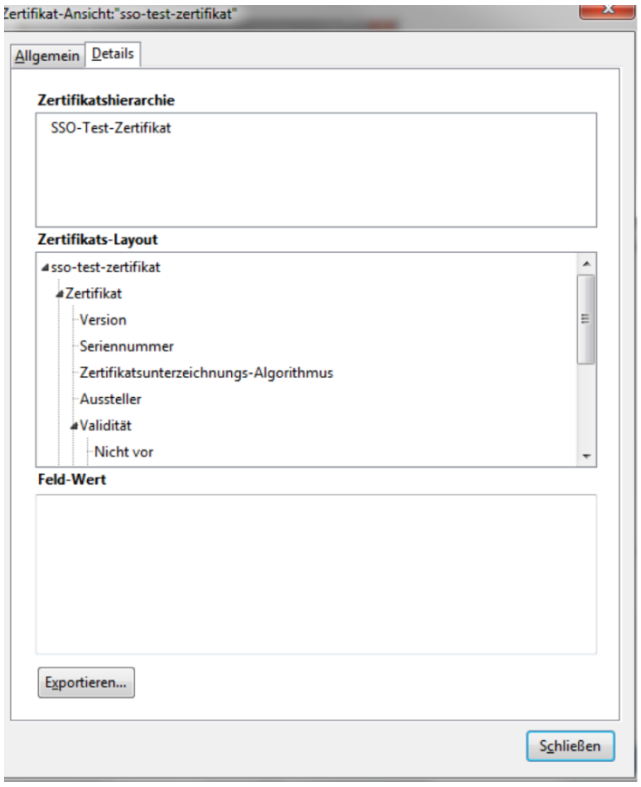

Abbildung 16: Zertifikate Ansicht

Nun klicken Sie auf „Exportieren“ und erhalten eine Datei mit dem öffentlichen Teil Ihrer Signatur (mit der Endung .cer, .crt oder .der). Diese Datei speichern Sie lokal auf Ihrem Rechner.

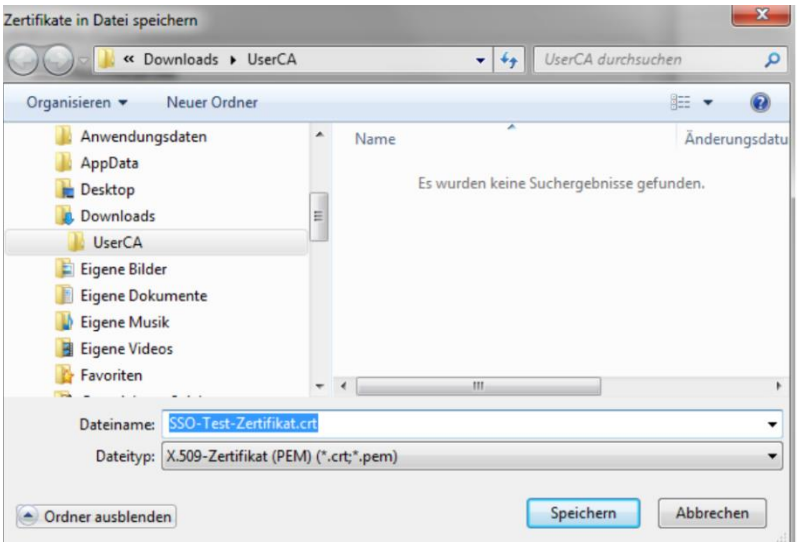

Abbildung 17: Sicherung des Zertifikats

5.3. Internet Explorer und Google Chrome

Um den öffentlichen Teil des Zertifikates für die Registrierung beim BfArM hochzuladen, extrahieren Sie diesen Teil Ihres Zertifikats. Hierzu öffnen Sie, wie unter Punkt 4. beschrieben, den Zertifikatmanager, markieren unter „Meine Zertifikate“ das gewünschte Zertifikat und klicken dann auf „Exportieren…“.

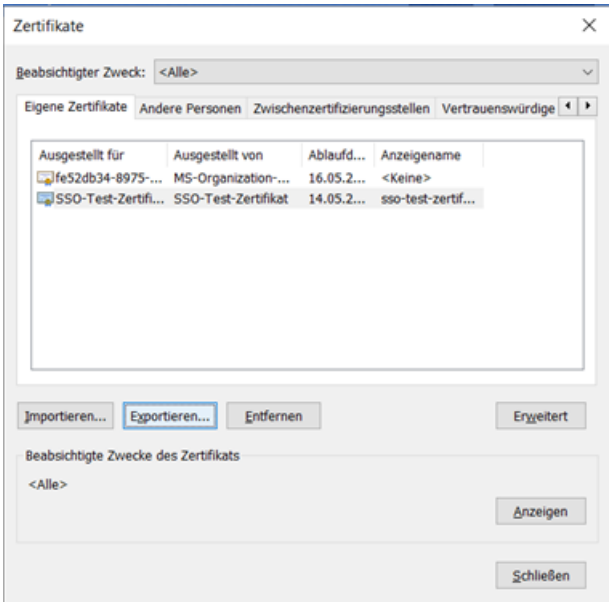

Abbildung 18: Exportieren des Zertifikats

Nun klicken Sie auf „Weiter“ und klicken im nächsten Fenster den Button „Nein, privaten Schlüssel nicht exportieren“ und bestätigen mit „Weiter“.

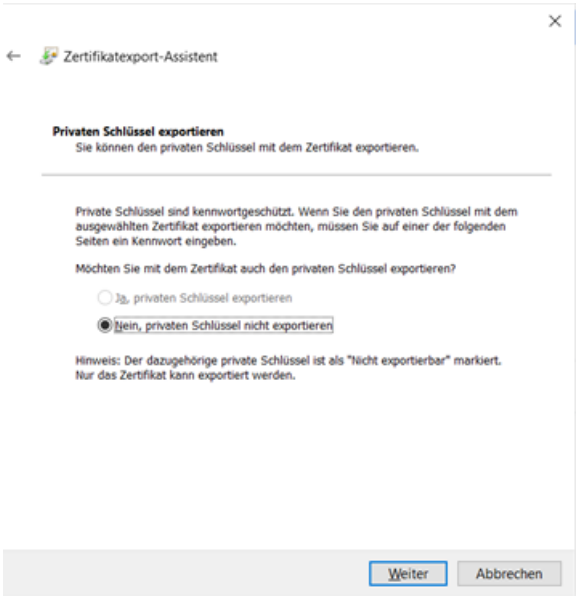

Abbildung 19: Sicherung des Zertifikats

Klicken Sie auf „DER-codiert-binär X.509 (.CER)“ und bestätigen mit „Weiter“.

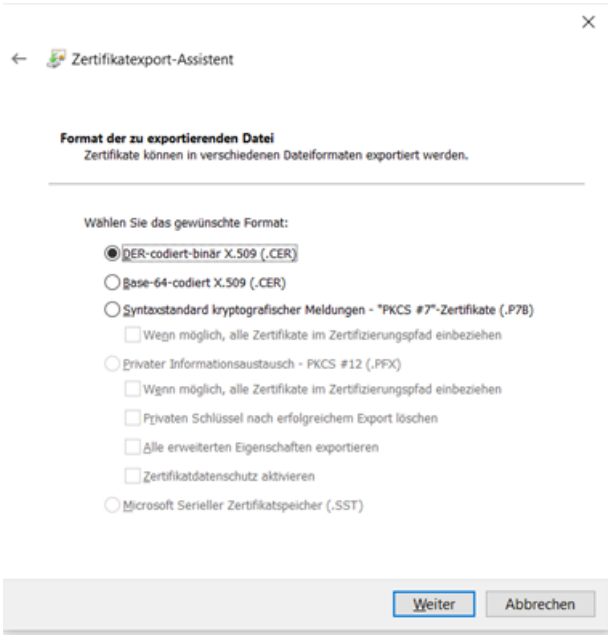

Abbildung 20: Einstellen des Formats

Klicken Sie im folgenden Fenster auf „Durchsuchen“ und wählen Sie das Verzeichnis aus, in welchem Sie die neue Datei abspeichern möchten. Geben Sie der Datei einen Namen und bestätigen Sie mit „Speichern“ und anschließend mit „Weiter“.

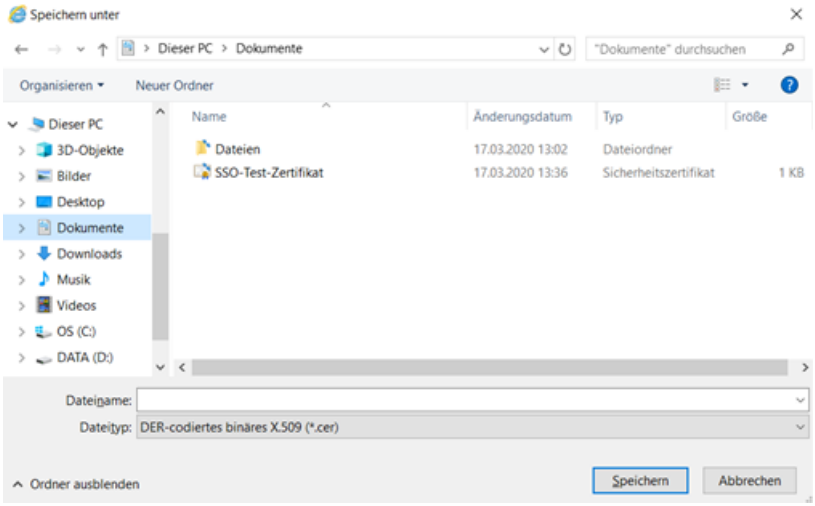

Abbildung 21: Speichern des öffentlichen Teils

Klicken Sie auf „Fertig stellen“ und suchen Sie in dem gewählten Verzeichnis nach der neu erstellten Datei.

6. Zertifikat hochladen

Bei der Erstregistrierung können Sie im Abschnitt „Zertifikat“ ein persönliches Zertifikat hochladen und speichern. Auf dem Formular gibt es einen allgemeinen Hinweis oder den Hinweis, dass für die von Ihnen gewählte Anwendung ein Zertifikat erforderlich ist.

Das Zertifikat kann nach der Registrierung auch nachträglich, im Bereich „meine Daten“, hochgeladen werden. Melden Sie sich dazu über „Meine Daten“ bei unserer Benutzerverwaltung an und wählen Sie die Option „Zertifikat“ aus dem Navigationsmenü.

Auf dem Formular wählen Sie über den Button „Durchsuchen“ die vorher gespeicherte Zertifikat-Datei (s. Abschnitt 5) aus und laden sie danach hoch.

Abbildung 22: Zertifikat hochladen - 1

Abbildung 23: Zertifikat hochladen - 2

Das Zertifikat kann auch später noch im Bereich „Meine Daten“ hochgeladen oder ausgetauscht werden (s. Abschnitt 7).

7. Erneuerung eines Zertifikats

Bevor Ihr Zertifikat abläuft erhalten Sie von uns eine Benachrichtigung per Mail. Beantragen Sie rechtzeitig eine Zertifikatverlängerung bei Ihrem Aussteller und laden Sie das neue Zertifikat wie unter Abschnitt 4 und 5 beschrieben in Ihren Browser.

Sie können ein neues Zertifikat auch noch nach Ablauf eines vorherigen Zertifikats hochladen, da der Bereich „Meine Daten“ ohne Zertifikat zugänglich ist.

Melden Sie sich über „Meine Daten“ bei unserer Benutzerverwaltung an und wählen Sie die Option „Zertifikat“ aus dem Navigationsmenü.

Auf dem Formular wählen Sie über den Button „Durchsuchen“ zunächst die Zertifikat-Datei (öffentlicher Teil) aus. Im zweiten Schritt laden Sie diese Datei über den entsprechenden Button hoch.

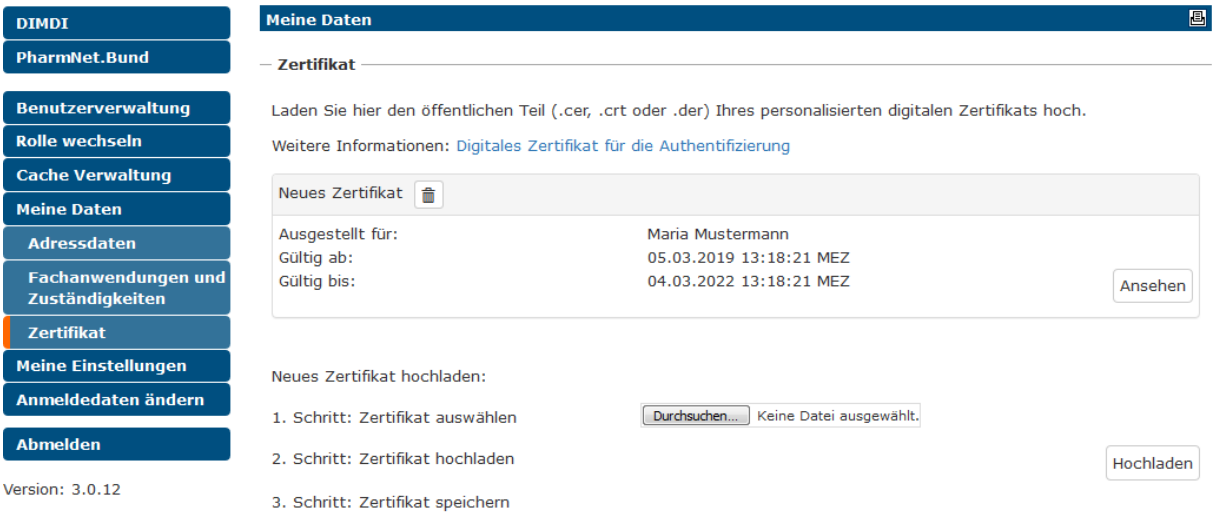

Abbildung 24: Erneuerung des Zertifikats - Schritt 2 Hochladen

Anschließend speichern Sie die Datei über den Speichern-Button.

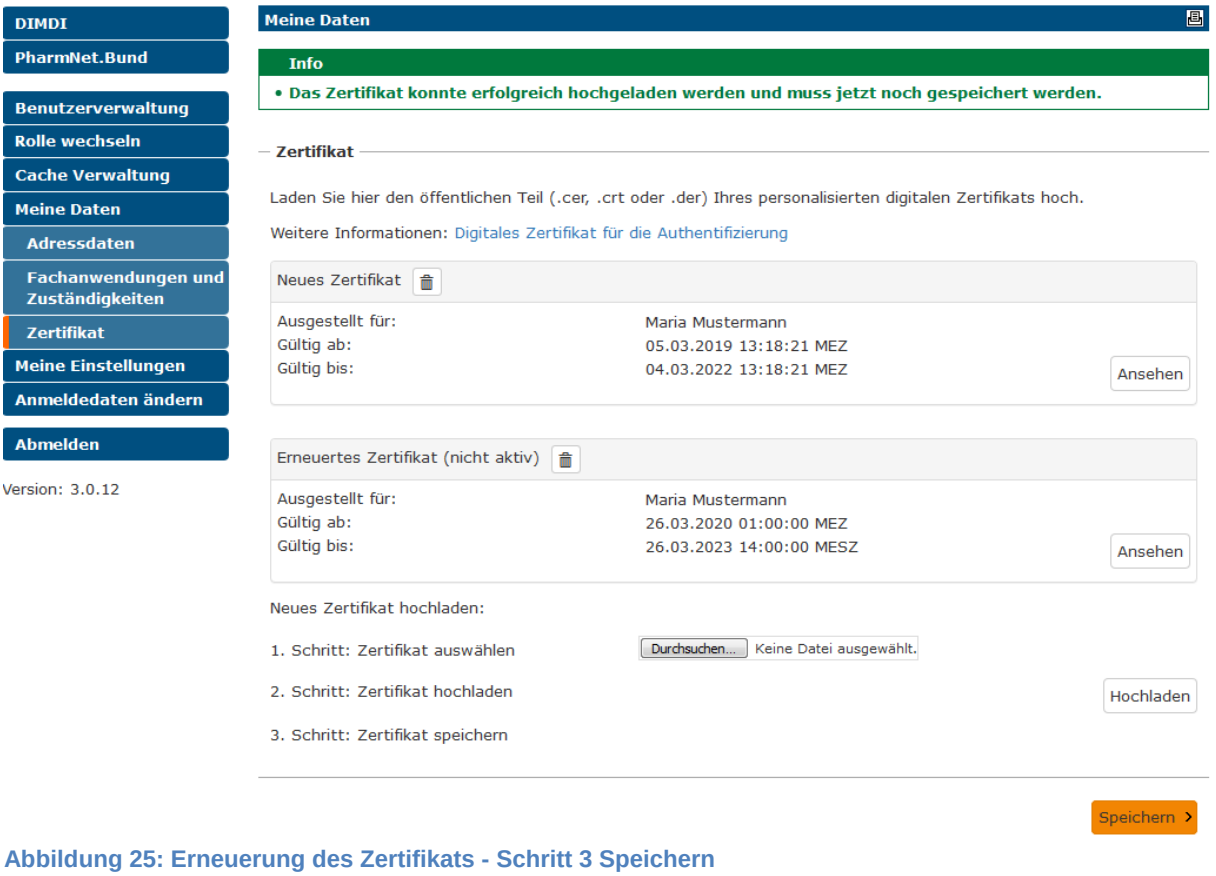

Abbildung 25: Erneuerung des Zertifikats - Schritt 3 Speichern

Nach dem Speichern wird geprüft, ob für den Nutzer bereits ein gültiges Zertifikat vorhanden ist. Ist dies der Fall, muss zunächst eine Bestätigung erfolgen, dass das bestehende Zertifikat überschrieben werden soll.

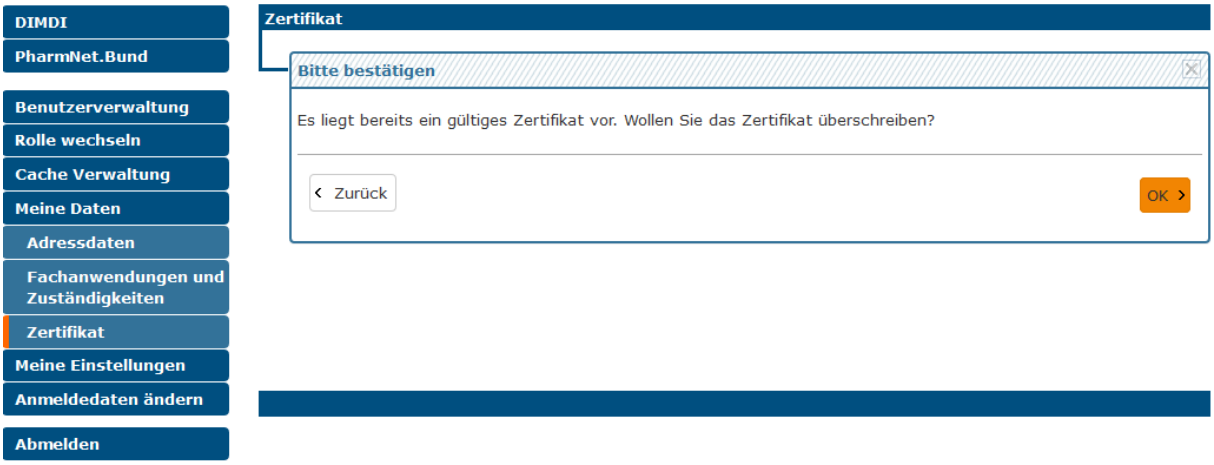

Abbildung 26: Erneuerung des Zertifikats - Schritt 4 Bestätigen

Nach Klicken auf "OK" muss das Zertifikat vom zuständigen Administrator aktiviert werden. Dieser muss die Identität des Zertifikatinhabers prüfen. Der Administrator erhält zu diesem Zweck eine entsprechende Benachrichtigung.

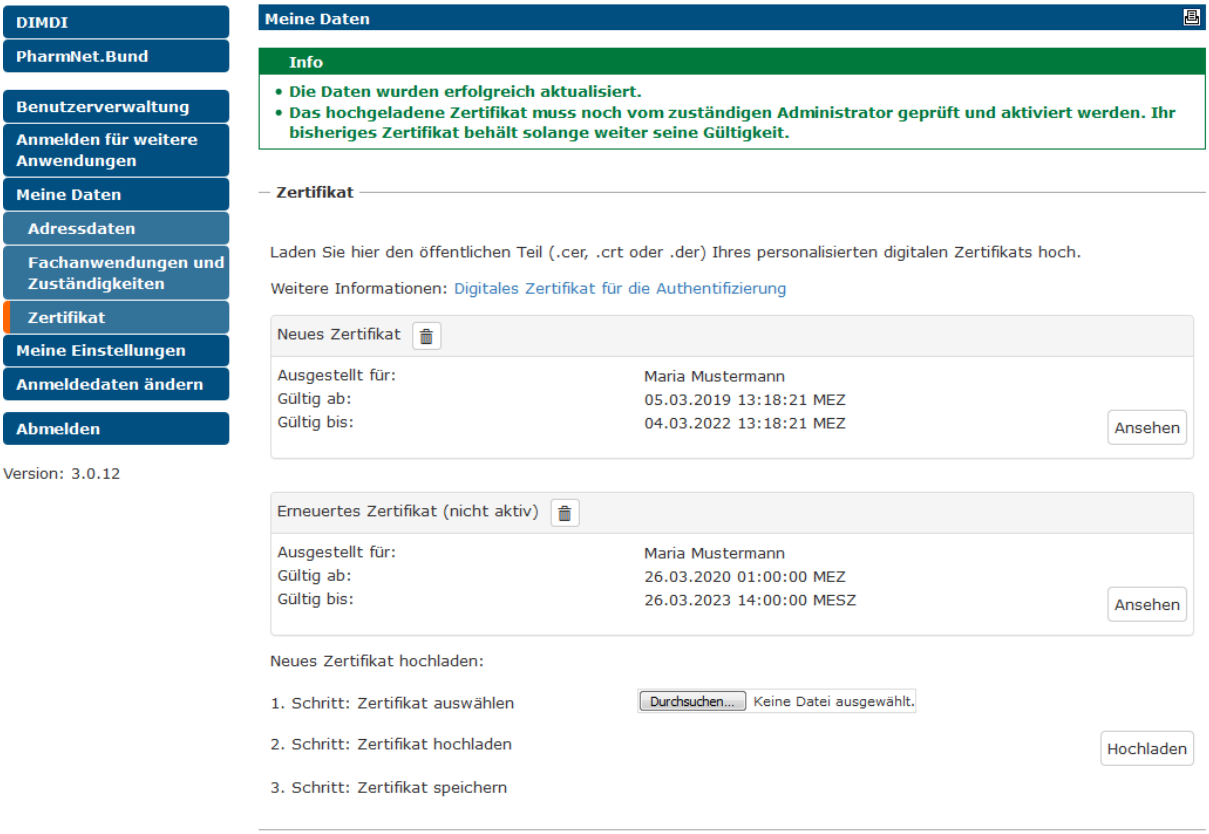

Abbildung 27: Erneuerung des Zertifikats - Schritt 5 Überprüfung

8. Anhang: Liste von Ausstellern der Zertifikate

Im Folgenden sind einige Zertifizierungsstellen aufgelistet, die digitale X.509-User-Zertifikate ausstellen. Wir akzeptieren nur Zertifikate von CAs, die standardmäßig von der Programmiersprache Java unterstützt werden (Stand März 2020). Die Reihenfolge der aufgeführten Liste ist keinesfalls als Verweis oder Empfehlung zum Kauf der Produkte eines bestimmten Unternehmens zu verstehen.

GlobalSign nv-sa, BE
SwissSign AG, CH
DigiCert Inc, US
COMODO CA Limited, GB
AC Camerfirma SA CIF A82743287, EU
Buypass AS-983163327, NO
QuoVadis Limited, BM
Starfield Technologies, Inc., US
Thawte, ZA
thawte, Inc., US
T-Systems Enterprise Services GmbH, DE
VeriSign, Inc., US
The USERTRUST Network, US
GeoTrust Inc., US
AffirmTrust, US
AddTrust AB, SE
Actalis S.p.A./03358520967, IT
CyberTrust Root, Baltimore, IE
Entrust, Inc., US
SECOM Trust.net, JP
SECOM Trust Systems CO.,LTD., JP
Internet Security Research Group, US
IdenTrust, US
GoDaddy.com, Inc., US
The Go Daddy Group, Inc., US
Sonera, FI
Thawte Consulting cc, ZA
XRamp Security Services Inc, US
SecureTrust Corporation, US"
LuxTrust s.a., LU
KEYNECTIS, FR
AC Camerfirma S.A., EU
Unizeto Sp. z o.o., PL
Unizeto Technologies S.A., PL
Chunghwa Telecom Co., Ltd., TW

Hinweis: Nicht alle Anbieter stellen X.509-Zertifikate mit der Erweiterung „Extended Key Usage: Client Authentication" aus.

Datenschutzrechtliche Hinweise zur Verarbeitung Ihrer personenbezogenen Daten und zu Ihren Rechten finden Sie unter: www.dimdi.de – Datenschutzerklärung