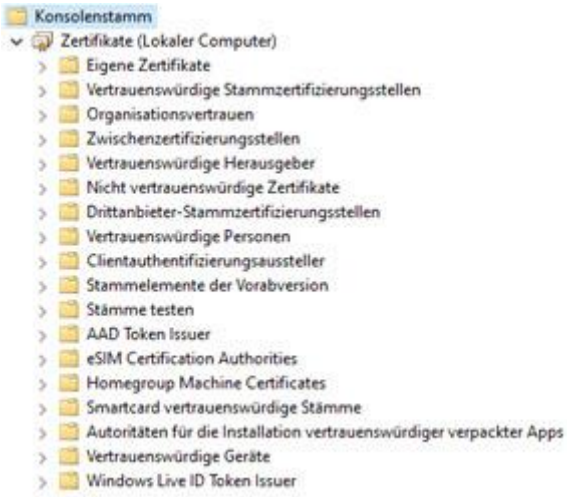
Windows Zertifikatsspeicher oder Container

Wofür sind die einzelnen Zertifikatsspeicher bzw. Container?



Je nach eingesetzter Windows Version (Client oder Server) unterscheiden sich die Speicher etwas in der Verfügbarkeit. Diese Speicher nennt man auch Logical Personal Store Layer.

Es gibt aber auch noch die Physical Store Layer für Benutzer, Computer oder Dienste.

Eigene Zertifikate (Personal Store)
In diesem Speicher werden die Zertifikate für den Computer oder den Benutzer gespeichert.

Vertrauenswürdige Stammzertifizierungsstellen (Trusted Root Certification Authorities)
In diesem Speicher liege die Stamm-Zertifizierungsstellen auf, denen der Client vertraut. Eine Zertifikatskette muss immer bis zu einer vertrauenswürdigen Stammzertifizierungsstelle gebildet werden können.

Organisationsvertrauen (Enterprise Trust)
In diesem Speicher können Stammzertifizierungsstellen von vertrauten Organisationen bzw. Unternehmen hinzugefügt werden. Anders als bei Zertifikaten, die von vertrauenswürdigen Stammzertifizierungsstellen stammen, können hier die Verwendungszwecke der Zertifikate von der Zertifizierungsstelle eingeschränkt werden und damit das Vertrauen »eingeschränkt« werden.

Zwischenzertifizierungsstellen (Intermediate CA)
In diesem Speicher liegen Zertifikate von Zwischenzertifizierungsstelle. Eine Zwischenzertifizierungsstelle ist eine Zertifizierungsstelle, die nicht als Stammzertifizierungsstelle (Root-CA) konfiguriert ist. Der Inhalt dieses Speichers kann auch über Gruppenrichtlinien gefüllt werden.

Vertrauenswürdige Herausgeber (Trusted Publishers)
In diesem Speicher können Zertifikate von Zertifizierungsstellen hinterlegt werden, denen über Softwareausführungsrichtlinien (Software Restriction Policies) vertraut werden soll. Die Einträge können auch über Gruppenrichtlinien verwaltet werden.

Nicht vertrauenswürdige Zertifikate (Untrusted Certificates)
In diesem Speicher werden Zertifikate abgelegt denen explizit nicht vertraut werden darf. In diesem Speicher können auch kompromittierte Zertifikate abgelegt werden. Dieser Speicher kann auch über Gruppenrichtlinien verwaltet werden.

Erstellt von Jörn Walter **17.10.2020**

Windows Zertifikatsspeicher oder Container

Drittanbieter-Stammzertifizierungsstellen (Third-Party Root Certification Authorities)
In diesen Speicher werden Nicht-Microsoft-Stammzertifizierungsstellen abgelegt. Dieser Speicher kann nicht per Gruppenrichtlinie verwaltet werden.

Vertrauenswürdige Personen (Trusted People)
In diesem Speicher werden Zertifikate (z. B. Applikationen) abgelegt, denen auch dann vertraut wird, wenn die ausstellende Zertifizierungsstelle nicht bekannt ist oder die Sperrliste nicht abgerufen werden kann. Dieser Speicher kann auch über Gruppenrichtlinien verwaltet werden.

Clientauthentifizierungsaussteller (Client Authentication Issuers)
In diesem Speicher werden Client Zertifikate abgelegt, wenn eine TLS-Verbindung zu einem Ziel aufgebaut werden soll. Wird der Speicher nicht verwendet, so wird gegen eine vertrauenswürdige Stammzertifizierungsstelle geprüft.

Stammelemente der Vorabversion (FlightRoot)
In diesem Speicher befinden sich Zertifikate von Microsoft-Zertifizierungsstellen, die von Windows-Vorabversionen verwendet werden kann. Diese Zertifikate sind nicht automatisch als vertrauenswürdig eingestuft.

Remotedesktop (Remotedesktop)
In diesem Speicher werden Zertifikate abgelegt, die auf dem System als Serverzertifikate für Remotedesktop-Verbindungen verwendent werden sollen.

Zertifikatregistrierungsanforderungen (Certificate Enrollment Requests)
In diesem Speicher werden noch ausstehende Anforderungen und abgelehnte Zertifikatsanforderungen abgelegt. Die Zertifizierungsstelle hat den ausstehenden Anforderungen noch keine Signatur (ausgestelltes Zertifikat) übermittelt.

Lokale Zertifikate für abgeschirmte VMs (Local Certificates for Shielded VMs)
In diesem Speicher werden Signatur- und Verschlüsselungszertifikate für abgeschirmte VMs abgelegt.

Vertrauenswürdige Geräte (Trusted Devices)
In diesem Speicher können Zertifikate abgelegt werden, mit denen der Zugriff auf geschützte Dokumente oder Applikationen gesteuert werden kann.

Smartcard vertrauenswürdige Stämme (Smart Card Trusted Roots)
In diesem Speicher können auch SmartCards von fremden Zertifizierungsstellen abgelegt werden.

Webhosting (Webhosting)
In diesem Speicher werden Zertifikate abgelegt auf den der IIS zugreift. Der Webserver kann Zertifikate aus dem Personal-Store (Eigene Zertifikate) oder dem Webhosting-Speicher verwenden.

Das sind die Namen der gängigen Speicher (Stores/Container), um mittels Skripts darauf zugreifen zu können.

Windows Zertifikatsspeicher oder Container

Hier findet ihr ein Artikel der zeigt, wie man auf einen der Speicher zugreift.

 # Maschinen Stores

Name : AuthRoot
Name : CA
Name : ClientAuthIssuer
Name : Disallowed
Name : FlightRoot
Name : Local NonRemovable Certificates
Name : My
Name : Remote Desktop
Name : REQUEST
Name : Root
Name : SmartCardRoot
Name : Trust
Name : TrustedDevices
Name : TrustedPeople
Name : TrustedPublisher
Name : Windows Live ID Token Issuer

 # User Stores

Name : ACRS
Name : AuthRoot
Name : CA
Name : ClientAuthIssuer
Name : Disallowed
Name : My
Name : REQUEST
Name : Root
Name : SmartCardRoot
Name : Trust
Name : TrustedPeople
Name : TrustedPublisher
Name : UserDS

Windows Zertifikatsspeicher oder Container

Die Namen der Speicher können mit diesem Befehl ermittelt werden.

certutil -enumstore