

INSTALLATION VON ZERTIFIKATEN

DATUM:

09.02.2021



Inhaltsverzeichnis

Einleitung	3
Mozilla Firefox	4
Microsoft Edge	8
Microsoft Internet Explorer	14
Google Chrome	20

Einleitung

Dieses Dokument beschreibt die Installation eines Zertifikats zur Nutzung der Vertrauensstelle nach §299 SGB V.

Im Folgenden wird die Installation für die Browser Mozilla Firefox, Microsoft Edge, Microsoft Internet Explorer und Google Chrome beschrieben.

Treten bei der Installation Fragen auf oder wünschen Sie eine Anleitung für weitere Browser, wenden Sie sich bitte an den Helpdesk. Die aktuellen Kontaktinformationen für den Helpdesk finden Sie unter: <http://www.vertrauensstelle-gba.de/kontakt.html>.

Ein wichtiger Hinweis:

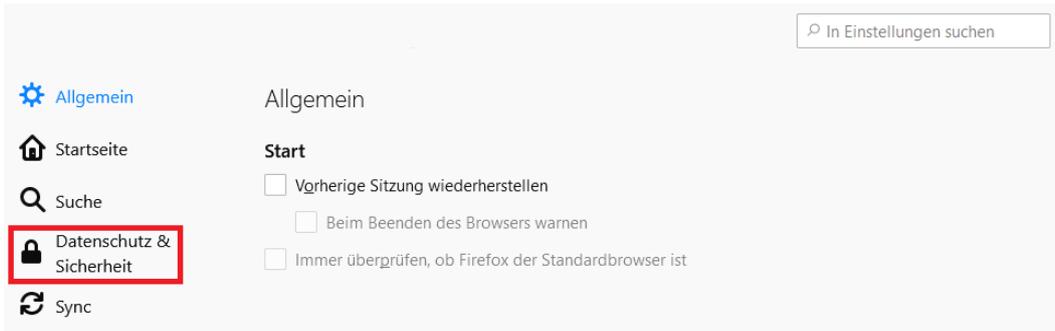
Sie sind für die Sicherheit der Zertifikate und der Ihnen mitgeteilten Kennwörter bzw. Zugangsdaten verantwortlich!

Haben Sie den Verdacht, dass Dritte Zugriff zu Ihrem Zertifikat bzw. zu den Kennwörtern erhalten haben, sind Sie verpflichtet, dies dem Helpdesk unverzüglich mitzuteilen.

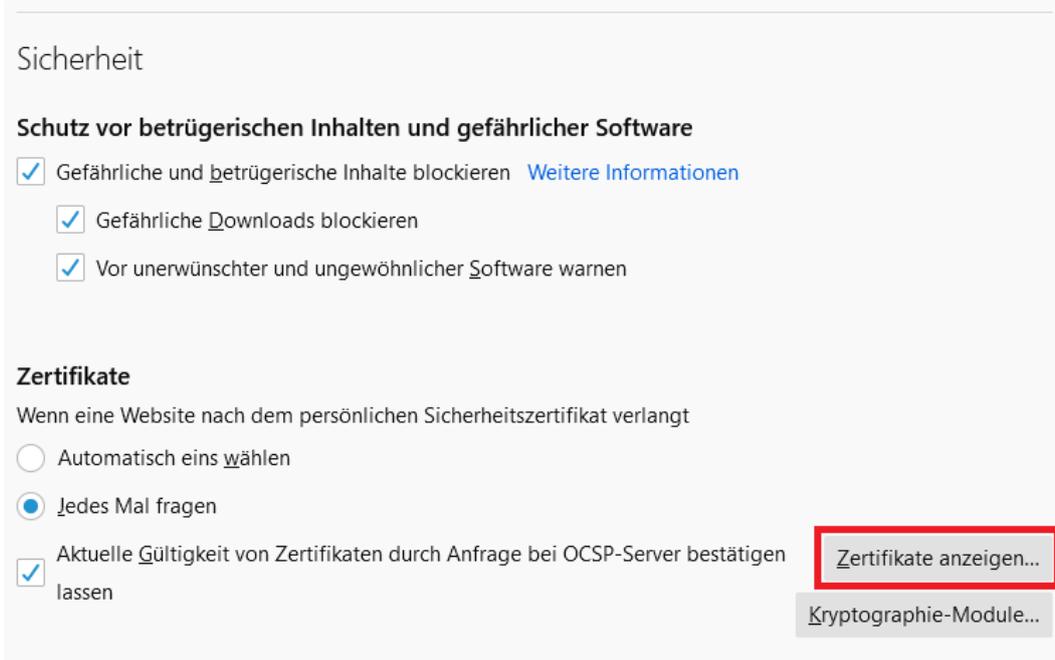
Mozilla Firefox

Speichern Sie zunächst die Ihnen gelieferte p12-Zertifikatsdatei lokal auf Ihrem Rechner.

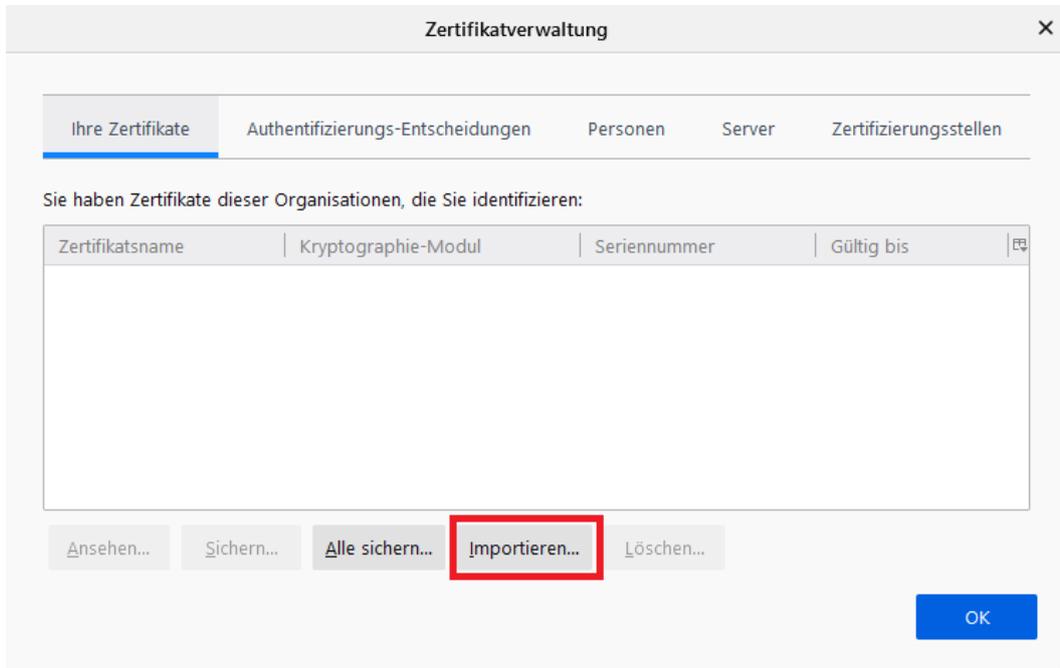
Starten Sie den Mozilla Firefox und wählen Sie oben rechts die drei Balken *Menü öffnen* und den Punkt *Einstellungen* aus. Klicken Sie dort links auf den Navigationspunkt *Datenschutz & Sicherheit*.



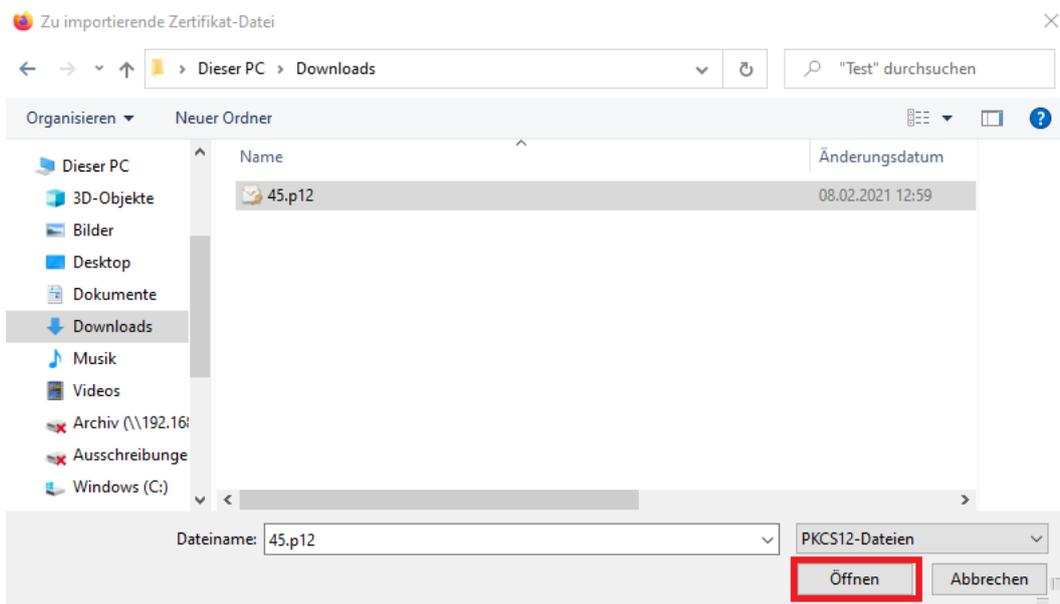
Unter dem Titel *Sicherheit* finden Sie den Unterpunkt *Zertifikate*. Dort wählen Sie die Schaltfläche *Zertifikate anzeigen*.



Es öffnet sich das Fenster für die Zertifikatsverwaltung. Über die Schaltfläche *Importieren* öffnet sich das Fenster *Zu importierende Zertifikat-Datei*.



Dort wählen Sie die entsprechende Datei aus und bestätigen über die Schaltfläche *Öffnen*.



Geben Sie das achtstellige Kennwort für die Zertifikatsinstallation ein und bestätigen Sie anschließend mit *OK*.

Passwort erforderlich - Mozilla Firefox ✕

 Bitte geben Sie das Passwort ein, das zur Verschlüsselung dieses Zertifikatbackups verwendet wurde:

Nun wird das importierte Zertifikat in der *Zertifikatsverwaltung* angezeigt.

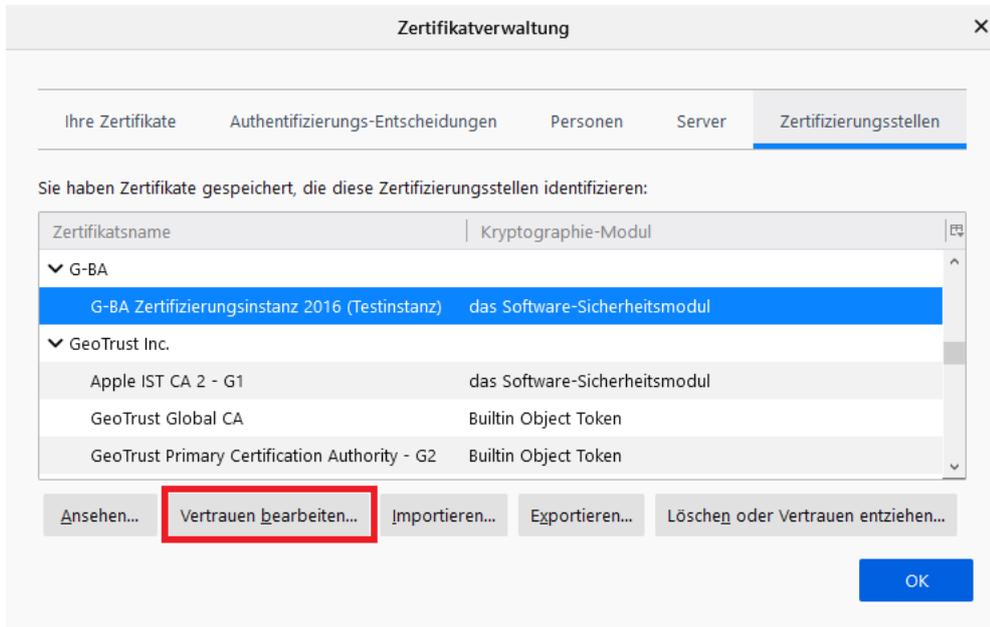
Zertifikatsverwaltung ✕

Ihre Zertifikate Authentifizierungs-Entscheidungen Personen Server Zertifizierungsstellen

Sie haben Zertifikate dieser Organisationen, die Sie identifizieren:

Zertifikatsname	Kryptographie-Modul	Seriennummer	Gültig bis	
▼ G-BA				
C0	das Software-Sicherheitsmodul	00:C0	Freitag, 17. Juni 2022	

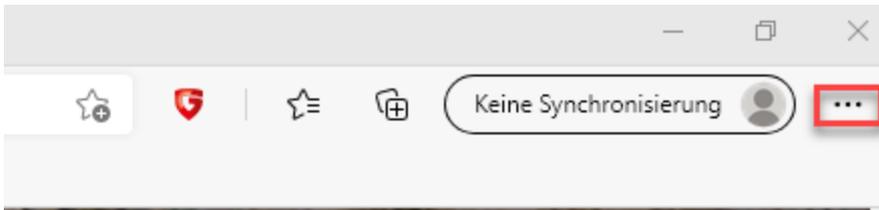
Wechseln Sie in der Zertifikatsverwaltung auf den Reiter *Zertifizierungsstellen*. Suchen Sie in der Liste nach G-BA und markieren Sie den Eintrag G-BA Zertifizierungsinstanz. Klicken Sie anschließend auf *Vertrauen bearbeiten*:



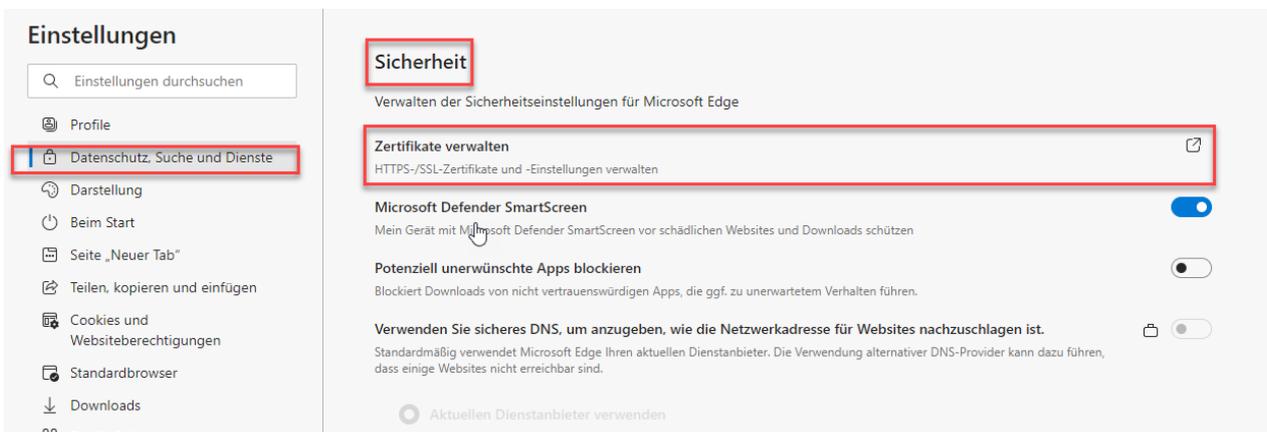
Es öffnet sich das Pop-up-Fenster *CA-Zertifikat-Vertrauenseinstellungen bearbeiten*. Markieren Sie beide Vertrauenseinstellungen (Websites, Mail-Benutzer und Software-Hersteller) und bestätigen Sie mit *OK* und danach noch einmal mit *OK* bestätigen.

Microsoft Edge

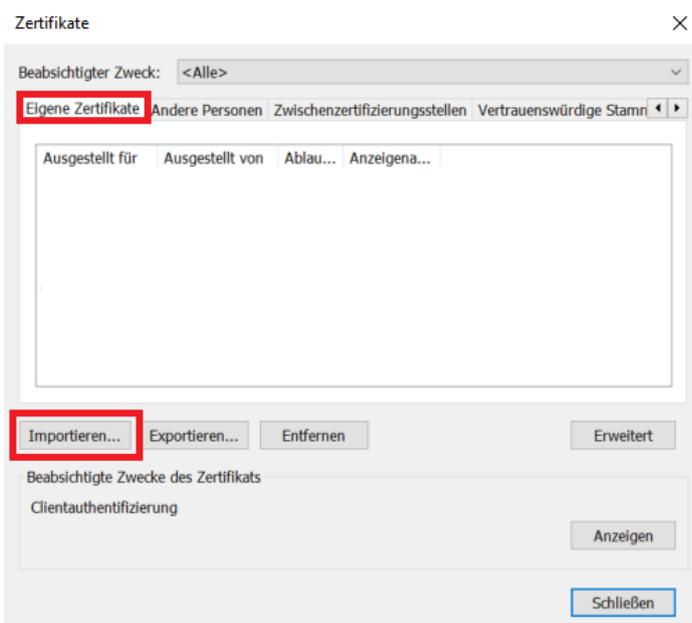
Starten Sie den Microsoft Edge Browser, öffnen Sie das Menü über die drei Punkte und wählen Sie dort den Punkt Einstellungen aus.



Wählen Sie den Punkt Datenschutz, Suche und Dienste aus und scrollen Sie im rechten Bildschirmbereich zum Punkt Sicherheit und wählen Sie Zertifikate verwalten aus.



Der Assistent zur Organisation von Zertifikaten öffnet sich. Dort klicken Sie unter dem Reiter *Eigene Zertifikate* auf die Schaltfläche *Importieren* und der Assistent für den Zertifikatsimport wird gestartet.



✕

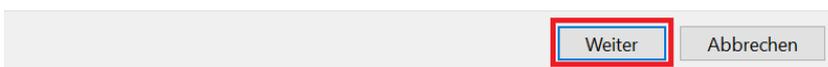
←  Zertifikatimport-Assistent

Willkommen

Dieser Assistent hilft Ihnen beim Kopieren von Zertifikaten, Zertifikatvertrauenslisten und Zertifikatssperrlisten vom Datenträger in den Zertifikatspeicher.

Ein von einer Zertifizierungsstelle ausgestelltes Zertifikat dient der Identitätsbestätigung. Es enthält Informationen für den Datenschutz oder für den Aufbau sicherer Netzwerkverbindungen. Ein Zertifikatspeicher ist der Systembereich, in dem Zertifikate gespeichert werden.

Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.



Geben Sie im Feld Dateiname manuell den Pfad und den Namen der p12-Datei an oder wählen Sie über die Schaltfläche *Durchsuchen* die Datei direkt aus. Achten Sie bei der Auswahl über *Durchsuchen* auf den entsprechenden Dateityp (.p12). Klicken Sie anschließend auf *Weiter*.

Zu importierende Datei

Geben Sie die Datei an, die importiert werden soll.

Dateiname:

Hinweis: Mehrere Zertifikate können in einer Datei in folgenden Formaten gespeichert werden:

Privater Informationsaustausch - PKCS #12 (.PFX,.P12)

Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)

Microsoft Serieller Zertifikatspeicher (.SST)

Geben Sie nun das achtstellige Kennwort für die Zertifikat-Installation ein. Wählen Sie bitte nur das dritte Feld *Alle erweiterten Eigenschaften mit einbeziehen* aus, indem Sie den entsprechenden Haken setzen. Anschließend klicken Sie auf *Weiter*.

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

Markieren Sie für den Zertifikatspeicher die Option *Zertifikatspeicher automatisch auswählen* und bestätigen Sie mit *Weiter*:

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:

Eigene Zertifikate

Durchsuchen...

Weiter

Abbrechen

Überprüfen Sie in dieser Ansicht Ihre Einstellungen und bestätigen Sie diese über die Schaltfläche *Fertig stellen*

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\Downloads\45.p12

Fertig stellen

Abbrechen

Es erscheint eine Sicherheitswarnung mit Informationen zur Zertifizierungsinstanz und dem Hinweis zur Kontrolle des Fingerabdrucks. Bestätigen Sie mit *Ja*.

Sicherheitswarnung



Sie sind im Begriff, ein Zertifikat von einer Zertifizierungsstelle zu installieren, die sich wie folgt darstellt:

G-BA Zertifizierungsinstanz 2016 (Testinstanz)

Es wird nicht bestätigt, dass das Zertifikat wirklich von "G-BA Zertifizierungsinstanz 2016 (Testinstanz)" stammt. Wenden Sie sich an "G-BA Zertifizierungsinstanz 2016 (Testinstanz)", um die Herkunft zu bestätigen. Die folgende Zahl hilft Ihnen bei diesem Prozess weiter:

Fingerabdruck (sha1): F793C1E9 04EECD83 C7EB6659 CE89B248
3310C124

Warnung:

Wenn Sie dieses Stammzertifikat installieren, wird automatisch allen Zertifikaten vertraut, die von dieser Zertifizierungsstelle ausgestellt werden. Die Installation mit einem unbestätigten Fingerabdruck stellt ein Sicherheitsrisiko dar. Falls Sie auf "Ja" klicken, nehmen Sie dieses Risiko in Kauf.

Möchten Sie dieses Zertifikat installieren?

Ja

Nein

Damit ist der Import des Zertifikats erfolgreich abgeschlossen. Bestätigen Sie mit *OK*.

Zertifikatimport-Assistent



Der Importvorgang war erfolgreich.

OK

Das Zertifikat erscheint nun in der Liste. Schließen Sie das Fenster und klicken Sie im Fenster der Internetoptionen auf *OK*.

Zertifikate ×

Beabsichtigter Zweck: <Alle> ▼

Eigene Zertifikate | Andere Personen | Zwischenzertifizierungsstellen | Vertrauenswürdige Stamm ◀ ▶

Ausgestellt für	Ausgestellt von	Ablau...	Anzeigena...
 45	G-BA Zertifizie...	17.06...	G-BA Vertr...

Importieren... | Exportieren... | Entfernen | Erweitert

Beabsichtigte Zwecke des Zertifikats

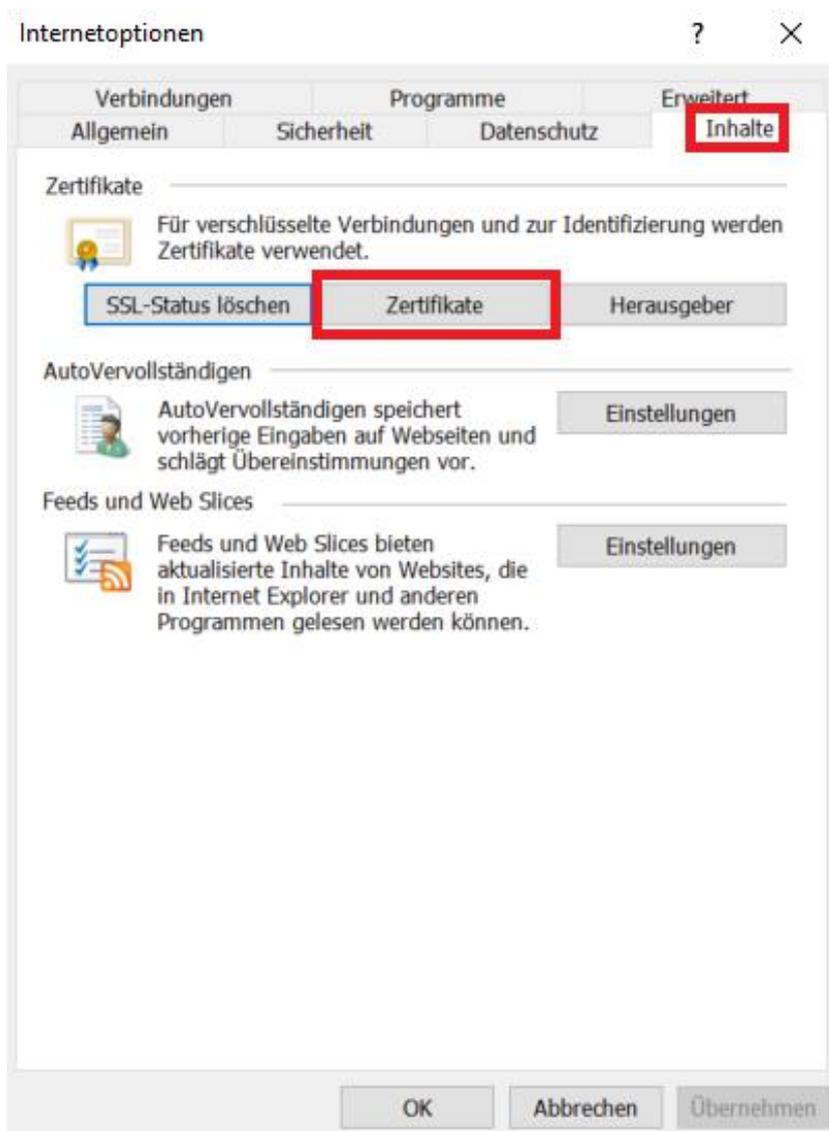
Serverauthentifizierung, Clientauthentifizierung Anzeigen

Schließen

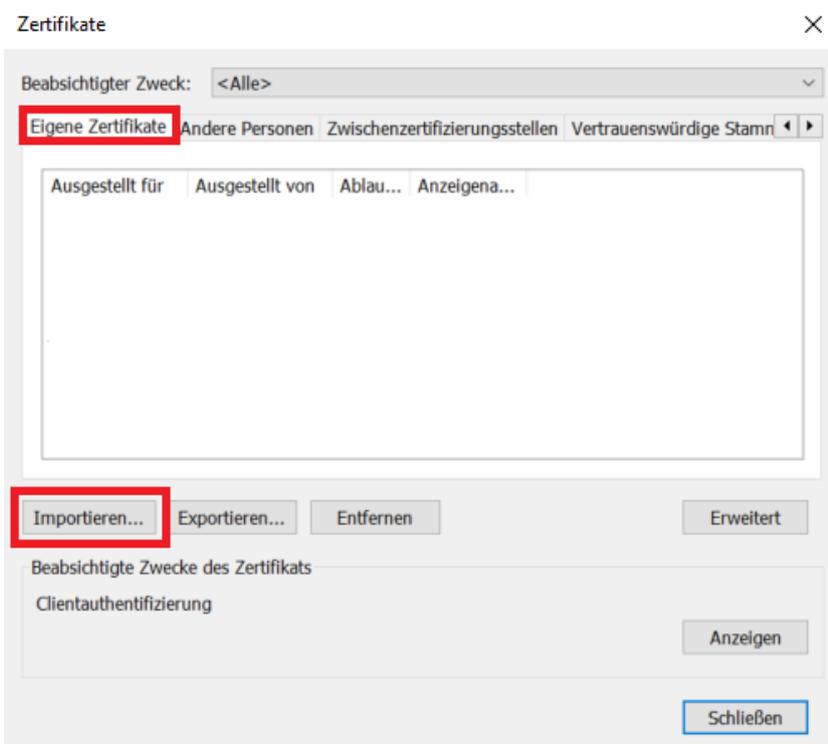
Microsoft Internet Explorer

Starten Sie den Microsoft Internet Explorer und wählen Sie im Menü *Extras* (bzw. über das Zahnrad-Symbol) den Punkt *Internetoptionen* aus.

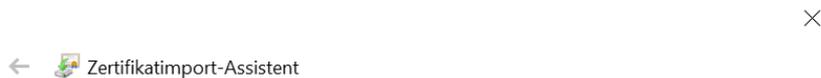
Bestätigen Sie den Reiter *Inhalte* und klicken Sie anschließend auf die Schaltfläche *Zertifikate*.



Der Assistent zur Organisation von Zertifikaten öffnet sich. Dort klicken Sie unter dem Reiter *Eigene Zertifikate* auf die Schaltfläche *Importieren* und der Assistent für den Zertifikatsimport wird gestartet.



Klicken Sie auf *Weiter*, um zur nächsten Bearbeitungsmaske zu gelangen.

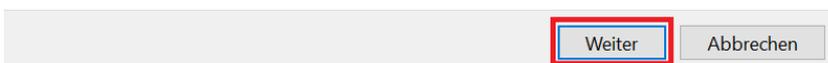


Willkommen

Dieser Assistent hilft Ihnen beim Kopieren von Zertifikaten, Zertifikatvertrauenslisten und Zertifikatssperrlisten vom Datenträger in den Zertifikatspeicher.

Ein von einer Zertifizierungsstelle ausgestelltes Zertifikat dient der Identitätsbestätigung. Es enthält Informationen für den Datenschutz oder für den Aufbau sicherer Netzwerkverbindungen. Ein Zertifikatspeicher ist der Systembereich, in dem Zertifikate gespeichert werden.

Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.



Geben Sie im Feld Dateiname manuell den Pfad und den Namen der p12-Datei an oder wählen Sie über die Schaltfläche *Durchsuchen* die Datei direkt aus. Achten Sie bei der Auswahl über *Durchsuchen* auf den entsprechenden Dateityp (.p12). Klicken Sie anschließend auf *Weiter*.

Zu importierende Datei

Geben Sie die Datei an, die importiert werden soll.

Dateiname:

Hinweis: Mehrere Zertifikate können in einer Datei in folgenden Formaten gespeichert werden:

Privater Informationsaustausch - PKCS #12 (.PFX,.P12)

Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)

Microsoft Serieller Zertifikatspeicher (.SST)

Geben Sie nun das achtstellige Kennwort für die Zertifikat-Installation ein. Wählen Sie bitte nur das dritte Feld *Alle erweiterten Eigenschaften mit einbeziehen* aus, indem Sie den entsprechenden Haken setzen. Anschließend klicken Sie auf *Weiter*.

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**

Markieren Sie für den Zertifikatspeicher die Option *Zertifikatspeicher automatisch auswählen* und bestätigen Sie mit *Weiter*:

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:

Eigene Zertifikate

Durchsuchen...

Weiter

Abbrechen

Überprüfen Sie in dieser Ansicht Ihre Einstellungen und bestätigen Sie diese über die Schaltfläche *Fertig stellen*

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\Downloads\45.p12

Fertig stellen

Abbrechen

Es erscheint eine Sicherheitswarnung mit Informationen zur Zertifizierungsinstanz und dem Hinweis zur Kontrolle des Fingerabdrucks. Bestätigen Sie mit *Ja*.

Sicherheitswarnung



Sie sind im Begriff, ein Zertifikat von einer Zertifizierungsstelle zu installieren, die sich wie folgt darstellt:

G-BA Zertifizierungsinstanz 2016 (Testinstanz)

Es wird nicht bestätigt, dass das Zertifikat wirklich von "G-BA Zertifizierungsinstanz 2016 (Testinstanz)" stammt. Wenden Sie sich an "G-BA Zertifizierungsinstanz 2016 (Testinstanz)", um die Herkunft zu bestätigen. Die folgende Zahl hilft Ihnen bei diesem Prozess weiter:

Fingerabdruck (sha1): F793C1E9 04EECD83 C7EB6659 CE89B248
3310C124

Warnung:

Wenn Sie dieses Stammzertifikat installieren, wird automatisch allen Zertifikaten vertraut, die von dieser Zertifizierungsstelle ausgestellt werden. Die Installation mit einem unbestätigten Fingerabdruck stellt ein Sicherheitsrisiko dar. Falls Sie auf "Ja" klicken, nehmen Sie dieses Risiko in Kauf.

Möchten Sie dieses Zertifikat installieren?

Ja

Nein

Damit ist der Import des Zertifikats erfolgreich abgeschlossen. Bestätigen Sie mit *OK*.

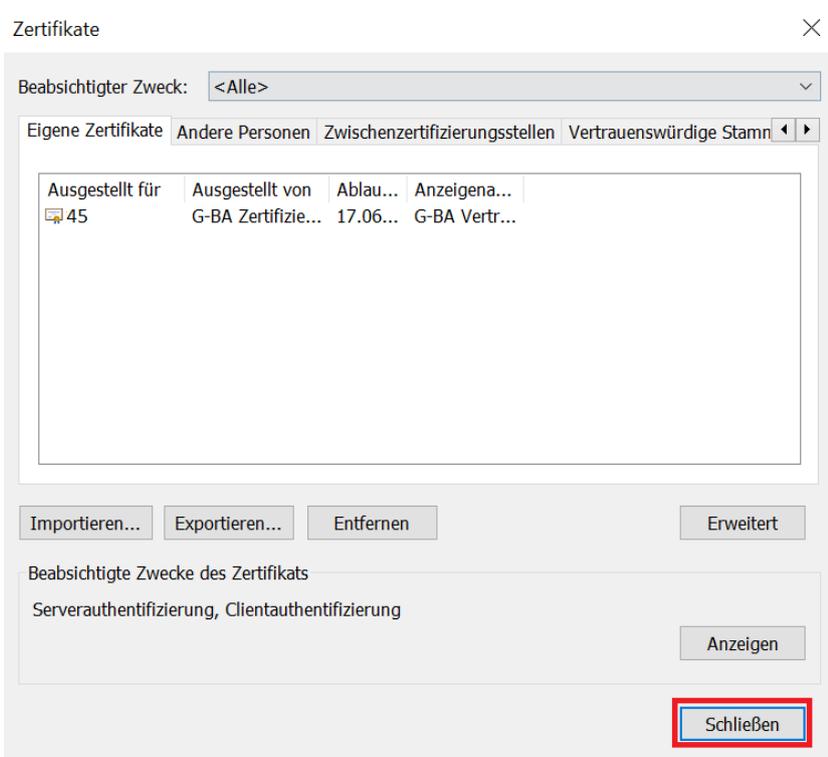
Zertifikatimport-Assistent



Der Importvorgang war erfolgreich.

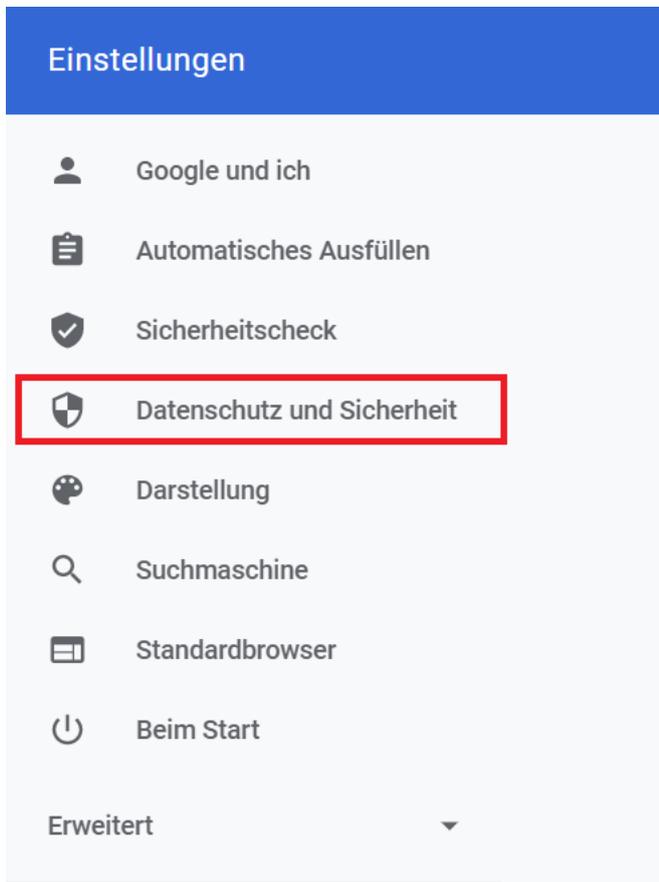
OK

Das Zertifikat erscheint nun in der Liste. Schließen Sie das Fenster und klicken Sie im Fenster der Internetoptionen auf *OK*.

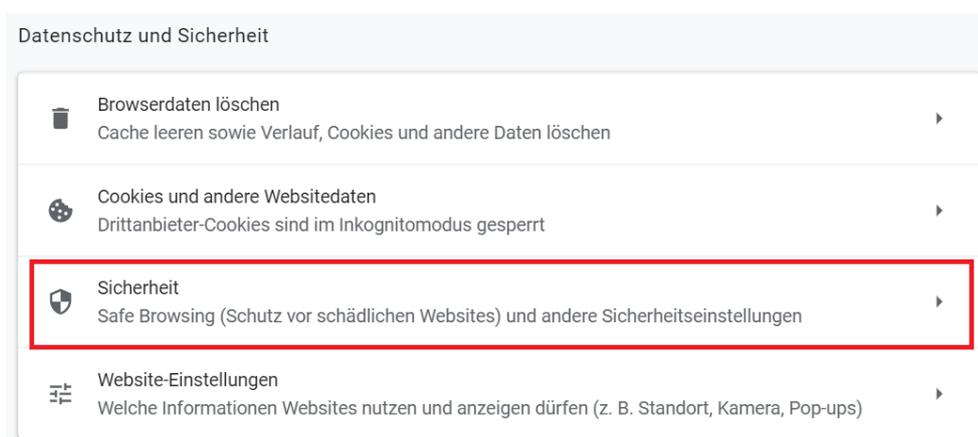


Google Chrome

Klicken Sie auf die drei Punkte in der rechten oberen Ecke des Browsers und navigieren Sie zu den *Einstellungen*. Wählen Sie nun im Menü auf der linken Seite *Datenschutz und Sicherheit* aus.



Es öffnen sich weitere Punkte. Klicken Sie dort auf den Punkt *Sicherheit* verwalten.



Scrollen Sie nach unten zu dem Abschnitt *Erweitert*, dort finden Sie den Menüpunkt *Zertifikate verwalten*.

Erweitert

Sicheres DNS verwenden ☐
Diese Einstellung ist bei verwalteten Browsern deaktiviert

Zertifikate verwalten 🔗
HTTPS/SSL-Zertifikate und -Einstellungen verwalten

Erweitertes Sicherheitsprogramm von Google 🔗
Schützt private Google-Konten jeglicher Nutzer vor gezielten Angriffen

Es öffnet sich das Fenster *Zertifikate*. Dort klicken Sie unter dem Reiter *Eigene Zertifikate* auf *Importieren*.

Zertifikate ✕

Beabsichtigter Zweck: <Alle> ▾

Eigene Zertifikate Andere Personen Zwischenzertifizierungsstellen Vertrauenswürdige Stamm ▾

Ausgestellt für	Ausgestellt von	Ablau...	Anzeigena...
-----------------	-----------------	----------	--------------

Importieren... Exportieren... Entfernen Erweitert

Beabsichtigte Zwecke des Zertifikats
Clientauthentifizierung Anzeigen

Schließen

Klicken Sie auf *Weiter*, um zur nächsten Bearbeitungsmaske zu gelangen.



←  Zertifikatimport-Assistent

Willkommen

Dieser Assistent hilft Ihnen beim Kopieren von Zertifikaten, Zertifikatvertrauenslisten und Zertifikatssperrlisten vom Datenträger in den Zertifikatspeicher.

Ein von einer Zertifizierungsstelle ausgestelltes Zertifikat dient der Identitätsbestätigung. Es enthält Informationen für den Datenschutz oder für den Aufbau sicherer Netzwerkverbindungen. Ein Zertifikatspeicher ist der Systembereich, in dem Zertifikate gespeichert werden.

Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.

Weiter

Abbrechen

Geben Sie im Feld Dateiname manuell den Pfad und den Namen der p12-Datei an oder wählen Sie über die Schaltfläche *Durchsuchen* die Datei direkt aus. Achten Sie bei der Auswahl über *Durchsuchen* auf den entsprechenden Dateityp (.p12). Klicken Sie anschließend auf *Weiter*.

Zu importierende Datei

Geben Sie die Datei an, die importiert werden soll.

Dateiname:

C:\Users\Downloads\45.p12

Durchsuchen...

Hinweis: Mehrere Zertifikate können in einer Datei in folgenden Formaten gespeichert werden:

Privater Informationsaustausch - PKCS #12 (.PFX, .P12)

Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)

Microsoft Serieller Zertifikatspeicher (.SST)

Weiter

Abbrechen

Geben Sie nun das achtstellige Kennwort für die Zertifikat-Installation ein. Wählen Sie bitte nur das dritte Feld *Alle erweiterten Eigenschaften mit einbeziehen* aus, indem Sie den entsprechenden Haken setzen. Anschließend klicken Sie auf Weiter.

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**

Weiter

Abbrechen

Markieren Sie für den Zertifikatspeicher die Option *Zertifikatspeicher automatisch auswählen* und bestätigen Sie mit *Weiter*:

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:

Eigene Zertifikate

Durchsuchen...

Weiter

Abbrechen

Überprüfen Sie in dieser Ansicht Ihre Einstellungen und bestätigen Sie diese über die Schaltfläche *Fertig stellen*

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\Downloads\45.p12

Fertig stellen

Abbrechen

Es erscheint eine Sicherheitswarnung mit Informationen zur Zertifizierungsinstanz und dem Hinweis zur Kontrolle des Fingerabdrucks. Bestätigen Sie mit *Ja*.

Sicherheitswarnung



Sie sind im Begriff, ein Zertifikat von einer Zertifizierungsstelle zu installieren, die sich wie folgt darstellt:

G-BA Zertifizierungsinstanz 2016 (Testinstanz)

Es wird nicht bestätigt, dass das Zertifikat wirklich von "G-BA Zertifizierungsinstanz 2016 (Testinstanz)" stammt. Wenden Sie sich an "G-BA Zertifizierungsinstanz 2016 (Testinstanz)", um die Herkunft zu bestätigen. Die folgende Zahl hilft Ihnen bei diesem Prozess weiter:

Fingerabdruck (sha1): F793C1E9 04EECD83 C7EB6659 CE89B248
3310C124

Warnung:

Wenn Sie dieses Stammzertifikat installieren, wird automatisch allen Zertifikaten vertraut, die von dieser Zertifizierungsstelle ausgestellt werden. Die Installation mit einem unbestätigten Fingerabdruck stellt ein Sicherheitsrisiko dar. Falls Sie auf "Ja" klicken, nehmen Sie dieses Risiko in Kauf.

Möchten Sie dieses Zertifikat installieren?

Ja

Nein

Damit ist der Import des Zertifikats erfolgreich abgeschlossen. Bestätigen Sie mit *OK*.

Zertifikatimport-Assistent



Der Importvorgang war erfolgreich.

OK

Das Zertifikat erscheint nun in der Liste. Schließen Sie das Fenster und klicken Sie im Fenster der Internetoptionen auf *OK*.

