

Zertifikatsverwaltung

unter Windows im Edge

Stand: 16.01.2023

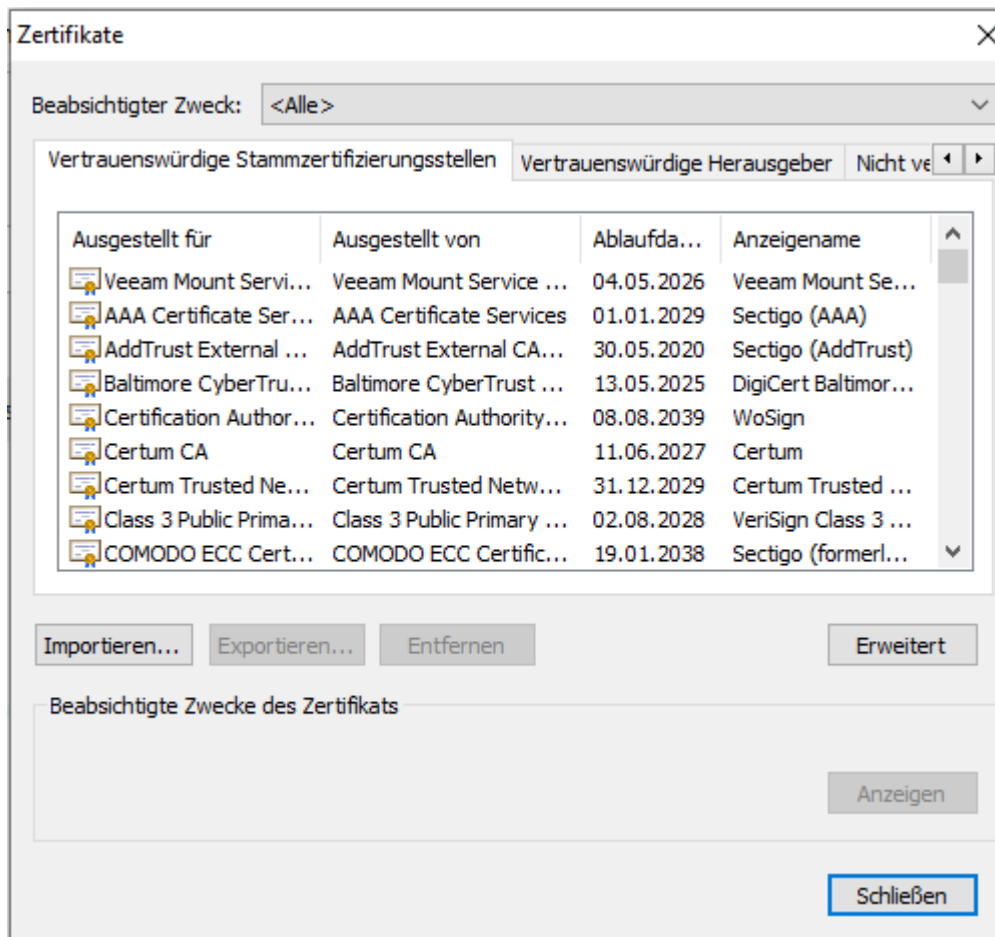
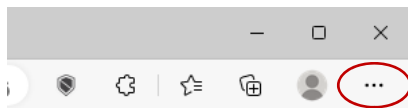
Inhalt

- | | |
|--|---|
| 1. Windows-Zertifikatsspeicher | 2 |
| 2. Export des eigenen Zertifikats mit privatem Schlüssel | 4 |
| 3. Eigenes Zertifikat einbinden für die Signierung | 5 |
| 4. Zertifikate anderer Personen importieren | 6 |

1. Windows-Zertifikatsspeicher

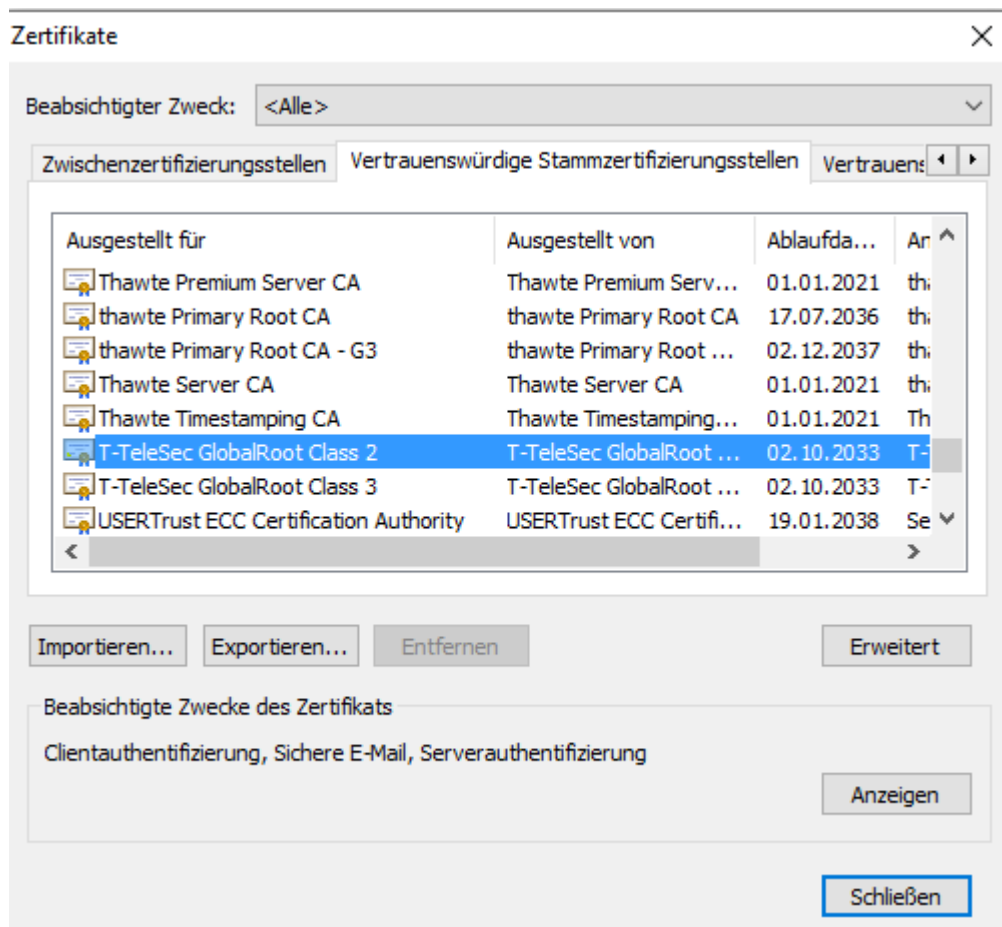
Alle Office-Anwendungen und Adobe Produkte nutzen für Ihre Zertifikatsverwaltung den Windows-Zertifikatsspeicher.

Die Verwaltung der Zertifikate erfolgt im Edge über das Menü ... in der rechten oberen Ecke -> „Einstellungen“ -> „Datenschutz, Suche und Dienste“ -> „Zertifikate verwalten“.



Die Registerfelder des Zertifikatsspeichers dienen zur Sortierung der Zertifikate.

- *Eigene Zertifikate*,
hier sind die eigenen Zertifikate hinterlegt, zu dem ein privater Schlüssel vorhanden ist.
- *Andere Personen*,
dies sind die öffentlichen Zertifikate von anderen Personen und Server, die eine verschlüsselte Verbindung nutzen.
- *Zwischenzertifizierungsstellen*,
Zertifikate der Zertifizierungsstellen, hier sollte das HS-Harz-CA Zertifikat zu finden sein.
- *Vertrauenswürdige Stammzertifizierungsstellen*,
Zertifikate für die Stammzertifizierungsstellen, hier sollte das Telecom Root-Zertifikat hinterlegt sein.
- *Vertrauenswürdige Herausgeber*
- *Nicht vertrauenswürdige Herausgeber*



Die nötige Zertifikatskette der HS-Harz-CA kann über das Webfrontend G2 heruntergeladen werden: https://pki.pca.dfn.de/dfn-ca-global-g2/cgi-bin/pub/pki?cmd=getStaticPage;name=index;id=2&RA_ID=2620

Die entsprechenden Buttons anklicken, dann wird das Zertifikat im Browser automatisch installiert.

2. Export des eigenen Zertifikats mit privatem Schlüssel

Für den Export in der Registerkarte „*Eigene Zertifikate*“ müssen Sie das gewünschte Zertifikat markieren und auf „*Exportieren*“ klicken. Es öffnet sich der Zertifikatsexport-Assistent. Beim Export sollten Sie darauf achten, dass die Häkchen „*Privaten Schlüssel exportieren*“ und „*alle Zertifikate im Zertifizierungspfad einbeziehen*“ gesetzt sind. Durchlaufen Sie die Schritte des Assistenten (Kennwort eingeben, Namen vergeben und klicken Sie am Ende auf „*Fertig stellen*“, um die Datei im pfx Format zu sichern.


← Zertifikatsexport-Assistent

Privaten Schlüssel exportieren

Sie können den privaten Schlüssel mit dem Zertifikat exportieren.

Private Schlüssel sind kennwortgeschützt. Wenn Sie den privaten Schlüssel mit dem ausgewählten Zertifikat exportieren möchten, müssen Sie auf einer der folgenden Seiten ein Kennwort eingeben.

Möchten Sie mit dem Zertifikat auch den privaten Schlüssel exportieren?

-  Ja, privaten Schlüssel exportieren
 Nein, privaten Schlüssel nicht exportieren

Weiter


Abbrechen

← Zertifikatsexport-Assistent

Format der zu exportierenden Datei

Zertifikate können in verschiedenen Dateiformaten exportiert werden.

Wählen Sie das gewünschte Format:

- DER-codiert-binär X.509 (.CER)
 Base-64-codiert X.509 (.CER)
 Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)
 Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
 Privater Informationsaustausch - PKCS #12 (.PFX)
 Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
 Privaten Schlüssel nach erfolgreichem Export löschen
 Alle erweiterten Eigenschaften exportieren
 Zertifikatdatenschutz aktivieren
 Microsoft Serieller Zertifikatspeicher (.SST)

Weiter

Abbrechen

3. Eigenes Zertifikat einbinden für die Signierung von Dokumenten

Eigene Zertifikate werden zur digitalen Signierung von E-Mails oder Dokumenten genutzt. Hierzu muss ein privater Schlüssel vorhanden sein. Durch die Signierung wird die Herkunft und die Unverfälschtheit eines Dokuments bestätigt.

Um ein eigenes Zertifikat in den Windows-Zertifikatsspeicher zu importieren, muss eine *p12* oder *px* Datei vorliegen. Diese Art von Datei enthält den privaten Schlüssel sowie das öffentliche Zertifikat. Die Installation erfolgt ganz einfach durch doppelklicken der Zertifikatsdatei im Windows Explorer.

Es öffnet sich der Zertifikatsimport-Assistent, bitte hier den Anweisungen folgen. Die Einsortierung erfolgt automatisch, es muss nur das Passwort angegeben werden, mit dem die Datei geschützt wurde.

Wichtig: Schlüssel als exportierbar markieren anklicken. Nur dann kann der Private Schlüssel zu einem späteren Zeitpunkt exportiert werden.

← Zertifikatsimport-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

Nach Abschluss müsste das eigene Zertifikat in der entsprechenden Registerkarte zu finden sein und kann Windows-weit zur Signierung von Dokumenten genutzt werden.

4. Zertifikate anderer Personen importieren

Im [Webfrontend G2](#) können Zertifikate anderer Personen mit dem Edge installiert werden. Einfach über den Menüpunkt „Zertifikat suchen“ den Namen oder die gesuchte E-Mailadresse im Suchfeld eingeben.

The screenshot shows a navigation menu with tabs for 'Zertifikate', 'CA-Zertifikate', 'Gesperrte Zertifikate', 'Policies', 'Hilfe', and 'Beenden'. Below this is a sub-menu with 'Nutzerzertifikat', 'Serverzertifikat', 'Zertifikat sperren', and 'Zertifikat suchen'. The 'Zertifikat suchen' section contains the following text: 'Bitte geben Sie den exakten Namen (keine Umlaute) oder die exakte E-Mail-Adresse aus dem Zertifikat ein, das Sie suchen. Es werden maximal 20 Zertifikate angezeigt.' Below the text is a text input field labeled 'Name oder E-Mail-Adresse'. At the bottom of the form are two buttons: 'OK' and 'Zurücksetzen'.

Klicken Sie auf die kleine Grafik links um sich die Detailansicht anzeigen zu lassen. Wenn sie ganz nach unten Scrollen, können Sie dann das Zertifikat installieren. Oder klicken Sie direkt auf die Seriennummer, um es zu installieren.

The screenshot shows a table with the following data:

Seriennummer	Name	E-Mail	Rolle
908049248716881		hs-harz.de	User

Below the table, there is a section titled 'Operationen' with the following options:

- Zertifikat abspeichern (with a 'PEM' dropdown and a 'Download' button)
- Zertifikat in den Browser installieren (with an 'Installieren' button)

A red arrow points to an information icon (i) next to the serial number '908049248716881'.

Die Zertifikate auf der lokalen Festplatte können wie das eigene Zertifikat über den Windows Explorer installiert werden, durch doppeltes Anklicken.