▲ Hochschule Harz

Rechenzentrum

Zertifikatsverwaltung

unter Windows mit dem Internet Explorer

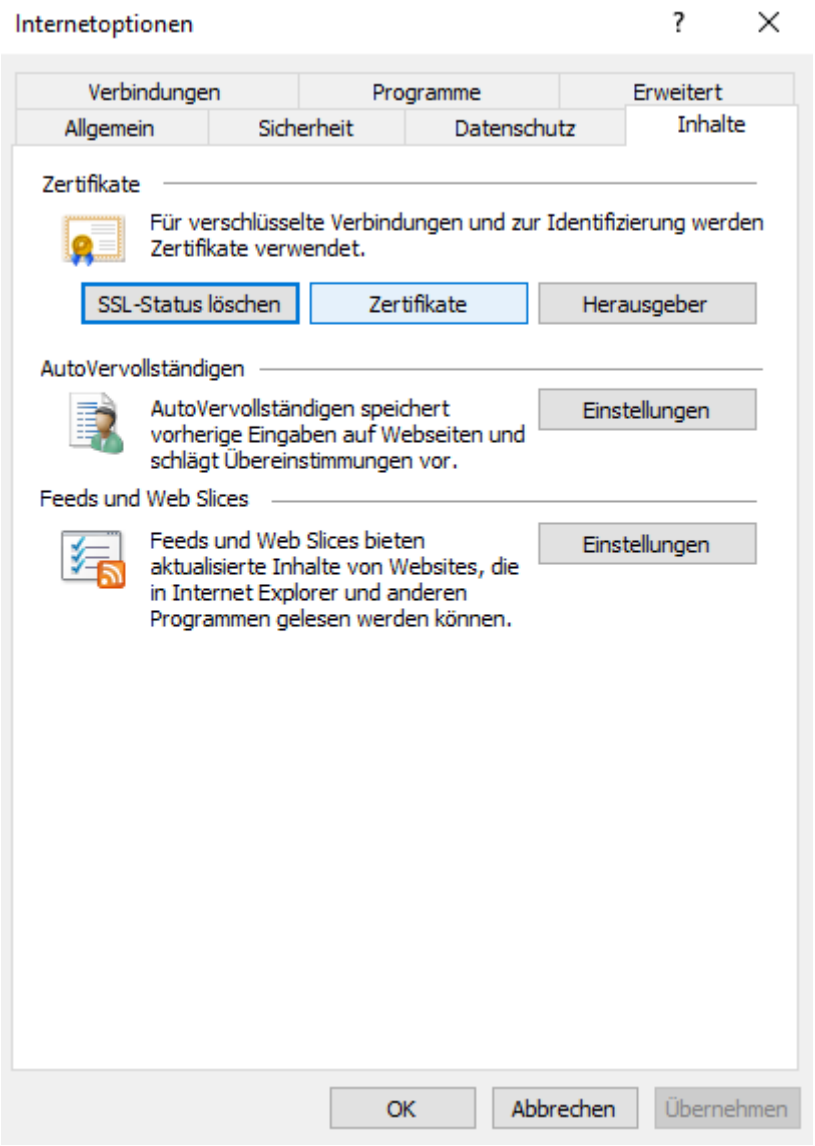
Stand: 12.10.2017

Inhalt

1. Windows-Zertifikatsspeicher

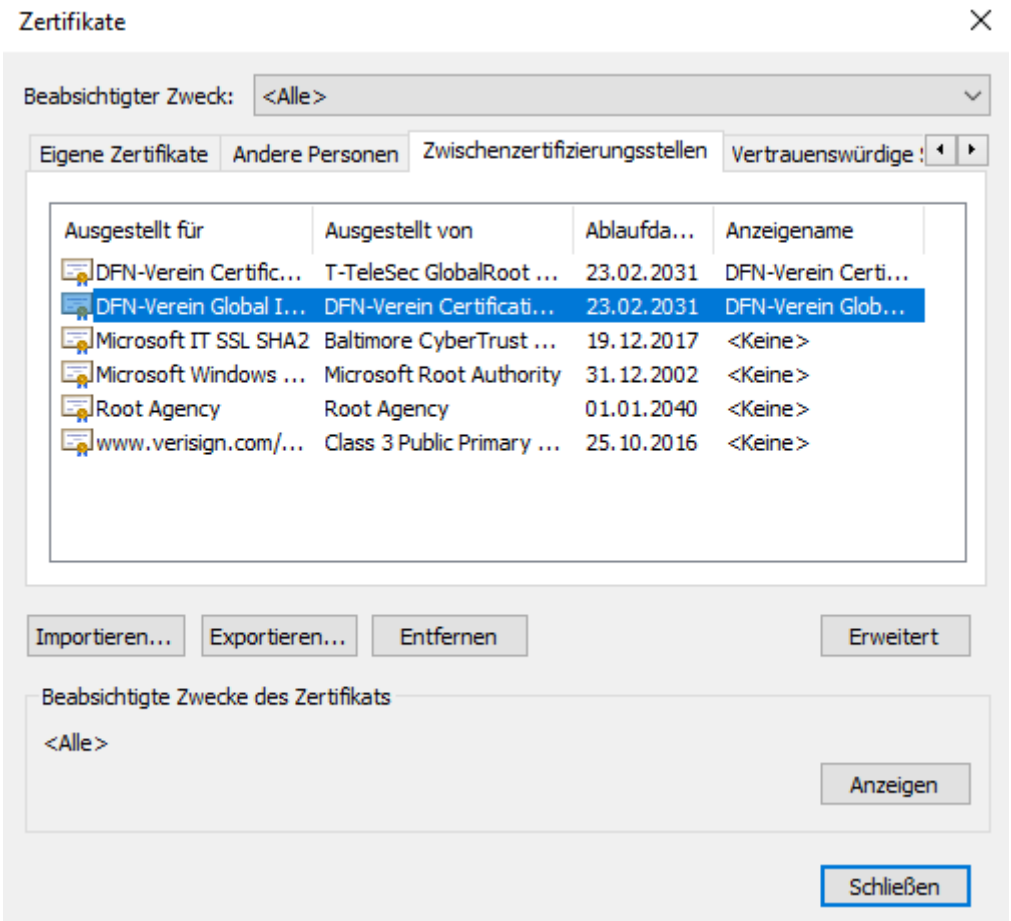
Alle Office-Anwendungen und Adobe Produkte nutzen für Ihre Zertifikatsverwaltung den Windows-Zertifikatsspeicher.

Die Verwaltung der Zertifikate erfolgt am besten über den Internet Explorer unter dem Menüpunkt „*Extras*“ -> „*Internetoptionen*“ -> *Registerkarte „Inhalte“* -> „*Zertifikate*“.



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*

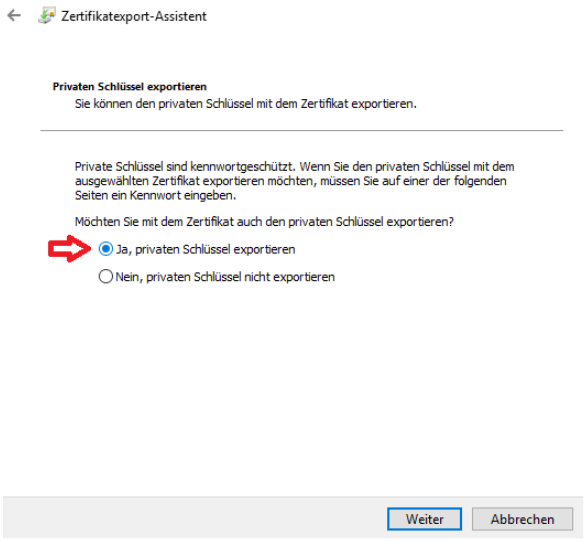


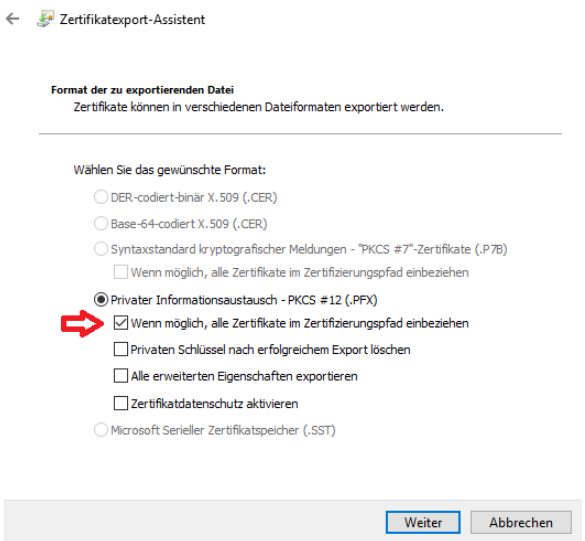
Die nötige Zertifikatskette der HS-Harz-CA kann über das Webfrontend G2 heruntergeladen werden: https://pki.pca.dfn.de/dfn-ca-global-g2/cgi-bin/pub/pki?cmd=getStaticPage;name=index;id=2&RA_ID=2620

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.



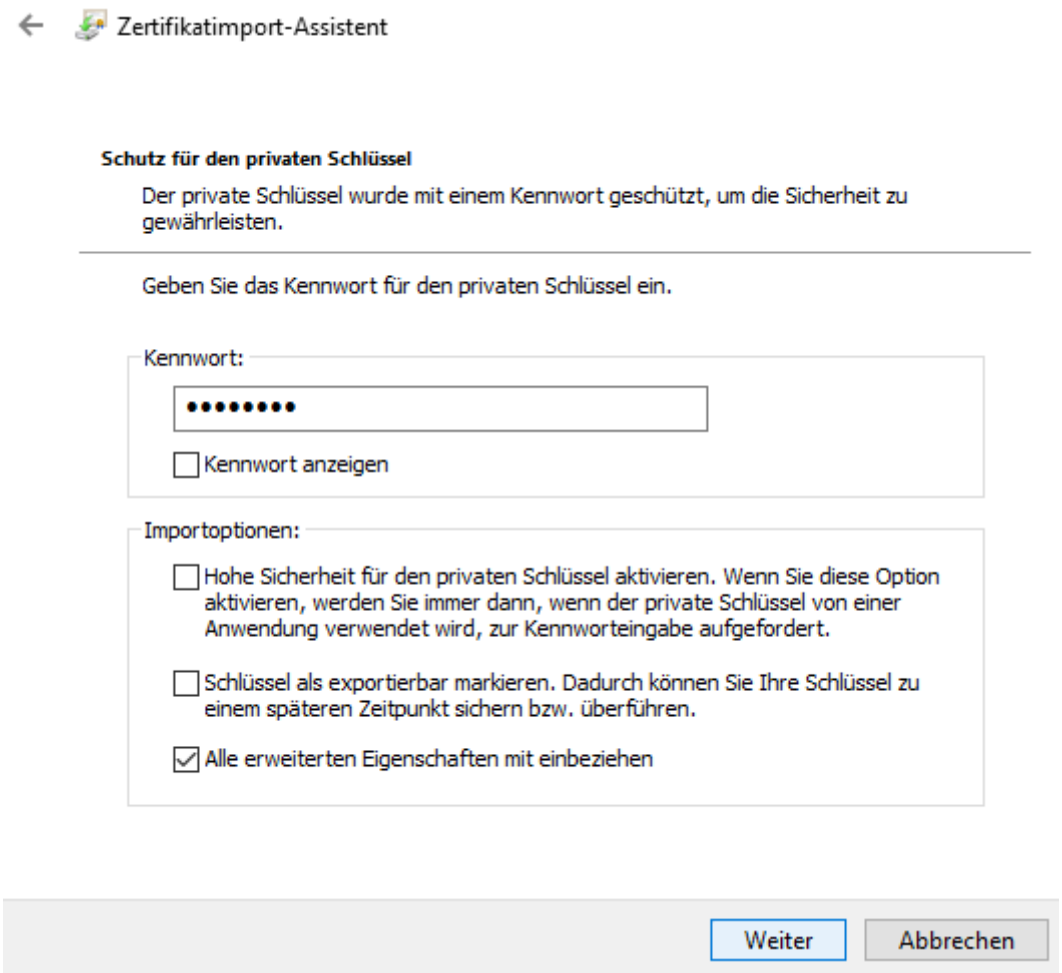


3. Eigenes Zertifikat einbinden für die Signierung

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 eines Dokuments bestätigt.

Um ein eigenes Zertifikat in den Windows-Zertifikatsspeicher zu importieren, muss eine *p12* oder *pfx* Datei vorliegen. Dieser Container enthält den privaten Schlüssel sowie das öffentliche Zertifikat. Die Installation erfolgt ganz einfach durch doppelt anklicken der Zertifikatsdatei im Windows Explorer.

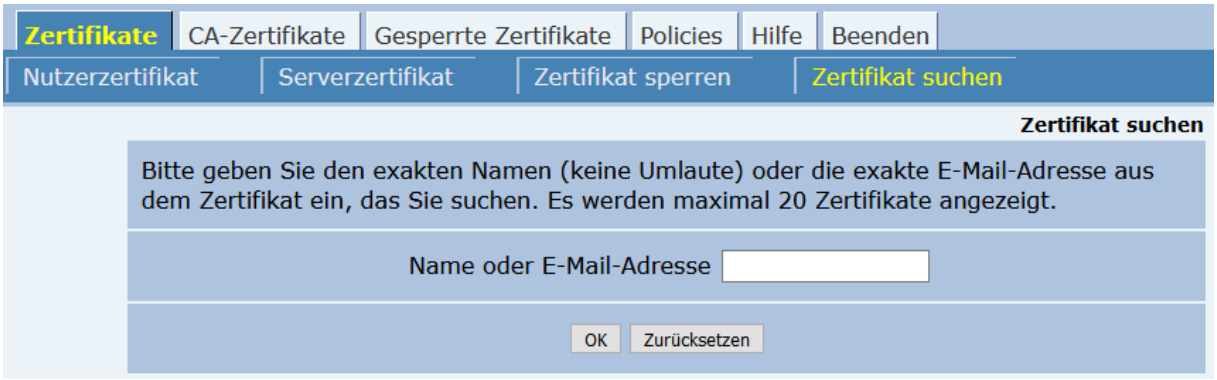
Es öffnet sich der Zertifikatsimport-Assistent, bitte hier den Anweisungen folgen. Die Einsortierung erfolgt automatisch, es muss nur das Passwort angegeben werden, mit dem die Datei geschützt wurde.



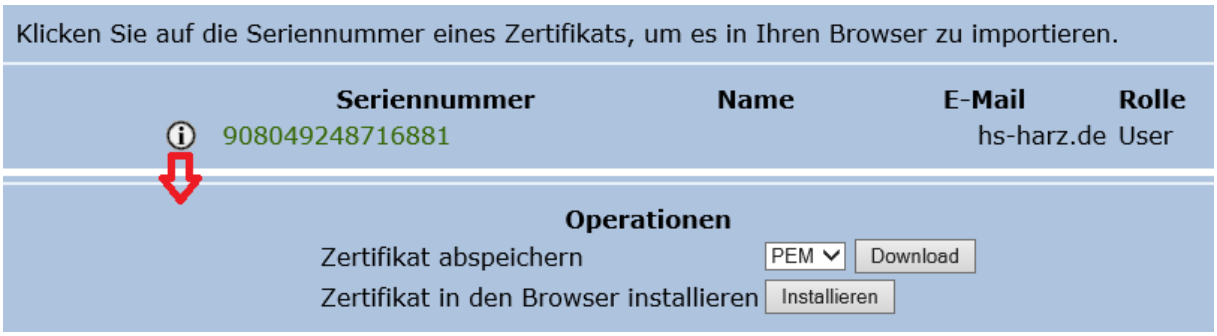
Nach Abschluss müsste das eigene Zertifikat in der entsprechenden Registerkarte zu finden sein und kann Windows-weit zur Signierung von Dokumenten und/oder E-Mail genutzt werden.

4. Zertifikate anderer Personen importieren

Im Webfrontend G2 können Zertifikate anderer Personen gedownloadet werden. Für die Installation im Windows am besten gleich den Internet Explorer nehmen. Einfach über den Menüpunkt *„Zertifikat suchen“* den Namen oder die gesuchte E-Mailadresse im Suchfeld eingeben.



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.



Die Zertifikate auf der lokalen Festplatte können wie das eigene Zertifikat über den Windows Explorer installiert werden, indem Sie sie doppelt anklicken.