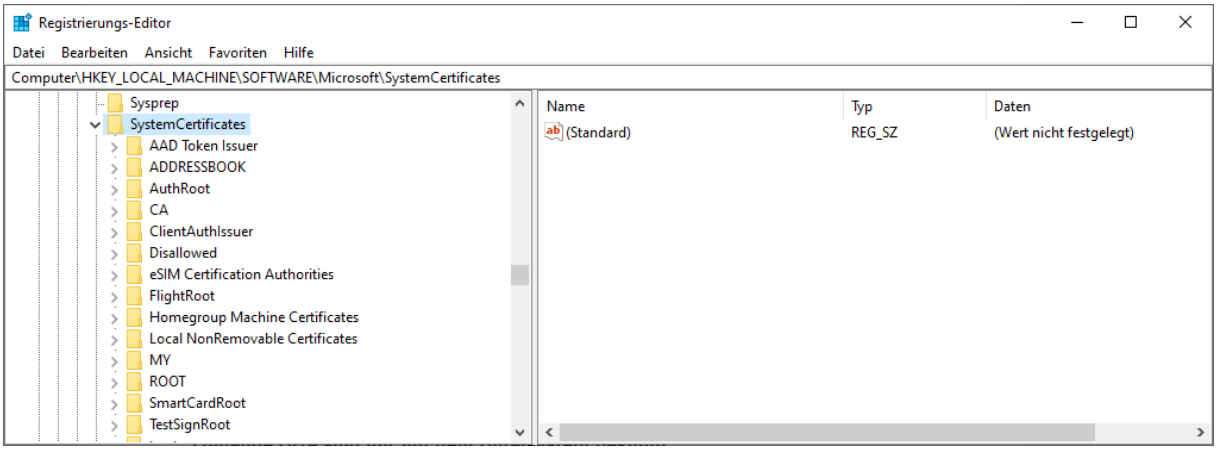
Speicherorte von Zertifikaten und deren Eigenschaften

Zertifikate auf einem Windows System werden an verschiedenen Orten abgelegt.

Zum einen in der Registry und zum anderen auf dem Filesystem.

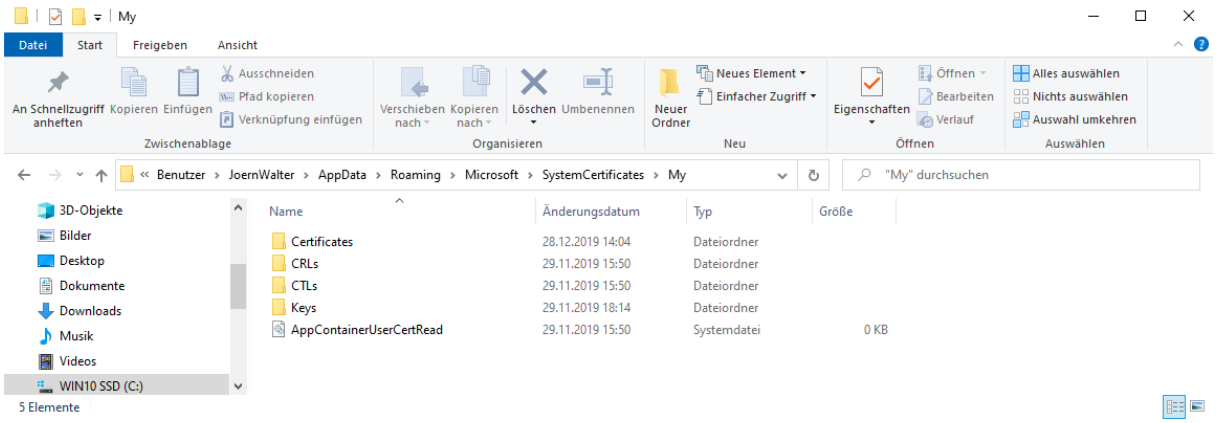
Folgende Orte sind mir in der Registry bekannt:



- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates
  - Speicher für benutzerspezifische öffentliche Schlüssel
- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SystemCertificates
  - Speicher für benutzerspezifische öffentliche Schlüssel, die von Active-Directory-Gruppenrichtlinienobjekten installiert werden
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates
  - Speicher für maschinenweite öffentliche Schlüssel
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Services
  - Speicher für Schlüssel, die einem definierten Dienst zugeordnet werden
- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SystemCertificates
  - Speicher für maschinenweite öffentliche Schlüssel, die von Active-Directory-Gruppenrichtlinienobjekten installiert werden
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EnterpriseCertificates
  - Speicher für maschinenweite öffentliche Schlüssel, die von den Enterprise PKI Containers in einem AD installiert werden

Speicherorte von Zertifikaten und deren Eigenschaften

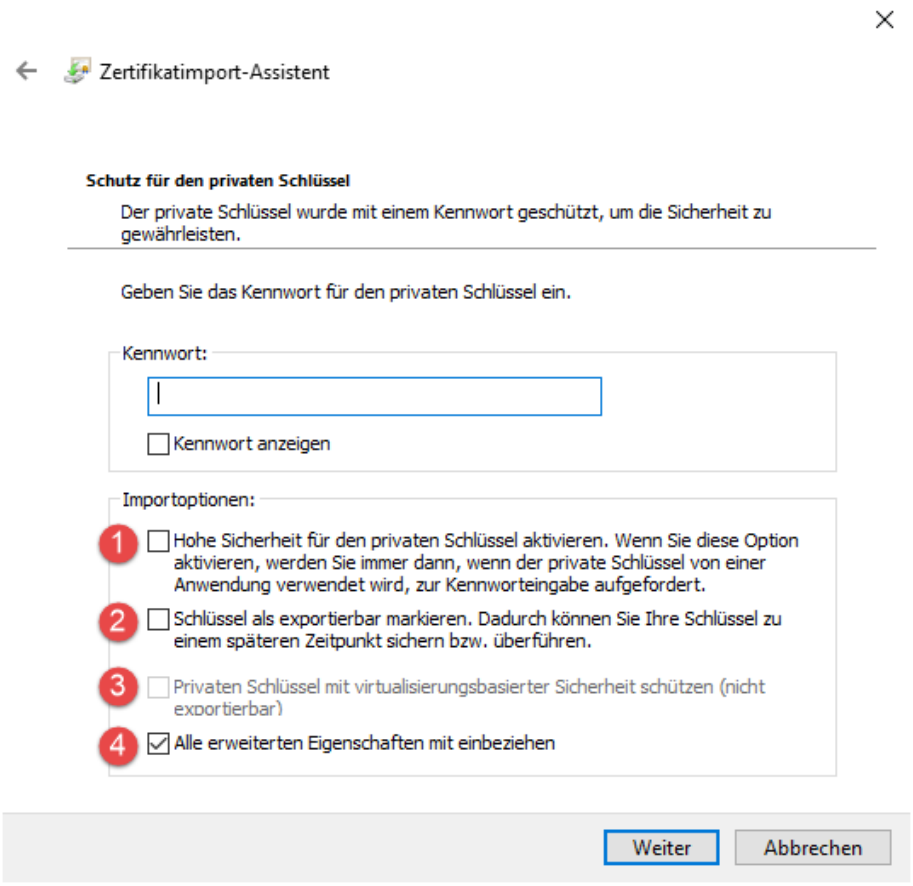
Folgende Orte sind mir auf dem Dateisystem bekannt:



- %APPDATA%\Microsoft\SystemCertificates\
  - Speicher für benutzerspezifische öffentliche Schlüssel und Verweis auf private Schlüssel
- %APPDATA%\Microsoft\Crypto\
  - Speicher für benutzerspezifische private Schlüsselcontainer
- %ProgramData%\Microsoft\Crypto\
  - Speicher für maschinenweite Container mit privatem Schlüssel

Speicherorte von Zertifikaten und deren Eigenschaften

Was bedeuten diese Optionen beim Import von Zertifikaten?

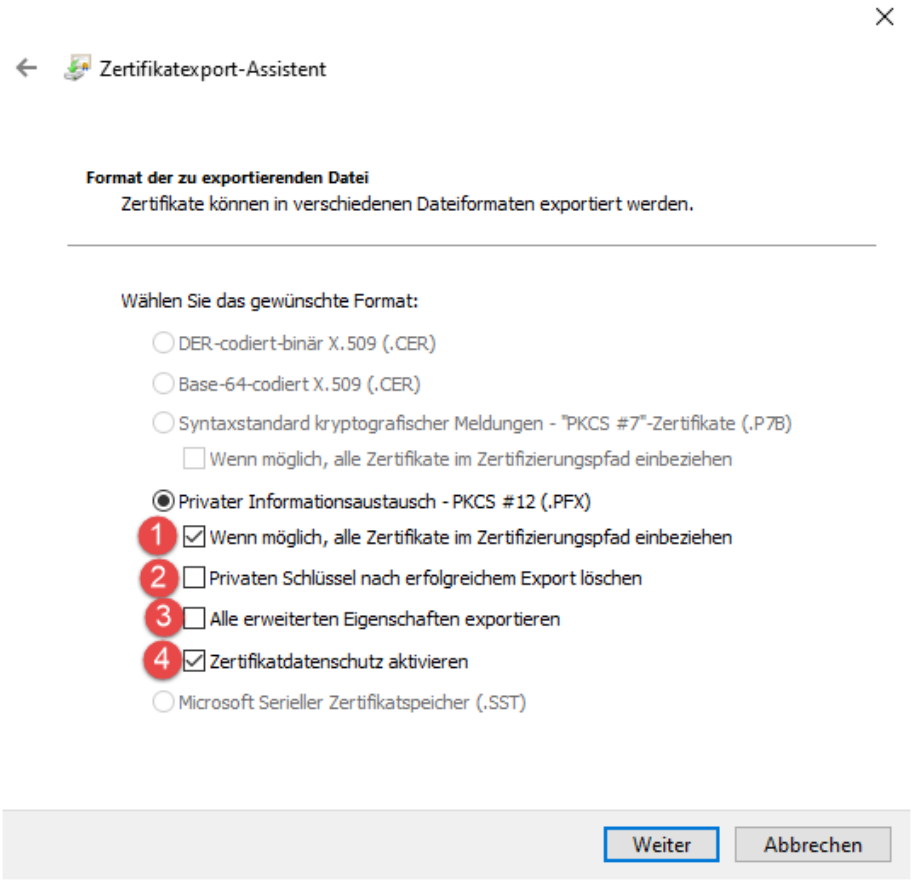


1) Hohe Sicherheit für den privaten Schlüssel aktivieren
    a. Die Eingabe des Passworts ist für jeden Zugriff auf den privaten Schlüssel erforderlich. Achtung! Diese Option wird nicht von jeder Software unterstützt
2) Schlüssel als exportierbar markieren
    a. Diese Option sollte vermieden werden sofern es geht. Private Schlüssel ähneln einem Zugangspasswort und sollten nicht noch einmal zugänglich gemacht werden
3) Privaten Schlüssel mit virtualisierungsbasierter Sicherheit schützen
    a. Diese Option bietet mehr Sicherheit zum Schutz privater Schlüssel in Bezug auf Cyber-Angriffen wie Schadsoftware
4) Alle erweiterten Eigenschaften mit einbeziehen
    a. Bei dieser Option werden alle zuvor exportierten Zertifikatserweiterungen importiert

Erstellt von Jörn Walter **28.12.2019**

Speicherorte von Zertifikaten und deren Eigenschaften

Was bedeuten diese Optionen beim Export von Zertifikaten?



1) Wenn möglich, alle Zertifikate im Zertifikatspfad einbeziehen
    a. Bei dieser Option werden alle Zertifikate in Kette mit exportiert. Es sind alle öffentlichen Schlüssel enthalten
2) Privaten Schlüssel nach erfolgreichem Export löschen
    a. Nach dem Export wird nur der private Schlüssel vom System gelöscht und ist somit nicht mehr verfügbar.
3) Alle erweiterten Eigenschaften exportieren
    a. Bei dieser Option werden alle Zertifikatserweiterungen mit exportiert
4) Zertifikatsdatenschutz aktivieren
    a. Diese Option verschlüsselt nicht nur den privaten Schlüssel, sondern auch alle enthaltenen öffentlichen Schlüssel

Speicherorte von Zertifikaten und deren Eigenschaften

Optional:

1) Gruppen- oder Benutzernamen (empfohlen)
    a. Diese Option ermöglicht das Verschlüsseln mit einem Benutzer- oder Gruppen-Prinzipal. Ein Kennwort ist auf jeden Fall nötig, sofern das exportierte Zertifikat außerhalb der Domäne eingesetzt wird.