



INSTALLATION VON ZERTIFIKATEN





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.

	P In Einstellungen suchen	
🔅 Allgemein	Allgemein	
Startseite	Start	
Q Suche	Vorherige Sitzung wiederherstellen	
Datenschutz & Sicherheit	Beim Beenden des Browsers warnen Immer über <u>p</u> rüfen, ob Firefox der Standardbrowser ist	
Sync		

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

Sicherheit

Schutz vor betrügerischen Inhalten und gefährlicher Software

- Gefährliche und betrügerische Inhalte blockieren Weitere Informationen
 - ✓ Gefährliche <u>D</u>ownloads blockieren
 - Vor unerwünschter und ungewöhnlicher Software warnen

Zertifikate

Wenn eine Website nach dem persönlichen Sicherheitszertifikat verlangt

- Automatisch eins <u>w</u>ählen
- Jedes Mal fragen
- Aktuelle <u>G</u>ültigkeit von Zertifikaten durch Anfrage bei OCSP-Server bestätigen lassen

Zertifikate anzeigen	
----------------------	--

Kryptographie-Module...



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

uthentifizierungs-Entscheidungen r Organisationen, die Sie identifizier	Personen Server	Zertifizierungssteller	n
r Organisationen, die Sie identifizier	en:		
Kryptographie-Modul	Seriennummer	Gültig bis	Ę
Kryptographie-Modul	Seriennummer	Gültig bis	₽
, F.O.3 F.I.2 (110 dai)		1	1 -
	Kryptographie-Modul	Kryptographie-Modul Seriennummer	Kryptographie-Modul Seriennummer Gültig bis

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

U importierende Zerti	Tikat-Datei	~	ē		chen
Organisieren 🔻 Neu	ier Ordner			== .	- 🗆 🔞
	Name	^		Änderungsdatum	
3D-Objekte	🎲 45.p12			08.02.2021 12:59	
Nilder					
Desktop					
🗎 Dokumente					
🖊 Downloads					
👌 Musik					
Videos					
🛶 Archiv (\\192.16					
🛶 Ausschreibunge					
🐛 Windows (C:)	· <				>
Dat	einame: 45.p12		~	PKCS12-Dateien	~
	L ·			Öffnen	Abbrechen



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 verwe	ndet wurde:
OK Abbrechen	

Nun wird das importierte Zertifikat in der Zertifikatsverwaltung angezeigt.

	Zertifikatverwa	Itung		
Ihre Zertifikate	Authentifizierungs-Entscheidungen	Personen Server	Zertifizierungsstellen	
ie haben Zertifikate	dieser Organisationen, die Sie identifiziere	en:		
Zertifikatsname	Kryptographie-Modul	Seriennummer	Gültig bis	٣,
✔ G-BA				
C0	das Software-Sicherheitsmodul	00:C0	Freitag, 17. Juni 2022	
<u>A</u> nsehen <u>S</u> i	chern <u>A</u> lle sichern <u>I</u> mportierer	 <u>L</u> öschen		



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:

	Zertifi	katverw	altung			
Ihre Zertifikate	Authentifizierungs-Entscheid	ungen	Personen	Server	Zertifizierungsst	ellen
ie haben Zertifikate	gespeichert, die diese Zertifizier	rungsstel	len identifizieren:			
Zertifikatsname		Kryp	tographie-Modul			E,
✔ G-BA						^
G-BA Zertifizie	rungsinstanz 2016 (Testinstanz)	das So	oftware-Sicherheit	tsmodul		
✔ GeoTrust Inc.						- 1
Apple IST CA 2	! - G1	das So	oftware-Sicherheit	smodul		
GeoTrust Glob	al CA	Builtin	Object Token			
GeoTrust Prima	ary Certification Authority - G2	Builtin	Object Token			
<u>A</u> nsehen Ver	trauen <u>b</u> earbeiten <u>I</u> mporti	eren	E <u>x</u> portieren	Lösche <u>n</u> o	der Vertrauen entzie	hen
						OK
						OK -

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.

Nortal

Microsoft Edge

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

			_	đ	\times
6	ן ל	Ē	Keine Synchronisierung	2	

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

Ein	stellungen	Sicherheit	
8	Profile Datenschutz, Suche und Dienste	Verwalten der Sicherheitseinstellungen für Microsoft Edge Zertifikate verwalten HTTPS-/SSI-Zertifikate und -Einstellungen verwalten	Ø
() ()	Darstellung Beim Start Saite, Navas Tab."	Microsoft Defender SmartScreen Mein Gerät mit Millmsoft Defender SmartScreen vor schädlichen Websites und Downloads schützen	
ľ	Teilen, kopieren und einfügen	Potenziell unerwünschte Apps blockieren Blockiert Downloads von nicht vertrauenswürdigen Apps, die ggf. zu unerwartetem Verhalten führen.	
u¢ Cø	Websiteberechtigungen Standardbrowser	Verwenden Sie sicheres DNS, um anzugeben, wie die Netzwerkadresse für Websites nachzuschlagen ist. Standardmäßig verwendet Microsoft Edge Ihren aktuellen Dienstanbieter. Die Verwendung alternativer DNS-Provider kann dazu führen, dass einige Websites nicht erreichbar sind.	–
<u>↓</u>	Downloads	Aktuellen Dienstanbieter verwenden	

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.



Zertifikate	×
Beabsichtigter Zweck: <alle></alle>	e
Eigene Zertifikate Andere Personen Zwischenzertifizierungsstellen Vertrauenswürdige Stamm	•
Ausgestellt für Ausgestellt von Ablau Anzeigena	
Importieren Entfernen Erweitert	
Beabsichtigte Zwecke des Zertifikats Clientauthentifizierung	
Anzeigen	
Schließen	

 \times

🔶 嵾 Zertifikatimport-Assistent

Dieser Assistent hilft Ihnen beim Kopieren von Zertifikaten, Zertifikatvertrauenslisten und Zertifikatssperlisten 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.

C:\Users\Downloads\45.p12	Durchsuchen
Hinweis: Mehrere Zertifikate können in einer Datei in folg werden:	genden Formaten gespeichert
Privater Informationsaustausch - PKCS #12 (.PFX,.P12	2)
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*.

Abbrechen

Weiter

ge	währleisten.
G	zben Sie das Kennwort für den privaten Schlüssel ein.
Ke	nnwort:
	••••••
	Kennwort anzeigen
In	iportoptionen:
	Hohe Sicherheit f ür den privaten Schl üssel aktivieren. Wenn Sie diese Option aktivieren, werden Sie immer dann, wenn der private Schl üssel 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)
ſ	🗹 Alle erweiterten Eigenschaften mit einbeziehen



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

indows kann automatisch einen Zertifikatspeicher auswählen, oder Sie können einer beicherort für die Zertifikate angeben.				
• Zertifikatspeicher automatisch auswählen	(auf dem Zertifikattyp basierend)			
O Alle Zertifikate in folgendem Speicher spe	ichern			
Zertifikatspeicher:				
Eigene Zertifikate	Durchsuche			

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 Einstellun	gen 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

 \times

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.



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



Zertifikate	×
Beabsichtigter Zweck: <alle></alle>	×1
Eigene Zertifikate Andere Personen Zwischenzertifizierungsstellen Vertrauenswürdige Stamn	•
Ausgestellt für Ausgestellt von Ablau Anzeigena 45 G-BA Zertifizie 17.06 G-BA Vertr	
Importieren Exportieren Entfernen Erweitert	
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.

	ngen	Programm	e	Erweitert
Allgemein	Sicher	heit D	atenschutz	Inhalte
Zertifikate Für Für Zer	verschlüsselte tifikate verwend	Verbindungen u let.	ınd zur Identifiz	ierung werden
SSL-Stat	us löschen	Zertifikate	He	rausgeber
AutoVervollstär	ndigen			
Aut vor sch	oVervollständig herige Eingaber lägt Übereinstin	en speichert n auf Webseiten nmungen vor.	und	stellungen
eeds und Web	Slices			
akt in I Pro	ualisierte Inhalt nternet Explore grammen geles	e von Websites, r und anderen en werden kön	die nen.	stenungen



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.

Zertifikate					>
Beabsichtigter Zweck: </th <th>Alle></th> <th></th> <th></th> <th></th> <th>~</th>	Alle>				~
Eigene Zertifikate Andere	Personen Z	wischenzer	tifizierungsstell	en Vertrauenswi	irdige Stamn 🔹 🕨
Ausgestellt für Ausg	estellt von	Ablau	Anzeigena		
Importieren Exporti Beabsichtigte Zwecke des	eren Zertifikats	Entfernen			Erweitert
Clientauthentifizierung					Anzeigen
					Schließen

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

 \times

🔶 🛿 🐓 Zertifikatimport-Assistent

Willkommen

Dieser Assistent hilft Ihnen beim Kopieren von Zertifikaten, Zertifikatvertrauenslisten und Zertifikatssperlisten 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*.

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 Forma werden:	ten gespeichert
Privater Informationsaustausch - PKCS #12 (.PFX,.P12)	
Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate	e (.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*.

Geben Sie das Kennwort für den privaten Schlüssel ein. Kennwort: Kennwort Kennwort anzeigen Importoptionen: Hohe Sicherheit für den privaten Schlüssel aktivieren. Wenn Sie diese Optior 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 späteren Zeitpunkt sichern bzw. überführen. Privaten Schlüssel mit virtualisierungsbasierter Sicherheit schützen (nicht exportierbar) Alle erweiterten Eigenschaften mit einbeziehen	
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 späteren Zeitpunkt sichern bzw. überführen. Privaten Schlüssel mit virtualisierungsbasierter Sicherheit schützen (nicht exportierbar) Alle erweiterten Eigenschaften mit einbeziehen	
 Kennwort anzeigen Importoptionen: Hohe Sicherheit für den privaten Schlüssel aktivieren. Wenn Sie diese Optior 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 späteren Zeitpunkt sichern bzw. überführen. Privaten Schlüssel mit virtualisierungsbasierter Sicherheit schützen (nicht exportierbar) ✓ Alle erweiterten Eigenschaften mit einbeziehen 	
Importoptionen: Hohe Sicherheit für den privaten Schlüssel aktivieren. Wenn Sie diese Optior 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 späteren Zeitpunkt sichern bzw. überführen. Privaten Schlüssel mit virtualisierungsbasierter Sicherheit schützen (nicht exportierbar) Alle erweiterten Eigenschaften mit einbeziehen	
 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 späteren Zeitpunkt sichern bzw. überführen. Privaten Schlüssel mit virtualisierungsbasierter Sicherheit schützen (nicht exportierbar) Alle erweiterten Eigenschaften mit einbeziehen 	
 Schlüssel als exportierbar markieren. Dadurch können Sie Ihre Schlüssel zu späteren Zeitpunkt sichern bzw. überführen. Privaten Schlüssel mit virtualisierungsbasierter Sicherheit schützen (nicht exportierbar) Alle erweiterten Eigenschaften mit einbeziehen 	ion
 Privaten Schlüssel mit virtualisierungsbasierter Sicherheit schützen (nicht exportierbar) Alle erweiterten Eigenschaften mit einbeziehen 	u einen
✓ Alle erweiterten Eigenschaften mit einbeziehen	



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

ndows kann automatisch einen Zertifik eicherort für die Zertifikate angeben.	atspeicher ausw	ählen, oder Sie	e können einen
Zertifikatspeicher automatisch ausv	vählen (auf den	n Zertifikattyp b	asierend)
O Alle Zertifikate in folgendem Speic	her speichern		
Zertifikatspeicher:			
Eigene Zertifikate			Durchsuchen

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

 \times

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?



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





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

Zertifikate >	<
Beabsichtigter Zweck: <a>Alle>	
Eigene Zertifikate Andere Personen Zwischenzertifizierungsstellen Vertrauenswürdige Stamn	
Ausgestellt fürAusgestellt vonAblauAnzeigena45G-BA Zertifizie17.06G-BA Vertr	
Importieren Entfernen Erweitert	
Beabsichtigte Zwecke des Zertifikats	
Anzeigen	
Schließen	



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.

Einstellungen		
•	Google und ich	
Ê	Automatisches Ausfüllen	
•	Sicherheitscheck	
0	Datenschutz und Sicherheit	
۲	Darstellung	
Q	Suchmaschine	
	Standardbrowser	
Ċ	Beim Start	
Erweitert -		

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

Datenschutz und Sicherheit Browserdaten löschen Î • Cache leeren sowie Verlauf, Cookies und andere Daten löschen Cookies und andere Websitedaten ٩ ▶ Drittanbieter-Cookies sind im Inkognitomodus gesperrt Sicherheit 0 ▶ Safe Browsing (Schutz vor schädlichen Websites) und andere Sicherheitseinstellungen Website-Einstellungen 랿 ۲ Welche Informationen Websites nutzen und anzeigen dürfen (z. B. Standort, Kamera, Pop-ups)



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	Z
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></alle>	\times
Eigene Zertifikate Andere Personen Zwischenzertifizierungsstellen Vertrauenswürdige Stamn	•
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 Abbrecher	١

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*.

Dateina	me:				
C:\Use	rs\Downloads\45.p	12			Durchsucher
Hinweis werden	: Mehrere Zertifikat :	e können in ein	er Datei in folge	enden Format	en gespeichert
Priv	ater Informationsau	stausch - PKCS	#12 (.PFX,.P12)	
Synt	axstandard kryptog	rafischer Meldu	ngen - "PKCS #	7"-Zertifikate	(.P7B)
Micr	osoft Serieller Zertif	ikatspeicher (.S	ST)		

hen	Abbrechen	Weiter



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.

(Geben Sie das Kennwort für den privaten Schlüssel ein.
K	iennwort:
	••••••
	Kennwort anzeigen
I	mportoptionen:
	Hohe Sicherheit f ür den privaten Schl üssel aktivieren. Wenn Sie diese Option aktivieren, werden Sie immer dann, wenn der private Schl üssel von einer Anwendung verwendet wird, zur Kennworteingabe aufgefordert.
	Schlüssel als exportierbar markieren. Dadurch können Sie Ihre Schlüssel zu einer 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:

ndows kann automatisch einen Zertifil eicherort für die Zertifikate angeben.	katspeicher auswähle	en, oder Sie	e können einen
Zertifikatspeicher automatisch aus	wählen (auf dem Ze	rtifikattyp b	asierend)
O Alle Zertifikate in folgendem Spei	cher speichern		
Zertifikatspeicher:			
Eigene Zertifikate			Durchsuchen

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

 \times

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?



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





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

Zertifikate ×
Beabsichtigter Zweck: <a>Alle>
Eigene Zertifikate Andere Personen Zwischenzertifizierungsstellen Vertrauenswürdige Stamn • •
Ausgestellt für Ausgestellt von Ablau Anzeigena 45 G-BA Zertifizie 17.06 G-BA Vertr
Importieren Exportieren Entfernen Erweitert
Serverauthentifizierung, Clientauthentifizierung
Anzeigen
Schließen