Client Zertifikate im Browser installieren

Um Webdienste besser abzusichern können Client-Zertifikate eingesetzt werden. Ein Zertifikat ist dabei eine Datei, mit der sich ein Programm gegenüber dem Server ausweist. Diese Zertifikate sind personalisiert und ermöglichen einen Zugriff so zu gestalten, dass nur Personen mit gültigen Zertifikaten auf bestimmte Dienste zugreifen können.

Das kann beispielsweise eine Nextcloud-Instanz sein, in der sensible Daten liegen und bei der z.B. ein Zugriff nur über ein Passwort zu unsicher wäre. Ein Client-Zertifikat stellt somit einen zweiten Faktor dar: Ich muss für den Zugriff etwas wissen und etwas haben.

Voraussetzung für dieses Vorgehen ist eine sogenannte Public-Key-Infrastrutkur (PKI). Diese besteht aus einer zentralen Zertifikatsinstanz, die Zertifikate für Server und für einzelne Personen herausgibt. Mensch kennt das von Webseiten, die über https (ssl) verschlüsselt sind.

Sogenannte Client-Zertifikate (also solche, die für Personen ausgestellt werden) können für folgende Anwendungen verwendet werden:

- VPN (virtuelles privates Netzwerk)]]
- Client-Zertifikate für Webbrowser zum Zugriff auf bestimmte Webdienste
- Verschlüsseln und Signieren von E-Mails

JedeR, der/die Zertifikate einsetzen möchte, benötigt dafür einen eigenen Schlüssel in einer pkcs12-Datei sowie das Wurzelzertifikat der jeweiligen PKI seiner Organisation.

Installation der Zertifikate im Browser

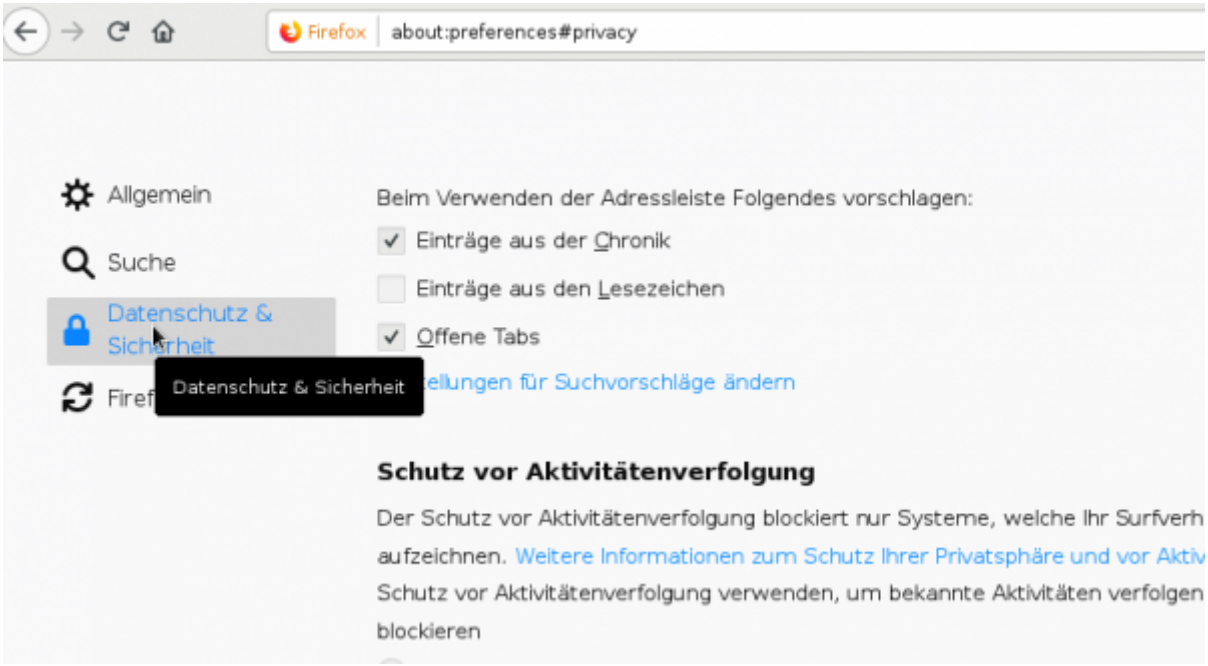
Die Zertifikate werden in der Regel für einzelne Organisationen vom Datenkollektiv zur Verfügung gestellt. In der Regel ist das eine Datei wie

```
vorname.nachname@organisation.org.p12
```

In dieser sind privater Schlüssel, öffentlicher Schlüssel sowie der CA-Schlüssel schon enthalten. Sie ist mit einem Passwort gesichert und kann in verschiedenen Programmen importiert werden.

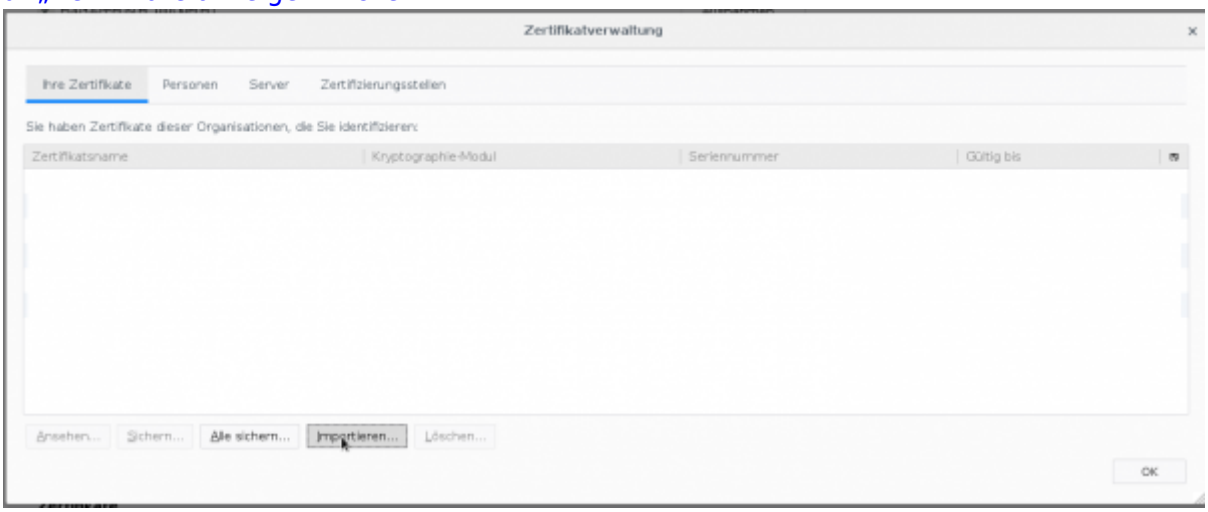
Client-Zertifikat installieren

Im Menü auf → Bearbeiten → Einstellungen gehen. Links „Datenschutz und Sicherheit“ auswählen.

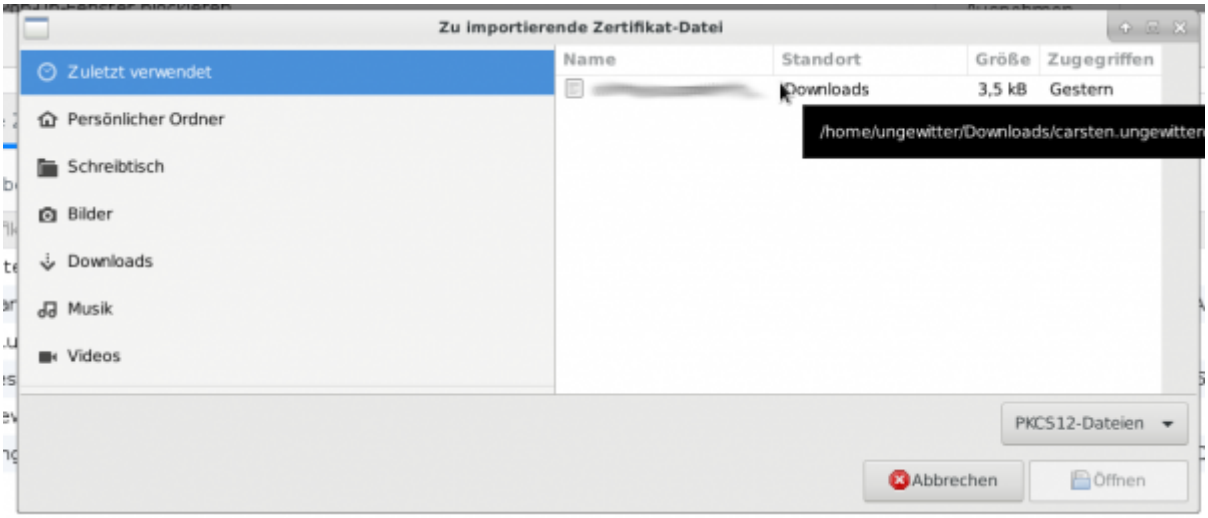


Ganz unten findet sich dann eine Rubrik „Zertifikate“

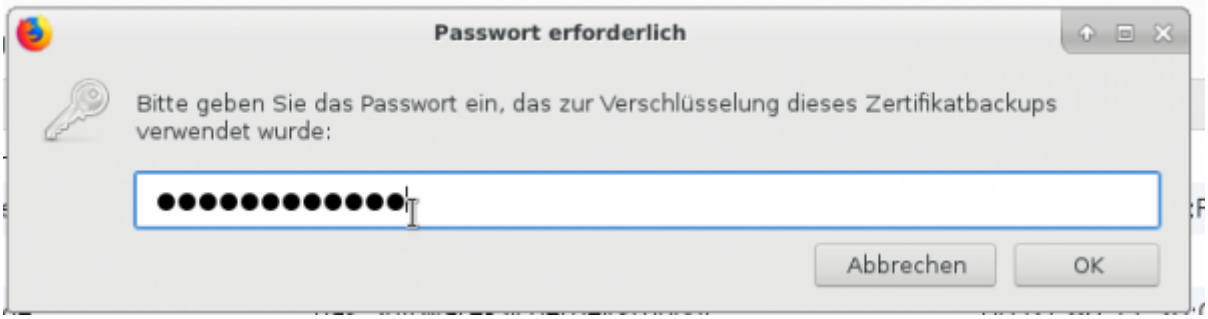
Hier auf „Zertifikate anzeigen klicken



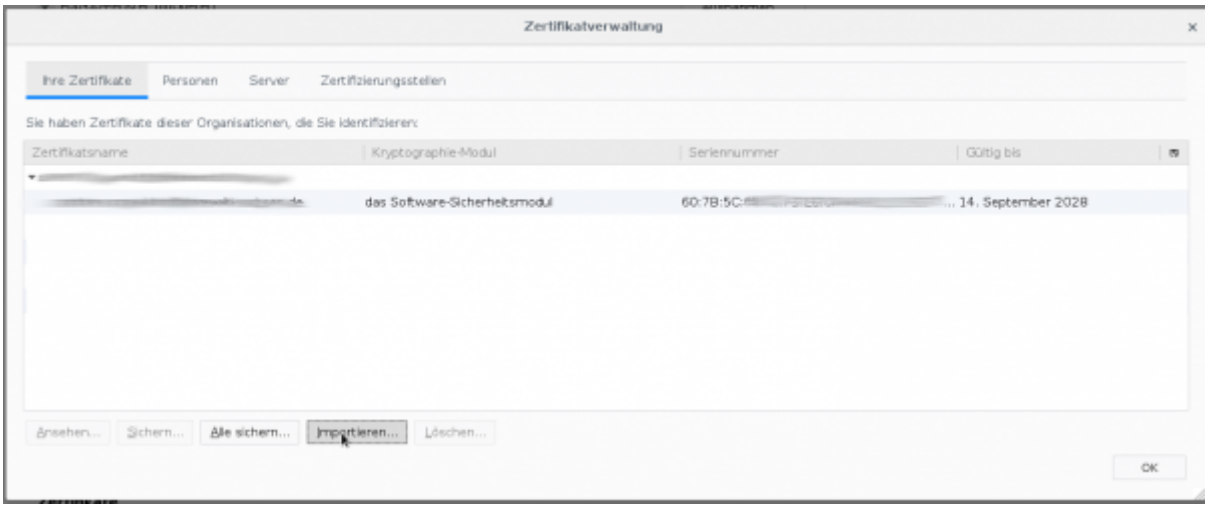
Weiter im Tab → `Ihre Zertifikate` Auf importieren klicken und das gespeicherte Zertifikat auswählen



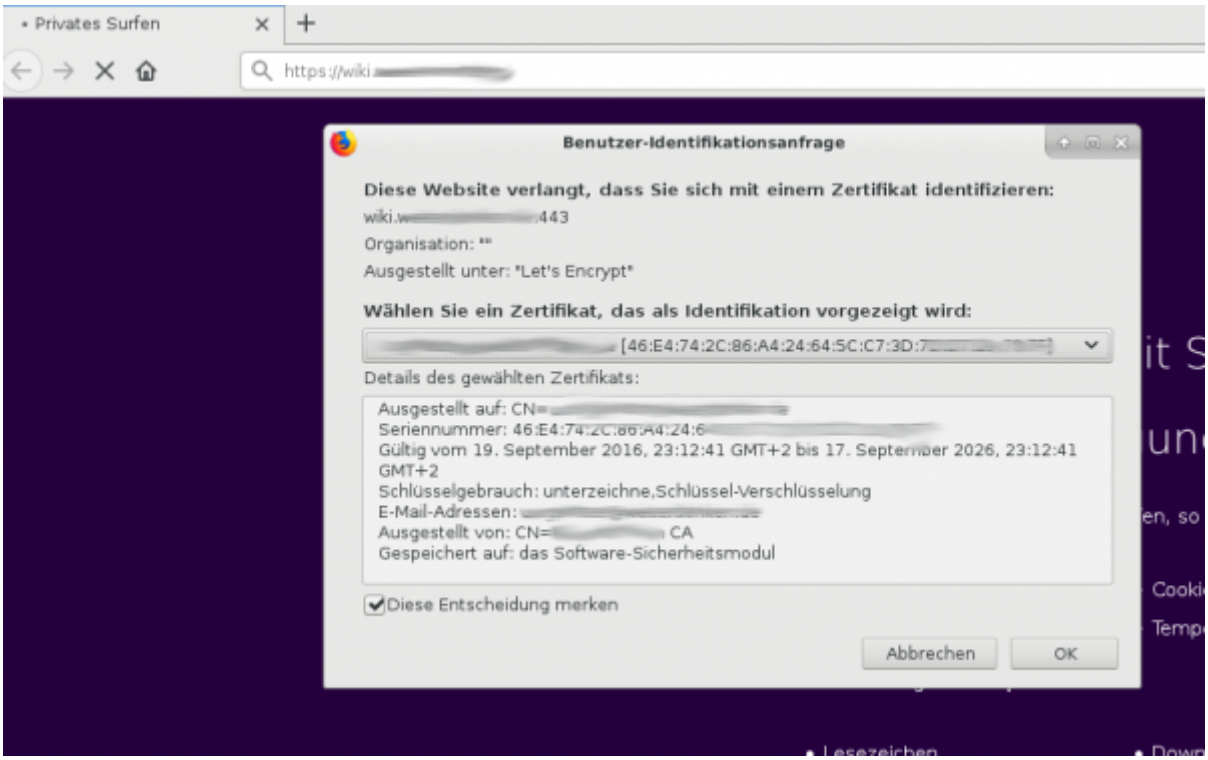
An dieser Stelle muss das Passwort, mit dem das Zertifikat gesichert ist, eingegeben werden.



Anschließend ist das Zertifikat im Browser installiert



Nach einem Neustart des Browsers sollte das Zertifikat installiert sein. Beim Zugriff auf eine per Client-Zertifikat abgesicherte Seite, erscheint dann eine Abfrage:



Hinweise zur Sicherheit

Client Zertifikate sind eine sehr sichere Möglichkeit, auf Web-Dienste zuzugreifen. Webdienste sollten grundsätzlich als potentiell angreifbar angesehen werden. Entweder durch Sicherheitslücken in der Software - oder aber durch ein erratenes oder versehentlich veröffentlichtes Passwort.

Ist ein Web-Dienst zusätzlich mit einem Client-Zertifikat abgesichert, genügt das Passwort alleine nicht mehr, um darauf zuzugreifen. Zusätzlich muss über das private Zertifikat verfügt werden. Damit können Angriffe über das Internet sehr sicher abgewehrt werden.

Da das Zertifikat jedoch im Browser gespeichert ist, kann jeder, der Zugriff auf den Browser des Nutzers (bei unbeaufsichtigten oder verlorgen gegangenen/gestohlenen Geräten), auch auf die abgesicherte Webseite zugreifen. Ist dann noch das Passwort für z.B. die Cloud im Browser gespeichert, ermöglicht das einen vollen Zugriff.

Daher ist es wichtig, bei Verlust des Geräts, oder wenn unklar ist, ob eine andere Person möglicherweise Zugriff auf das Geräte hatte, das Zertifikat sofort sperren zu lassen. So ähnlich wie bei einer verloren gegangenen EC-Karte.