



# Anleitung Client-Zertifikat mit Microsoft Edge / Mozilla Firefox

## Inhaltsverzeichnis

1	Zugriff einrichten .....	2
	Microsoft Edge.....	2
	Mozilla Firefox.....	8
2	Zugriff verlängern / Zertifikat löschen .....	12
	Microsoft Edge.....	12
	Mozilla Firefox.....	13
3	Fehlerquellen und mögliche Behebungsansätze .....	17
	Bekannte Fehler .....	17
	Lösungsansätze.....	17



## Impressum

IT-Systemhaus – TEC12  
Tafelhofstraße 4  
90443 Nürnberg  
[www.arbeitsagentur.de](http://www.arbeitsagentur.de)

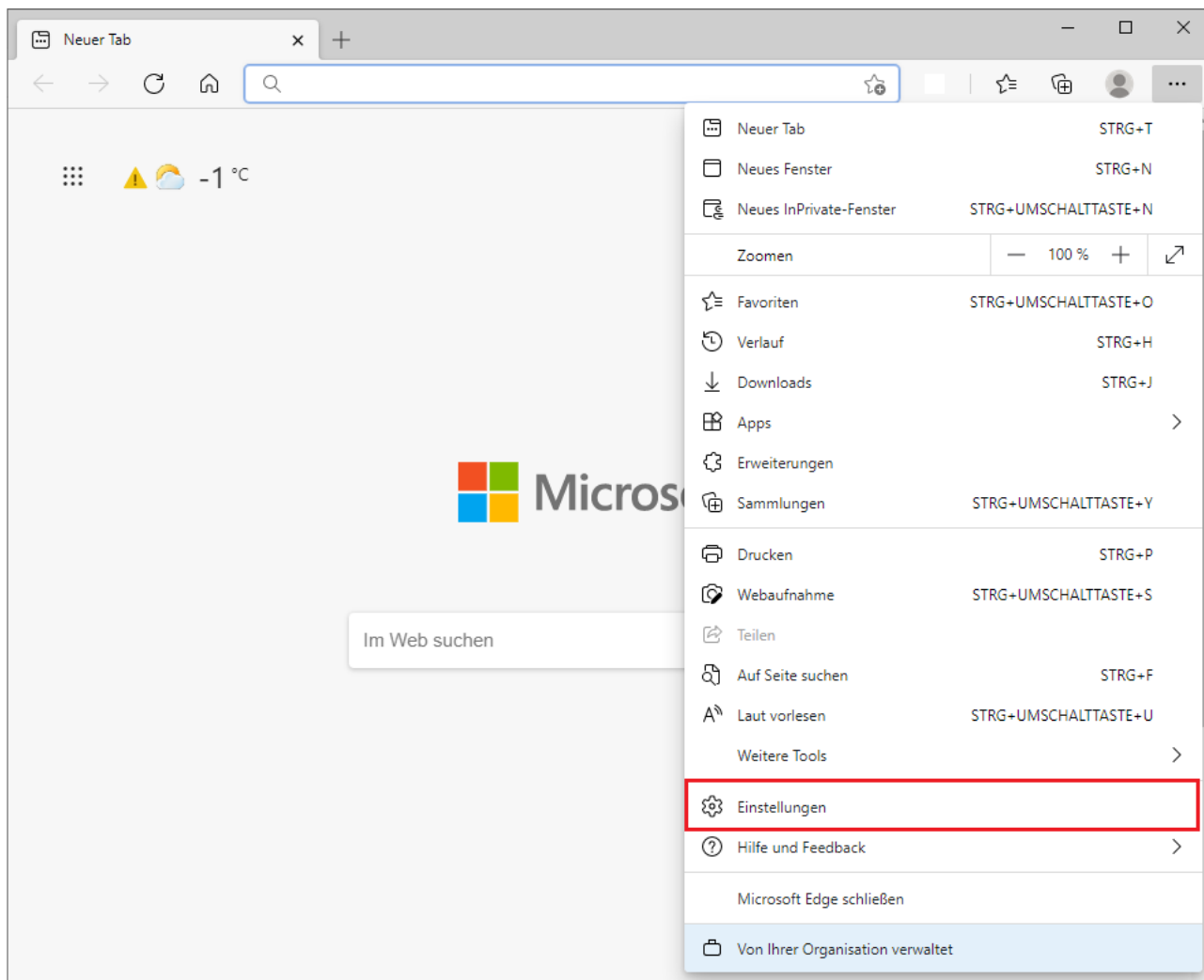
# 1 Zugriff einrichten

## Microsoft Edge

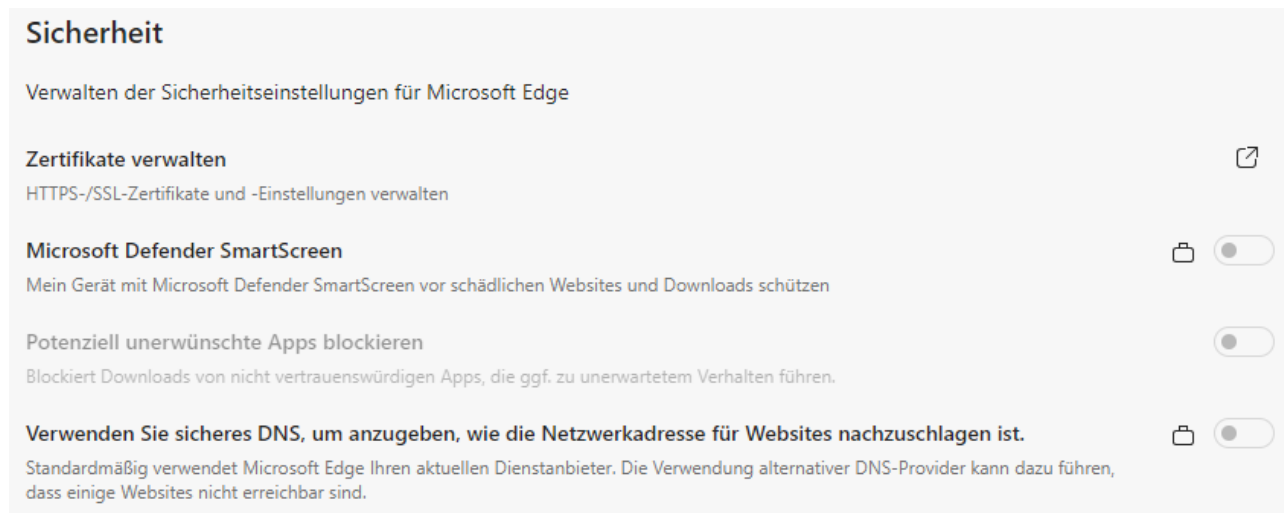
Die folgende Anleitung beschreibt das Vorgehen für die Installation der Zertifikatsdatei für den Microsoft Edge Browser.

Bevor das per E-Mail eingegangene Zertifikat installiert werden kann, muss die per Mail erhaltene „.p12“-Datei an einem beliebigen Ort abgespeichert werden. Laden Sie sich dazu die entsprechende Datei mit dem Link aus der E-Mail herunter. Nachdem Sie das erledigt haben, erhalten Sie in einer weiteren Mail ein Passwort, das Sie im weiteren Verlauf benötigen.

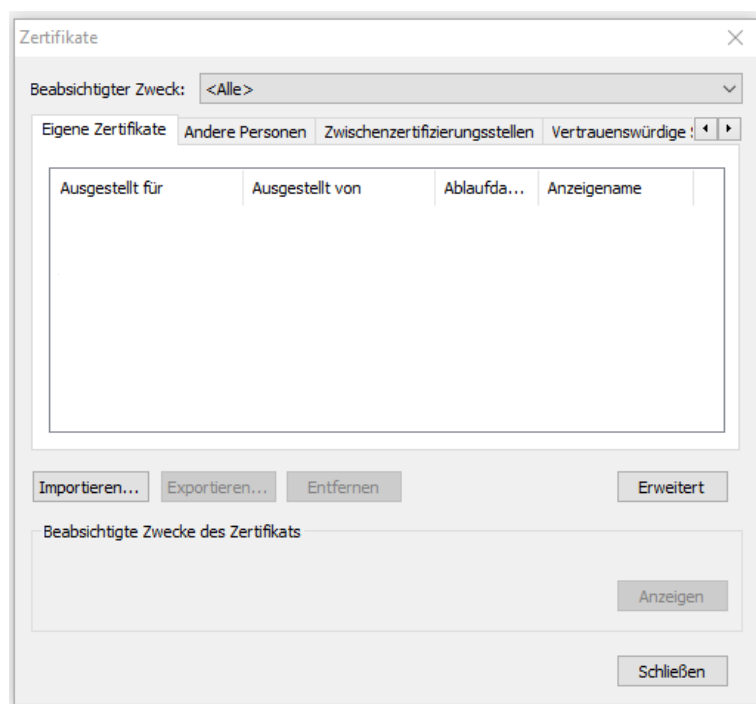
Öffnen Sie den Microsoft Edge Browser und wählen Sie über die drei Punkte in der rechten, oberen Ecke das Menü aus. Klicken Sie anschließend auf den Punkt "Einstellungen".



Im Einstellungsmenü navigieren Sie zu der Unterseite "Datenschutz, Suche und Dienste". Scrollen Sie nach unten, bis Sie die Sicherheitseinstellungen finden, und klicken auf den Button "Zertifikate verwalten".

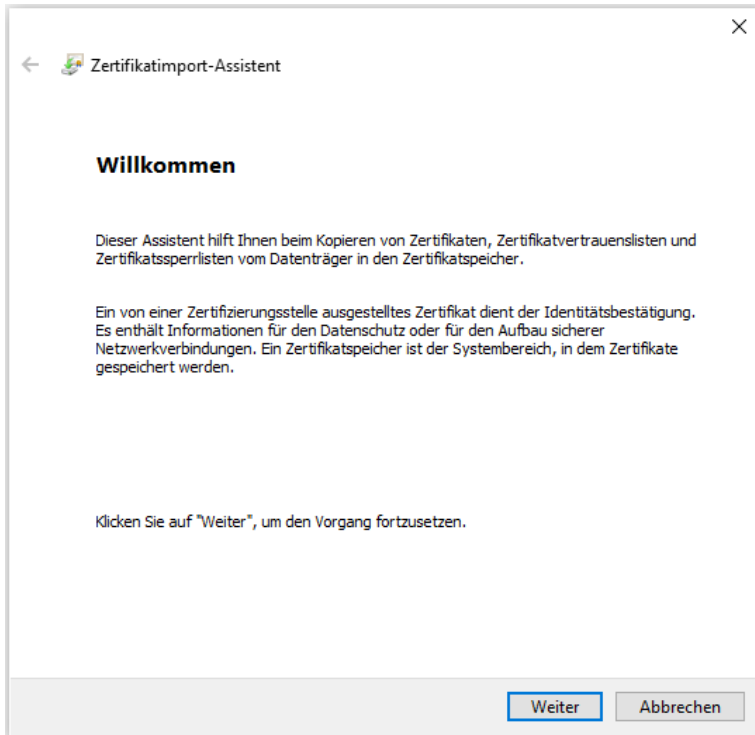


Das Fenster "Zertifikate" öffnet sich.

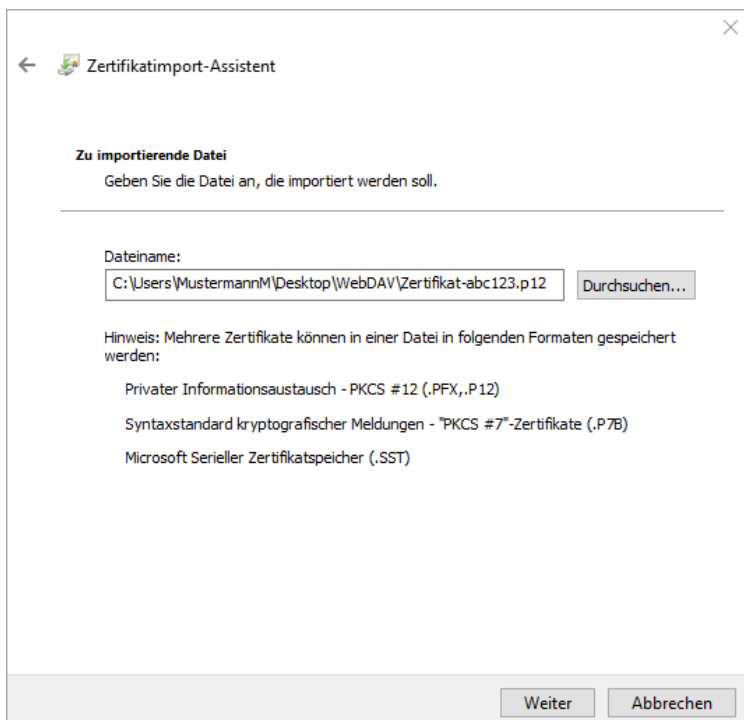


Sollten sich hier noch "alte" oder abgelaufene Zertifikate befinden, sind diese über die Schaltfläche Entfernen zu löschen. Sie erkennen diese über das angezeigte Datum in der Spalte „Ablaufdatum“. Anschließend wird mit Hilfe der Schaltfläche Importieren der Zertifikatsimport-Assistent gestartet.

Das erste Fenster kann einfach mit Weiter bestätigt werden.



Nun kann die Importdatei ausgewählt werden. Wurde der Import-Assistent per Doppelklick auf die .p12-Datei gestartet, ist hier automatisch ein entsprechender Pfad hinterlegt (dieser muss nicht mehr geändert werden). Wurde der Assistent über das beschriebene Zertifikats-Fenster aufgerufen, muss die vorher gespeicherte .p12-Datei ausgewählt werden. Beim Durchsuchen empfiehlt sich nach Alle Dateien (\*.\*) zu suchen.



Im folgenden Fenster wird das Passwort für das Zertifikat eingegeben, das Sie aus der zweiten E-Mail entnehmen können. Das eingegebene Kennwort wird später auch für die Nutzung des Zertifikates benötigt. Weiterhin muss Hohe Sicherheit angehakt werden.

Nach der Eingabe des Kennwortes Weiter drücken.

← 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

Weiter   Abbrechen

"Zertifikatsspeicher automatisch auswählen (auf dem Zertifikattyp basierend)" auswählen und auf Weiter klicken.

← Zertifikatimport-Assistent

**Zertifikatsspeicher**  
Zertifikatsspeicher sind Systembereiche, in denen Zertifikate gespeichert werden.

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

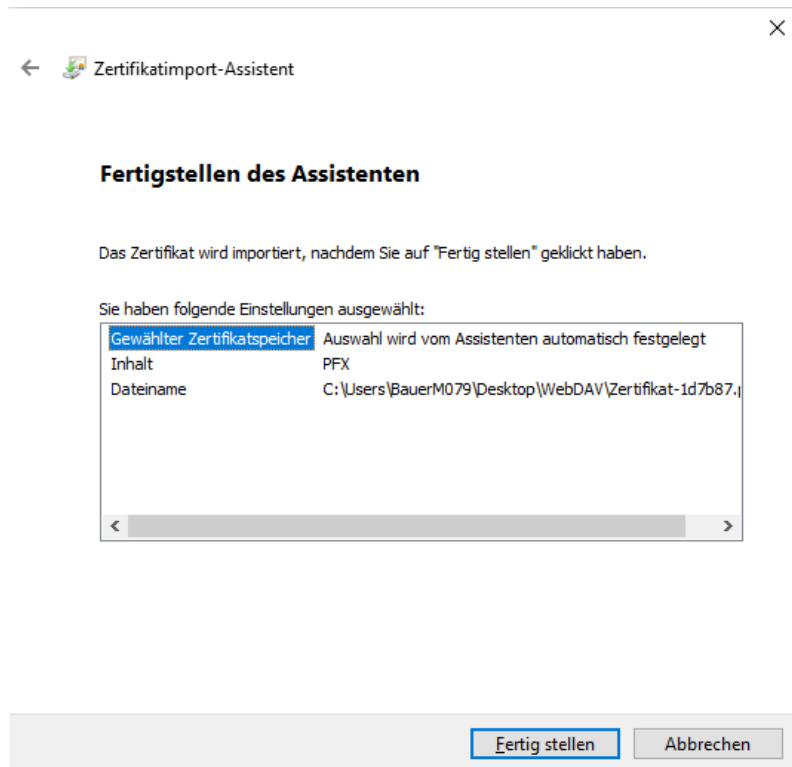
☒ Zertifikatsspeicher automatisch auswählen (auf dem Zertifikattyp basierend)

☐ Alle Zertifikate in folgendem Speicher speichern

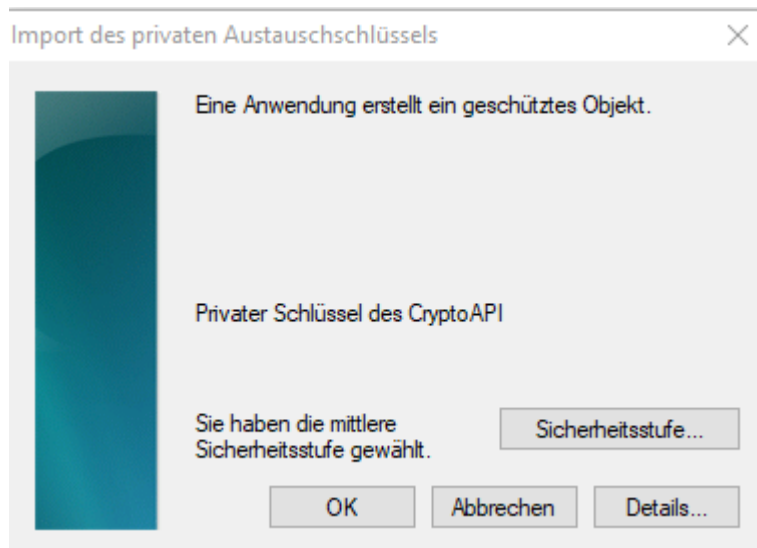
Zertifikatsspeicher:

Weiter   Abbrechen

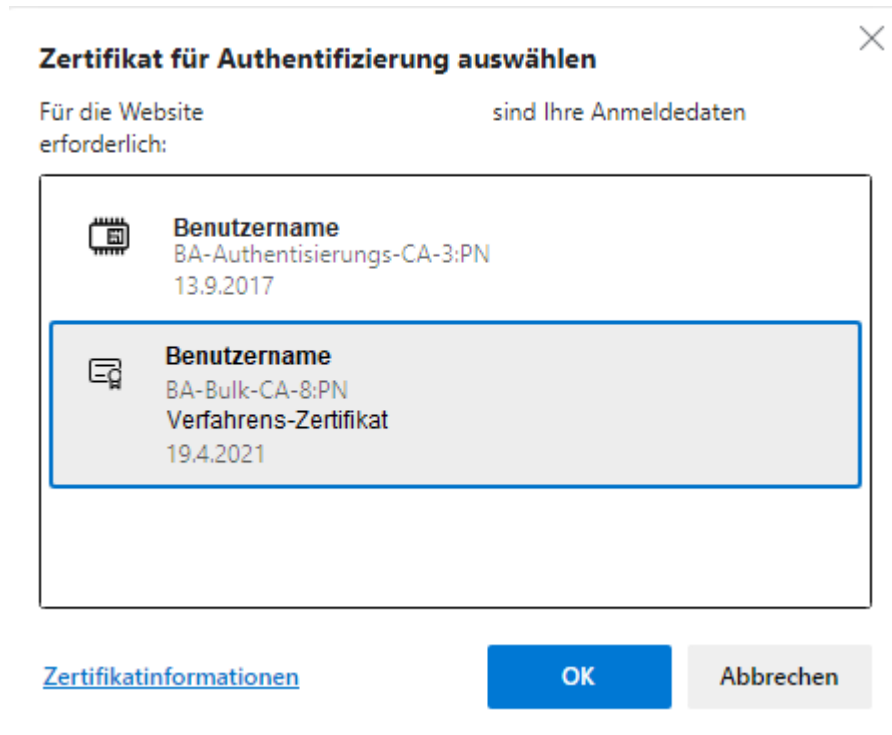
Im folgenden Fenster auf Fertig stellen drücken.



Im folgenden Fenster OK drücken und die Meldung über den erfolgreichen Import ebenfalls mit OK bestätigen. Nun ist das Zertifikat importiert.



**Wichtiger Hinweis:** Für die Authentifizierung im Microsoft Edge Browser geben Sie zunächst die Adresse des Verfahrens in die Adresszeile des Browsers sein. Im nächsten Fenster wählen Sie das installierte Client-Zertifikat aus der Übersicht aus und bestätigen die Auswahl mit "OK".



Anschließend öffnet sich die Oberfläche im Browser.

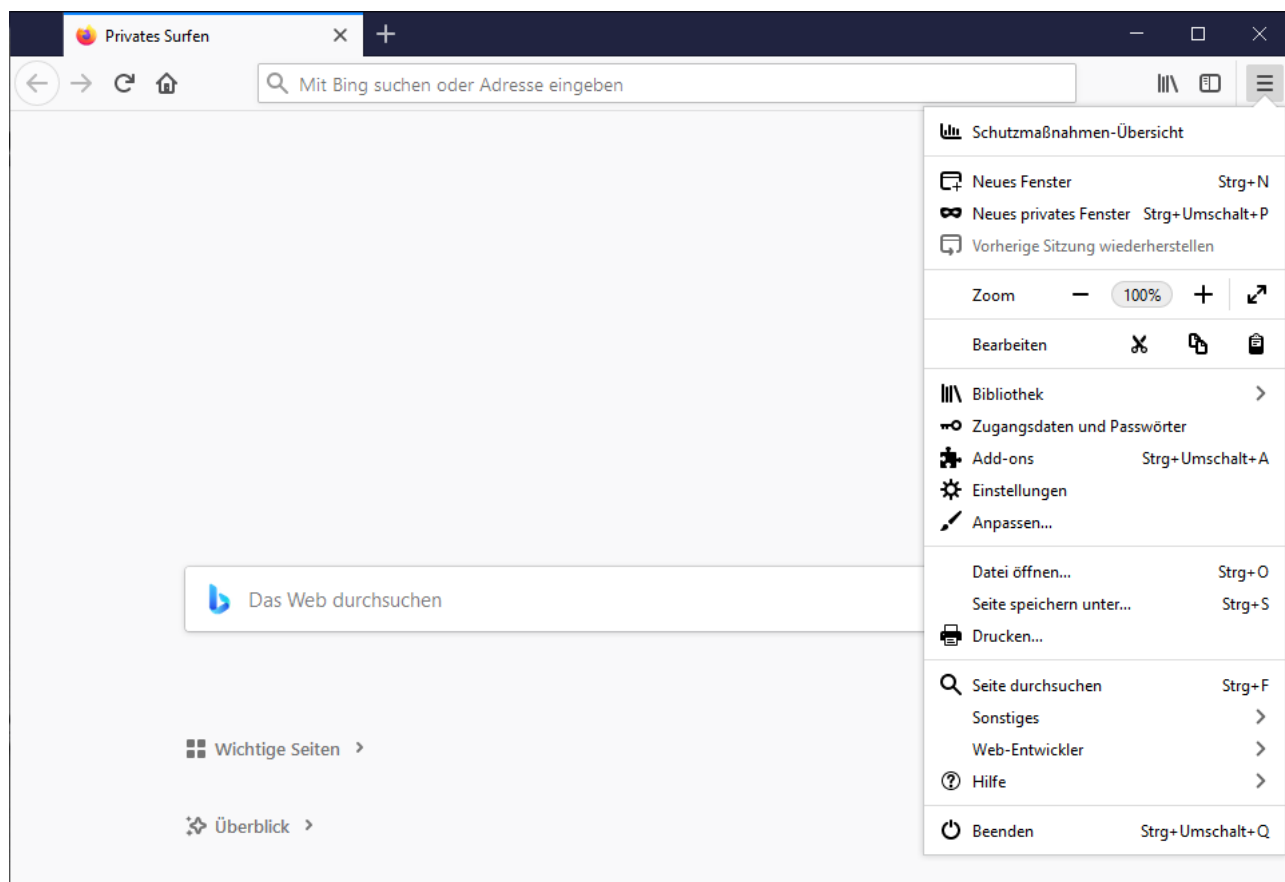


## Mozilla Firefox

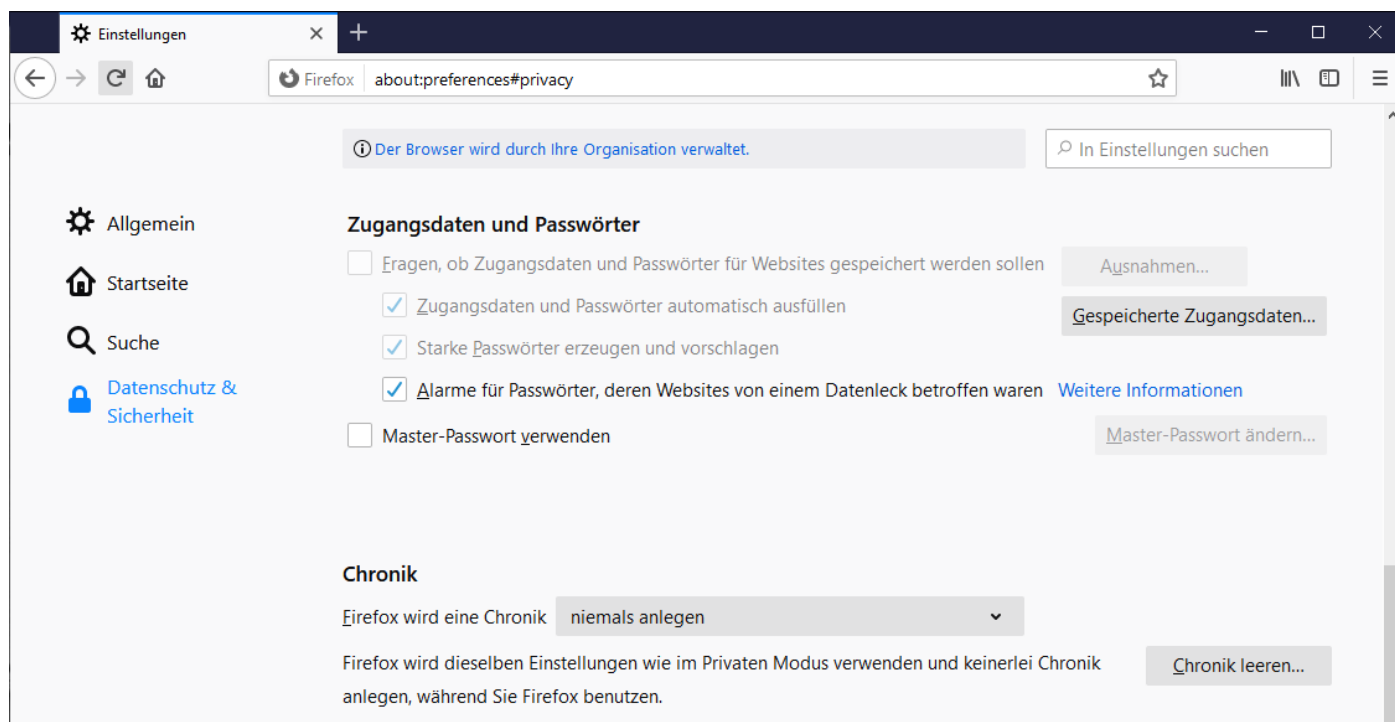
Die folgende Anleitung beschreibt das Vorgehen für die Installation der Zertifikatsdatei für den Mozilla Firefox Browser.

Bevor das per E-Mail eingegangene Zertifikat installiert werden kann, muss die per Mail erhaltene „p12“-Datei an einem beliebigen Ort abgespeichert werden. Laden Sie sich dazu die entsprechende Datei mit dem Link aus der E-Mail herunter. Nachdem Sie das erledigt haben, erhalten Sie in einer weiteren Mail ein Passwort, das Sie im weiteren Verlauf benötigen.

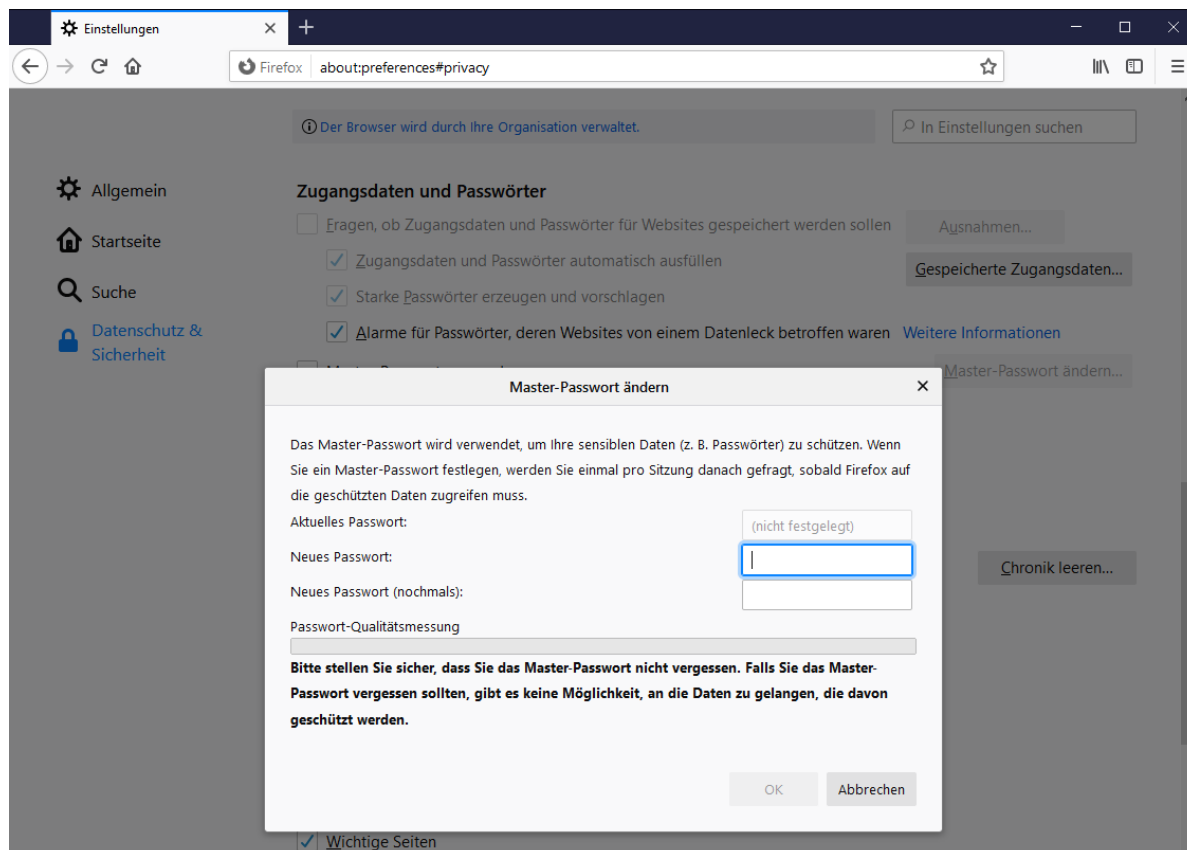
Öffnen Sie den Firefox-Browser und wählen Sie über die drei Striche in der rechten, oberen Ecke das Menü aus. Klicken Sie anschließend auf den Punkt "Einstellungen".



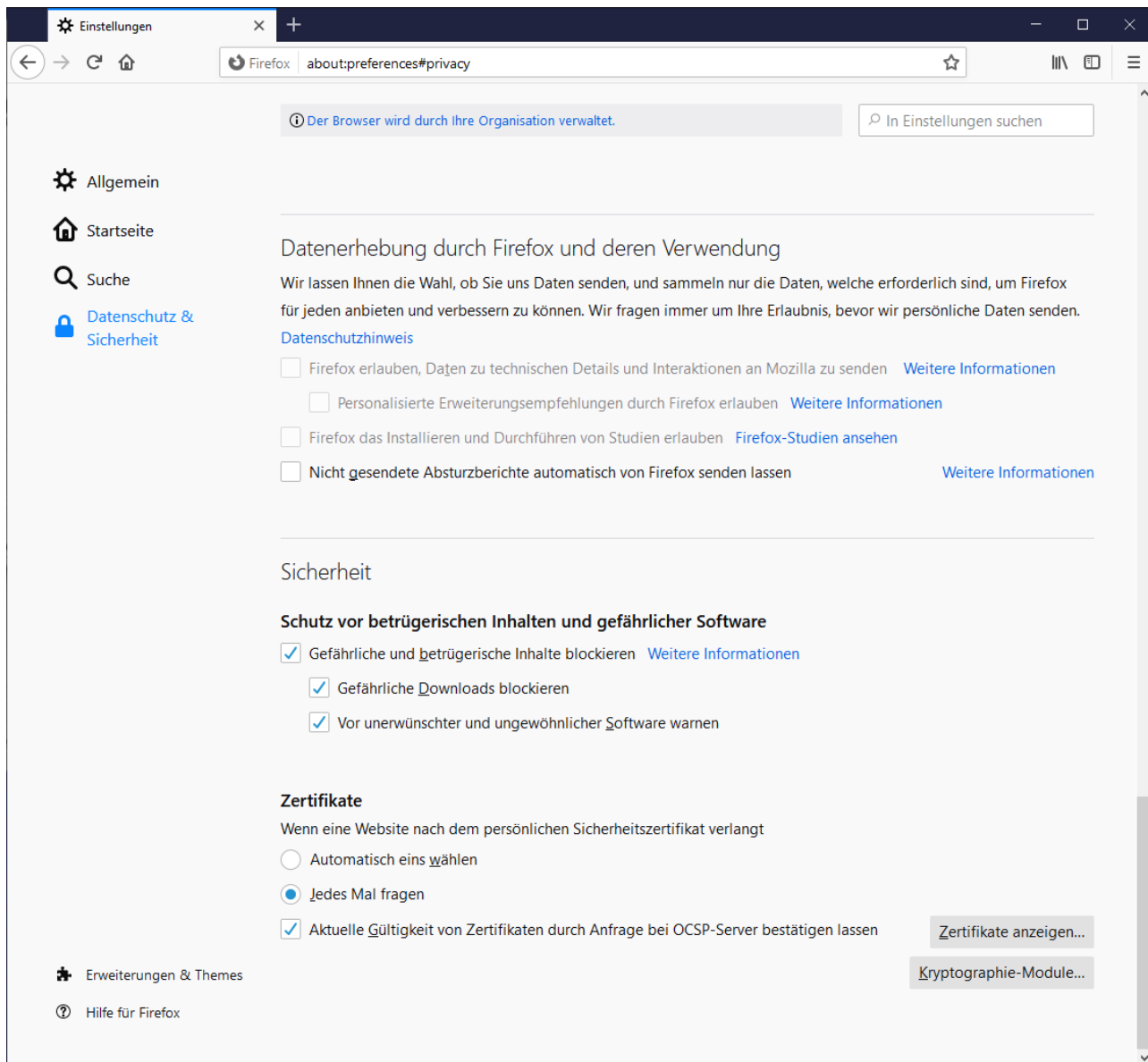
Im Einstellungsmenü navigieren Sie zu der Unterseite Datenschutz & Sicherheit und setzen den Haken für die Option "Master Passwort verwenden".



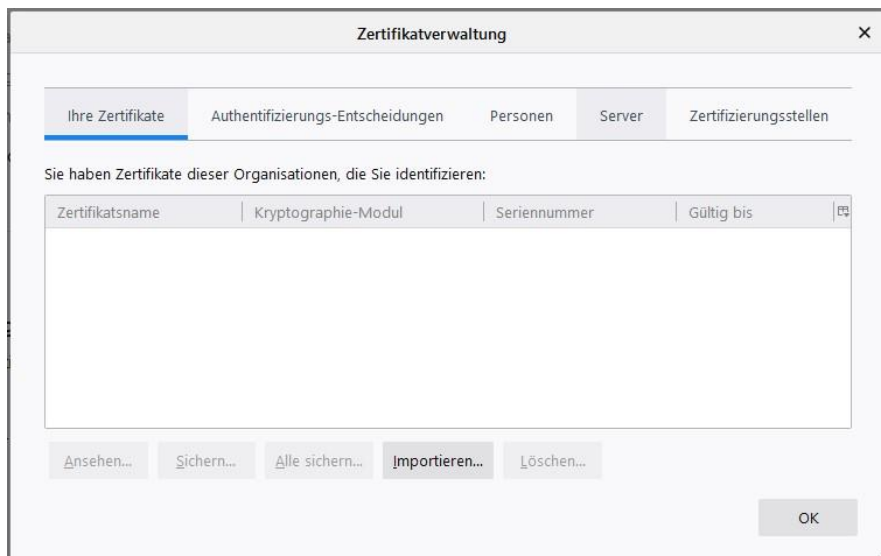
Anschließend müssen Sie, sofern dies noch nicht erfolgt ist, ein neues Master-Passwort vergeben. Sollten Sie bereits ein Master-Passwort für Ihren Firefox verwenden, können Sie diesen Schritt überspringen. Bitte beachten Sie die Warnmeldung des Browsers.



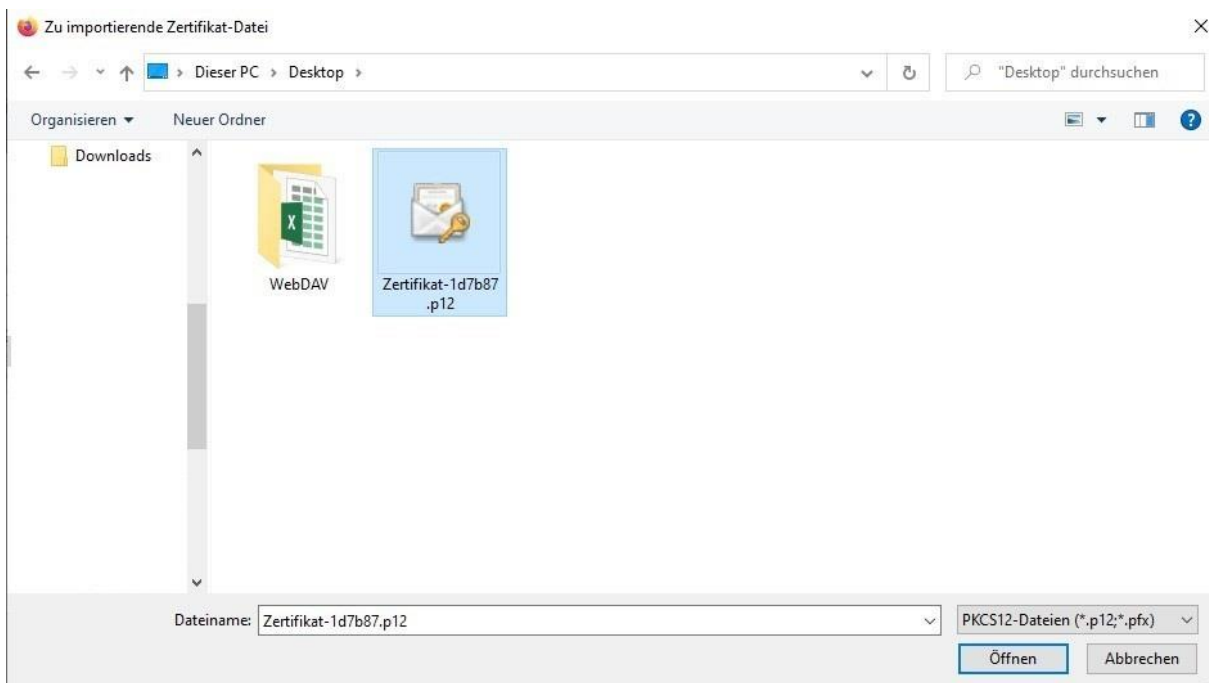
Nachdem das Master-Passwort vergeben wurde, scrollen Sie jetzt bis an das Ende des Menüs und wählen den Punkt "Zertifikate Anzeigen" aus.



In dem neu geöffneten Fenster wählen Sie bitte zunächst den Reiter "Ihre Zertifikate" aus. Sollten sich hier noch "alte" oder abgelaufene Zertifikate befinden, sind diese über die Schaltfläche "Löschen..." zu entfernen. Anschließend wird mit Hilfe der Schaltfläche "Importieren..." der Zertifikatsimport gestartet.



Für den Importvorgang wird die zuvor abgespeicherte Zertifikatsdatei benötigt. Bitte navigieren Sie zum gewählten Speicherort der .p12-Datei aus der E-Mail, wählen diese aus und bestätigen den Vorgang mit "Öffnen".



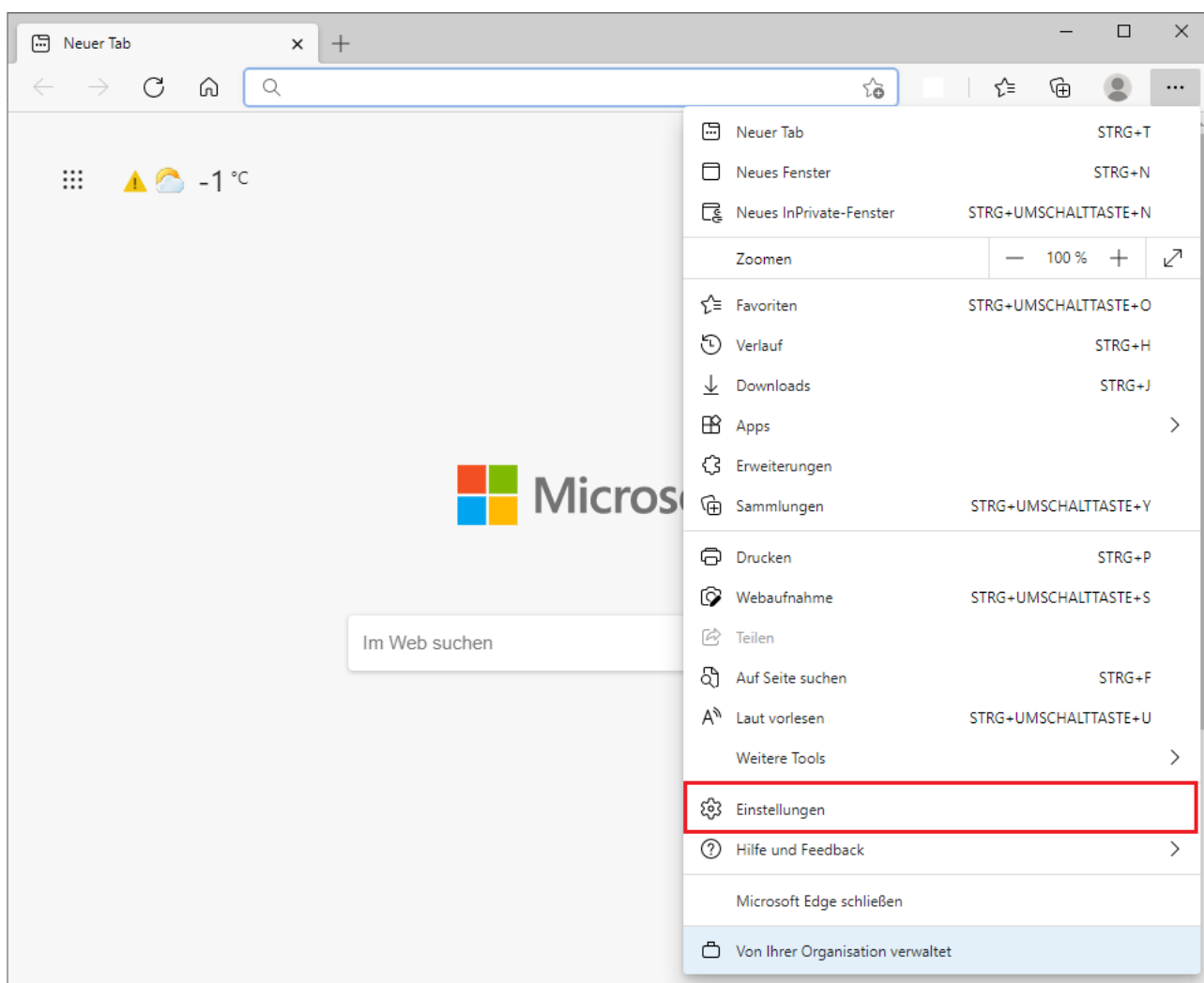
Sie werden jetzt aufgefordert, ein Kennwort einzugeben. Tragen Sie das Kennwort aus der zweiten E-Mail vollständig in das Kennwortfeld ein und bestätigen die Eingabe mit "OK". Wurde das Kennwort korrekt eingegeben, schließt sich das Dialogfenster und Sie finden das installierte Zertifikat in der Liste "Ihre Zertifikate". Mit einem Klick auf "OK" gelangen Sie zurück in das Optionsmenü. Die Installation ist hiermit abgeschlossen und Sie können den Zugriff testen.

## 2 Zugriff verlängern / Zertifikat löschen

Wurde Ihr bereits bestehendes und installiertes Client-Zertifikat verlängert, ändern sich ein paar Schritte bei der Installation des neuen Zertifikates. Damit der Zugriff authentifiziert werden kann, muss zuerst das "alte" Zertifikat entfernt und anschließend das neue Zertifikat importiert werden.

### Microsoft Edge

Öffnen Sie den Microsoft Edge Browser und wählen Sie über die drei Punkte in der rechten, oberen Ecke das Menü aus. Klicken Sie anschließend auf den Punkt "Einstellungen".



Im Einstellungsmenü navigieren Sie zu der Unterseite "Datenschutz, Suche und Dienste". Scrollen Sie nach unten, bis Sie die Sicherheitseinstellungen finden, und klicken auf den Button "Zertifikate verwalten".

## Sicherheit

Verwalten der Sicherheitseinstellungen für Microsoft Edge

### Zertifikate verwalten

HTTPS-/SSL-Zertifikate und -Einstellungen verwalten

### Microsoft Defender SmartScreen

Mein Gerät mit Microsoft Defender SmartScreen vor schädlichen Websites und Downloads schützen

### Potenziell unerwünschte Apps blockieren

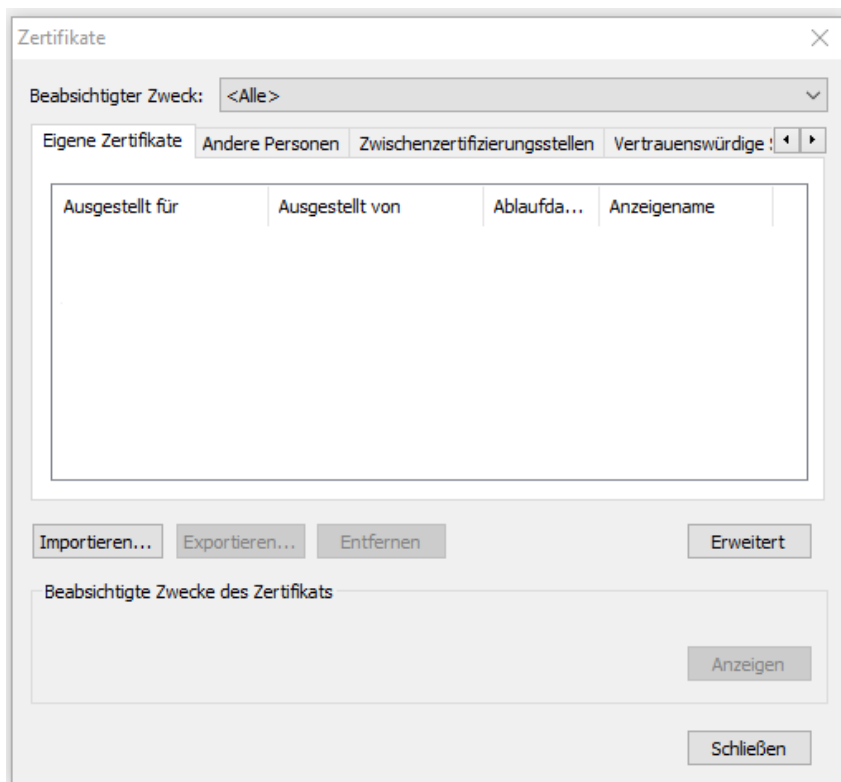
Blockiert Downloads von nicht vertrauenswürdigen Apps, die ggf. zu unerwartetem Verhalten führen.

### 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.

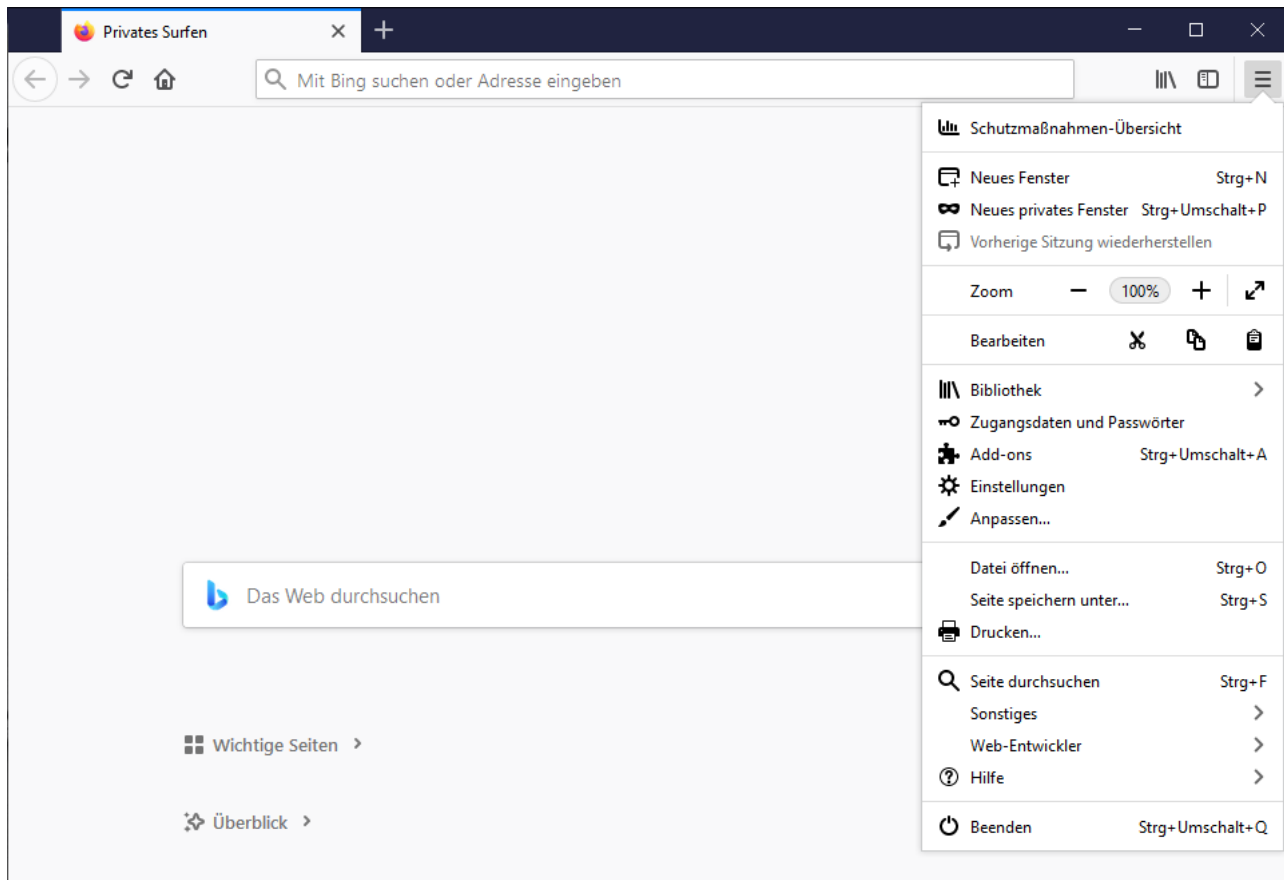
Das Fenster "Zertifikate" öffnet sich.

- Wählen Sie das alte Zertifikat aus (zu Erkennen am überschrittenen Ablaufdatum) und löschen Sie dieses mit einem Klick auf "Entfernen"
- Anschließend führen Sie die Installation des neuen Zertifikates durch wie es im Kapitel "Zugriff einrichten" für den Microsoft Edge beschrieben ist.

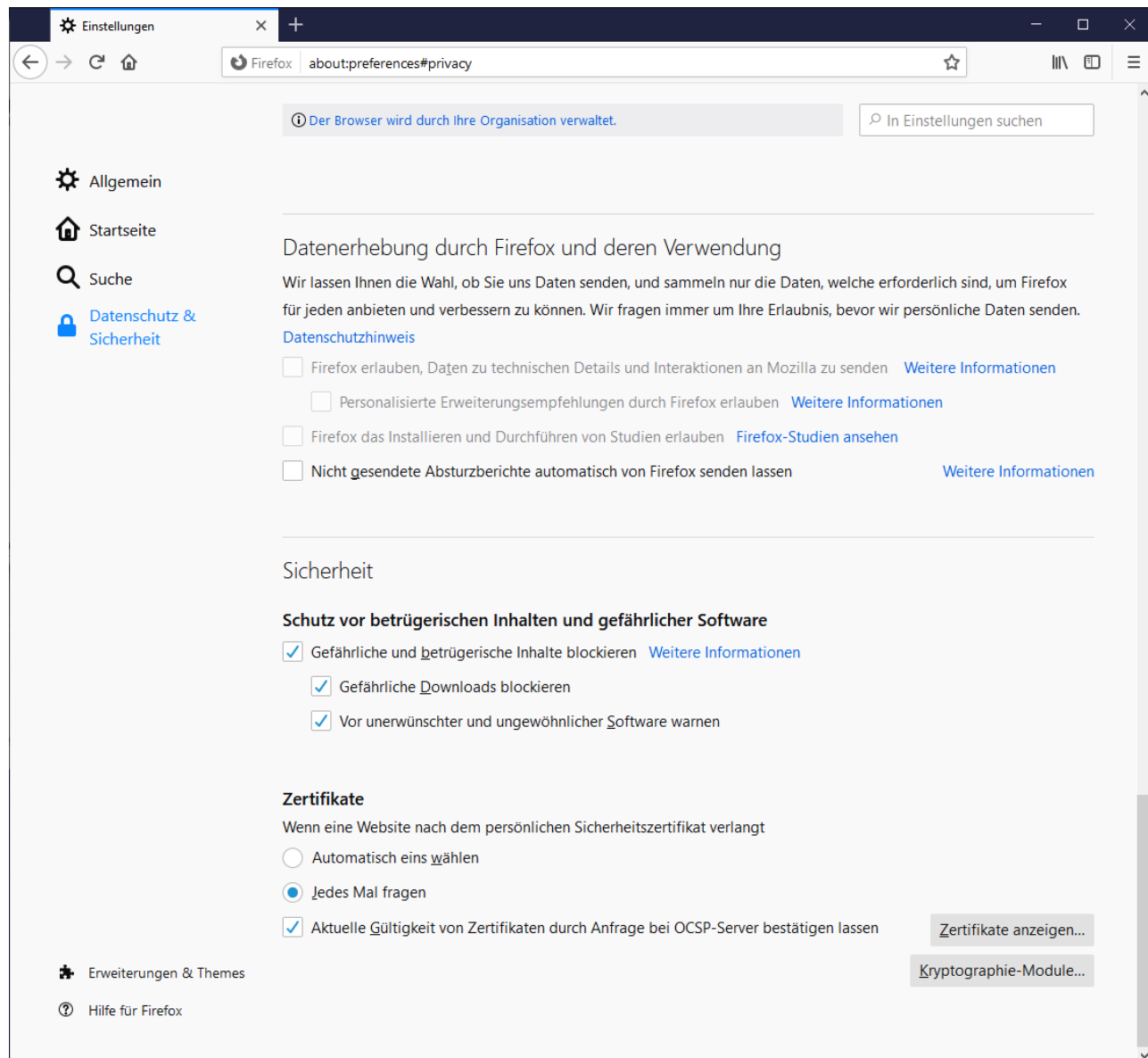


## Mozilla Firefox

Öffnen Sie den Firefox-Browser und wählen Sie über die drei Striche in der rechten, oberen Ecke das Menü aus. Klicken Sie anschließend auf den Punkt "Einstellungen".



Scrollen Sie jetzt bis an das Ende des Menüs und wählen den Punkt "Zertifikate anzeigen" aus.

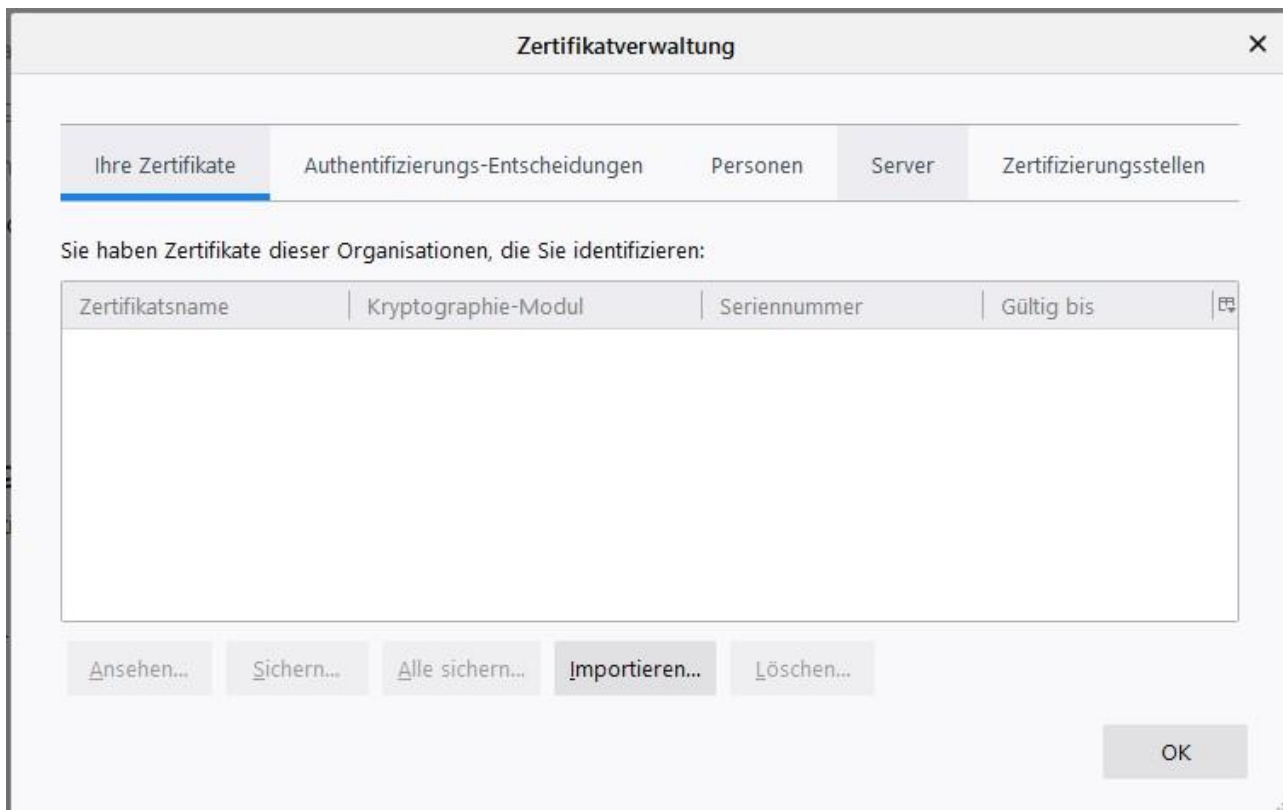


Hinweis: Sollten Sie noch kein Master-Passwort gesetzt haben, schauen Sie im Kapitel "Zugriff einrichten", wie Sie das Master Passwort für den Mozilla Firefox vergeben können.



In dem neu geöffneten Fenster wählen Sie bitte zunächst den Reiter "Ihre Zertifikate" aus.

- Wählen Sie das alte Zertifikat aus (zu Erkennen am überschrittenen Ablaufdatum in der Spalte "Gültig bis") und löschen Sie es mit einem Klick auf "Löschen..."
- Anschließend führen Sie die Installation des neuen Zertifikates durch wie es im Kapitel "Zugriff einrichten" für den Mozilla Firefox beschrieben ist.



## 3 Fehlerquellen und mögliche Behebungsansätze

In diesem Abschnitt finden Sie einige mögliche Fehlerquellen und passende Lösungsansätze zu Ihrem Zugriff über das Client-Zertifikat. Die folgenden Inhalte richten sich zum Teil an erfahrene Nutzer bzw. Administratoren und enthalten daher Fachbegriffe, die nicht weiter erläutert werden. Eine ausführliche Beschreibung und Dokumentation jedes Vorganges ist jedoch gegeben.

### Bekannte Fehler

Folgende Fehlermeldungen sind im Zusammenhang mit Client-Zertifikaten bekannt:

- Die Seite kann nicht aufgerufen werden – Fehler bei der Authentifizierung
- Zugriff verweigert
- Objekt nicht gefunden
- Hmm... diese Seite ist leider nicht erreichbar

Die unten beschriebenen Lösungsansätze sollten, unabhängig von der Fehlermeldung, Schritt für Schritt geprüft werden.

### Lösungsansätze

#### Installation der Zertifikatsdatei überprüfen

Überprüfen Sie, ob das Client-Zertifikat korrekt installiert ist und keine weiteren (möglicherweise abgelaufenen) Zertifikate für den Zugriff installiert sind. Dies können Sie im Zertifikatsmanager einsehen, welchen Sie bereits bei der Einrichtung des Zertifikates aufgerufen haben.

- Für Microsoft Edge: Unter Einstellungen, Datenschutz, Suche und Dienste, Sicherheit, Zertifikate verwalten
- Für Mozilla Firefox: Unter Einstellungen, Datenschutz & Sicherheit, Zertifikate Anzeigen, Ihre Zertifikate



## SSL-Status (Cache-Speicher) zurücksetzen

Den Zwischenspeicher des Browsers zu löschen ermöglicht dem Client-Zertifikat, eine neue Authentifizierungsanfrage zu senden, sollten vorherige Zugriffsversuche nicht erfolgreich gewesen sein. Dies kann insbesondere bei einem "Fehler bei der Authentifizierung" helfen.

- Für Microsoft Edge: Unter Einstellungen, Datenschutz, Suche und Dienste, Browserdaten für Internet Explorer löschen, bestätigen mit Löschen
- Anschließend den Browser neustarten und die Verbindung erneut testen
- Für Mozilla Firefox: Unter Einstellungen, Datenschutz & Sicherheit, Cookies und Website-Daten, Daten entfernen, Leeren
- Anschließend den Browser neustarten und die Verbindung erneut testen

## Überprüfen des Eingabedialoges

Bei einem erfolgreichen Zugriff erscheint das Eingabedialog-Fenster für die Auswahl des Client-Zertifikates im Hintergrund. Es verbirgt sich oftmals hinter dem geöffneten Browser-Fenster und wird nicht in der Windows-Oberfläche hervorgehoben, kann jedoch in der Taskleiste oder durch das Minimieren anderer Fenster gefunden werden. Erfolgt die Auswahl des Zertifikates nicht schnell genug, wird der Zugriff automatisch abgelehnt, obwohl das Zertifikat korrekt installiert wurde.

## Überprüfen, ob das Client-Zertifikat übertragen wird

Lassen Sie von Ihrem IT-Administrator prüfen, ob noch weitere Freischaltungen innerhalb der Infrastruktur notwendig sind. Gegebenenfalls wird die Installation des Client-Zertifikates erlaubt, allerdings die Verwendung im Internet unterbunden. Es kann notwendig sein, dass die Adresse in entsprechende Ausnahmelisten am Gateway-Virenschanner oder anderen zentralen Komponenten hinterlegt werden muss.