

Auf meiner Zertifizierungsstelle mit dem Namen SRVSUBCA habe ich 2 Zertifikatsvorlagen erstellt.

Die Vorlage mit dem Namen WEBSHA384 und die Vorlage mit dem Namen WEBSHA256.

🖀 Konsole1 - [Konsolenstamm\Zertifizierungsstelle (Lokal)\SRVSUBCA	Zertifikatvorlagen] —	□ ×
Batei     Aktion     Ansicht     Favoriten     Fenster     ?            ← ➡ │		- & ×
Konsolenstamm Name	Beabsichtigter Zweck Ak	tionen
V Zertifizierungsstelle (Lokal)	4 Serverauthentifizierung, Clientauthentifizierung Zer	rtifikatv 🔺
▼ ■ SNUSECA     @ WESSHA2       @ WESSHA2     @ WESSHA2       ■ Ausgestellte Zertifikate     @ Kerberos       ■ Ausgestellte Zertifikate     @ Kerberos       ■ Ausgestellte Zertifikate     @ Kerberos       ■ Exchange     @ RDPAuth       ■ Zertifikatvorlagen     @ WEB       > @ Zertifikate (Lokaler Computer)     @ WEB       > @ Unternehmens-PKI     @ WEBSHA2	6v2         Serverauthentifizierung           Clientauthentifizierung         Serverauthentifizierung           Serverauthentifizierung         Remote Desktop Authentication           Serverauthentifizierung, Clientauthentifizierung         Serverauthentifizierung           Serverauthentifizierung         Clientauthentifizierung           Serverauthentifizierung         Clientauthentifizierung           6         Clientauthentifizierung	Weite 🕨

Die Vorlage WEBSHA384 ist so eingestellt, dass die eingehende Zertifikatsanfrage genehmigt werden muss.

Zertifikatvorlagenkonsole			- 🗆 X
Datei Aktion Ansicht ?			
🗢 🌳 💼 🗙 🗊 🛃 🚺		Eigenschaften von WEBSHA384 ? X	
Zertifikatvorlagen (DC1.dwp.loc	Vorlagenanzeigename	Abgelöste Vorlagen Erweiterungen Sicherheit Server	^ Aktionen
	🖳 Exchange Enrollment Age	Allgemein Kompatibilität Anforderungsverarbeitung Kryptografie	Zertifikatv 🔺
	Exchange-Benutzer	Schlüsselnachweis Antragstellemame Ausstellungsvoraussetzungen	Weite >
	PSec IPSec	Registrierung erfordert Folgendes:	
	Resec (Offlineanforderung	Genehmigung von Zertifikatverwaltung der Zertifizierungsstelle	WEBSHA384 🔺
	Kerberos	g, Serverauthentifizierung, Smarto	ard-Anme Weite 🕨
	Rerberos-Authentifizieru	g, Serverauthentifizierung, Smarto	:ard-Anme
	Key Recovery Agent	Die automatische Registherung kann nicht verwendet werden, wenn Sie mehr als ein Zertifikat anfordem.	
	Renutzersignatur	Erforderlicher Richtlinientvp für Signatur:	
	Nur Exchange-Signatur	✓	
	CCSP-Antwortsignatur	Anwendungsrichtlinie:	
	RAS- und IAS-Server	g, Serverauthentifizierung	
	RUPAuth	Ausstellungsrichtlinien:	
	Smartcard-Anmeldung	Hinzufügen	
	Smartcard-Anniedung	5.4	
	Stammzertifizierungsstell	Entremen	
	Übergreifende Zertifizieri	Emerite Beristrierung erfordet Folgendee:	
	Untergeordnete Zertifizie	Chicke Kitaise wis für Desisties ver	
	Vertrauenslistensignatur		
	🖳 Verzeichnis-E-Mail-Replik	Schlüges Vorrandenes Zertinkat	
	Reg WEB	Generate de la contraction de la contractio	
	Webserver	Zertifikatanforderung.	
	Rebsha256	g, Serverauthentifizierung	
	Rebsha256v2	g	
	WEBSHA384	g, Clientauthentifizierung	
	Rertifizierungsstellenaust	OK Abbrechen Übernehmen Hilfe aten Schlüssels	~
< >	<		>
41 Zertifikatvorlagen			



Anders ist es bei der Vorlage WEBSHA256. Hier ist keine Genehmigung nötig.

Zertifikatvorlagenkonsole			- 🗆 ×
Datei Aktion Ansicht ?			
⇐ ➡ 💼 🗙 🗉 🗟 🖪		Eigenschaften von WEBSHA256 ? ×	
R Zertifikatvorlagen (DC1.dwp.loc	Vorlagenanzeigename	Abgelöste Vorlagen Erweiterungen Sicherheit Server	^ Aktionen
	Exchange Enrollment Ag	Allgemein Kompatibilität Anforderungsverarbeitung Kryptografie	Zertifikaty 🔺
	Exchange-Benutzer	Schlüsselnachweis Antragstellemame Ausstellungsvoraussetzungen	Waita
	IPSec	Registrierung erfordert Folgendes:	Weiten. P
	IPsec (Offlineanforderun)	Genehmigung von Zertifikatverwaltung der Zertifizierungsstelle	WEBSHA256 🔺
	Kerberos		g, Serverauthentifizierung, Smartcard-Anme Weite 🕨
	Kerberos-Authentifizieru		g, Serverauthentifizierung, Smartcard-Anme
	Key Recovery Agent	Die automatische Registrierung kann nicht verwendet werden, wenn Sie mehr als ein Zertifikat anfordern	
	Rur Benutzersignatur	Erforderlicher Bichtlinientun für Signatur:	
	Nur Exchange-Signatur		
	CCSP-Antwortsignatur	Anwendungsrichtlinie:	
	RAS- und IAS-Server	×	g, Serverauthentifizierung
	RDPAuth	Ausstellungsrichtlinien:	entication
	Kouter (Offlineanforderu	Hinzufügen	
	Smartcard-Anmeidung		
	Stammzertifizierungsstell	Entremen	
	Illhergreifende Zertifizien	Emerida Banistina una enfandest Felerendeau	
	Intergeordnete Zertifizie	Chicks Kitarian wie für Desistien von	
	Vertrauenslistensignatur		
	Werzeichnis-E-Mail-Repli		fail-Replikation
	WEB .		g
	Webserver	Zertifikatanforderung.	
	WEBSHA256	-	g, Serverauthentifizierung
	WEBSHA256v2		g
	WEBSHA384		g, Clientauthentifizierung
	Zertifizierungsstellenaust	OK Abbrechen Übernehmen Hilfe	aten Schlüssels
< >	<		>
41 Zertifikatvorlagen			

Nun wechlse ich auf ein Client-System und prüfe im Vorfeld, ob es noch alte Zertifikatsanfragen gibt. Nein, OK.

📓 Konsole1 - [Konsolenstamm\Zertifikate (Lokaler C	omputer)\Zertifikatregistrierungsanforderungen]	_	$\Box$ ×
🚟 Datei Aktion Ansicht Favoriten Fenster	?		- 8 ×
🗢 🔿 🙍 🖬 🗎 🖓 🔂 📷			
Konsolenstamm	Objekttyp	Aktionen	
V 🙀 Zertifikate (Lokaler Computer)		Zertifikatregistrierungsanforderungen	
Eigene Zertifikate	in dieser Ansicht werden keine Elemente angezeigt.	Weiters Aktienen	
Zertifikate		Weitere Aktionen	•
Vertrauenswurdige Stammzertifizierungsste			
> Organisationsvertrauen			
Vertrauenswürdige Herausgeber			
Nicht vertrauenswürdige Zertifikate			
Drittanbieter-Stammzertifizierungsstellen			
Vertrauenswürdige Personen			
> 📔 Clientauthentifizierungsaussteller			
> Stammelemente der Vorabversion			
> Stämme testen			
> 🔛 Remotedesktop			
> Zertifikatregistrierungsanforderungen			
> Smartcard vertrauenswürdige Stämme			
> Vertrauenswürdige Geräte			
> Webhosting			
> windows Live ID Token issuer			
< >>			
Der Speicher "Zertifikatregistrierungsanforderungen" er	thält keine Zertifikate.		



Nun öffne ich die Powershell mit administrativen Rechten und frage ein Zertifikat gemäß dieser Konfiguration bei der CA zur Signierung an.

Get-Certificate -Template "WEBSHA256" -DnsName "SRVTOOLS.dwp.local" -CertStoreLocation cert:\LocalMachine\My -SubjectName "CN=SRVTOOLS.dwp.local, C=DE, L=Essen, O=DERWINDOWSPAPST, OU=IT, S=NRW"



Nachdem ich den Befehl abgesetzt habe, bin ich auch schon im Besitz des Zertifikats.

🖀 Konsole1 - [Konsolenstamm\Zertifikate (Lokaler C	Computer)\Eigene Zertifikate\Zert	fikate]				-	- 🗆 ×
🚟 Datei Aktion Ansicht Favoriten Fenster	?						_ 8 ×
⇐ ⇒   2 📰   ४ 🖻 🗙 🖻 🔒 🛛 🖬							
📔 Konsolenstamm	Ausgestellt für	Ausgestellt von	Ablaufdatum	Beabsichtigte Zwecke	Anzeigename St	atus Zertifikatvorlage	Aktionen
✓  ☐ Zertifikate (Lokaler Computer)	Ccs.dwp.local	SRVSUBCA	18.04.2022	Clientauthentifizierung, Serverauthentifizierung	<keine></keine>	WEBSHA256	Zertifikate
✓	SRVTOOLS.dwp.local	SRVSUBCA	21.04.2022	Clientauthentifizierung, Serverauthentifizierung	<keine></keine>	WEBSHA256	
🚞 Zertifikate	SRVTools.dwp.local	SRVSUBCA	14,12,2020	Remote Desktop Authentication	<keine></keine>	RDPAuth	weite •
> Vertrauenswürdige Stammzertifizierungsste							SRVTOOLS 🔺
> Organisationsvertrauen							Weite •
> Zwischenzertifizierungsstellen							
Nicht vertrauenswürdige Zertifikate							
Drittanbieter-Stammzertifizierungsstellen							
> Vertrauenswürdige Personen							
> 📋 Clientauthentifizierungsaussteller							
> 📔 Stammelemente der Vorabversion							
> 🧮 Stämme testen							
> 🧮 Remotedesktop							
> Zertifikatregistrierungsanforderungen							
> Smartcard vertrauenswürdige Stämme							
> Vertrauenswürdige Geräte							
> Webhosting							
> windows Live ID Token issuer							
< >>							
Der Speicher enthält "Eigene Zertifikate" 3 Zertifikate.							



Bei dieser Vorlage ist eine Genehmigung seitens des CA-Managers nötig.

Get-Certificate -Template "WEBSHA384" -DnsName "SRVTOOLS.dwp.local" -CertStoreLocation cert:\LocalMachine\My -SubjectName "CN=SRVTOOLS.dwp.local, C=DE, L=Essen, O=DERWINDOWSPAPST, OU=IT, S=NRW"



Nachdem ich die Zertifikatsanfrage über die Powershellkonsole abgesetzt haben, befindet sich diese zur Prüfung im Ordner "Ausstehende Anforderungen".

Kurzehand überprüft und ausgestellt.

Konsole1 - [Konsolenstamm\Zertifizierungsst	elle (Lokal)\SRVSUBC	A\Ausstehende Anforder	ungen]				_	οx	
Tatei Aktion Ansicht Favoriten Fenst	ter ?							- 8	×
Konsolenstamm Tottifizierungsstelle (Lokal)	Anforderungs-ID	Binäre Anforderung	Anforderung: Statuscode	Anforderung: Dispositionsmeldung	Anforderung: Einreichungsdatum	Antragstellername	Anforderung: Land/Region	Aktionen	_
V J SRVSUBCA	51 	Alle Aufgaben	Attribute/Enweiterungen anzeige	Rei Übermittlung :n	21.04.2020 09:30	DWP\SRVTOOLSS	DE	Ausstehen · Weite	•
Ausgestellte Zertifikate		Aktualisieren	Binärdaten exportieren					61 .	•
Eehlgeschlagene Anforderungen		Hilfe	Ausstellen Verweigern					Weite	۲
<ul> <li>Zertifikatvorlagen</li> <li>Zertifikate (Lokaler Computer)</li> </ul>									
> 🏥 Unternehmens-PKI									
Fash Vis dia Atalanan dia ang dara Fisanana darahara	<						>		_
Enthält die Aktionen, die an dem Element durchge	führt werden können								

Die Anforderung hat die ID 61 und die vorherige Anforderung die ID 60.

Datei Aktion Ansicht Favoriten Fenst	er ?								- 8 ×
Konsolenstamm     Karsolenstamm     Korsolenstamm     Korsole	Anforderungs-ID	Antragstellername DWP\SRVTOOLS\$	Bināres Zertifikat	Zertifikatvorlage WEBSHA384 (1.3.6.1.4.1.311.21.8.13280848.51	Seriennummer 68000003dd45	Anfangsdatum des Zertifikats 21.04.2020 09:21	Ablaufdatum des Zertifikats 21.04.2022 09:21	Ausgestellt: ^	Aktionen Ausgestell ▲
Gesperte Zertifikate Ausgestellte Zertifikate	59 58	DWP\SRVTOOLSS DWP\SRVTOOLSS DWP\SRVTOOLSS	BEGIN CERTI BEGIN CERTI BEGIN CERTI	WEBSHA256 (1.3.6.1.4.1.311.21.8.13280848.51 WEBSHA384 (1.3.6.1.4.1.311.21.8.13280848.51 WEBSHA384 (1.3.6.1.4.1.311.21.8.13280848.51 WEBSHA384 (1.3.6.1.4.1.311.21.8.13280848.51	68000003c81af 68000003b9dc 68000003a97d	21.04.2020 09:18 21.04.2020 08:56 21.04.2020 08:52	21.04.2022 09:18 21.04.2022 08:56 21.04.2022 08:52	DE DE DE	Weite ►
<ul> <li>Fehlgeschlagene Anforderungen</li> <li>Zertifikatvorlagen</li> <li>Zertifikate (Lokaler Computer)</li> </ul>	54 53	DWP\SRVTOOLSS DWP\SRVTOOLSS DWP\SRVSUBCAS DWP\DC15	BEGIN CERTI BEGIN CERTI BEGIN CERTI	WEBSHA256 (1.3.6.1.4.1.311.21.8.15280848.51 WEBSHA256 (1.3.6.1.4.1.311.21.8.13280848.51 WEBSHA256 (1.3.6.1.4.1.311.21.8.13280848.51 2.6.1.4.1.311.21.8.13280848.51	68000003664b 680000003664b 6800000035c59f	21.04.2020 08:50 21.04.2020 08:42 21.04.2020 08:38 20.04 2020 21:49	21.04.2022 08:50 21.04.2022 08:42 21.04.2022 08:38 20.04.2021 21:49	DE DE DE	Weite 🕨
א און Unternehmens-₽Ki	43 42 41	DWP\SRVKMS\$ DWP\SRVTOOLS\$ DWP\DC15	BEGIN CERTI BEGIN CERTI BEGIN CERTI	RDPAuth (1.3.6.1.4.1.311.21.8.13280848.51700 WEBSHA256 (1.3.6.1.4.1.311.21.8.13280848.51700 UCC (1.2.6.1.4.1.311.21.8.13280848.51 DCc (1.2.6.1.4.1.311.21.8.13280848.51	680000002bdd0 680000002a56cf	19.04.2020 13:33 18.04.2020 16:39	19.04.2021 13:33 18.04.2022 16:39		
	40 39	DWP\SRVSUBCA\$ DWP\SRVFILE\$	BEGIN CERTI BEGIN CERTI	Zertifizierungsstellenaustausch (CAExchange) RDPAuth (1.3.6.1.4.1.311.21.8.13280848.51700	680000028109 680000028109	15.04.2020 19:29 13.02.2020 20:15	22.04.2020 19:39 12.02.2021 20:15		
	35 35 39	DWP\SRVSUBCAS DWP\WIN10-1909\$ DWP\DC1\$	BEGIN CERTI BEGIN CERTI	Zertifizierungsstellenaustausch (LAExchange) RDPAuth (1.3.6.1.4.1.311.21.8.13280848.51700 Kerberos (1.3.6.1.4.1.311.21.8.13280848.51700	68000000242e0f 6800000023a8b 6800000013724	04.02.2020 09:46 12.01.2020 16:56	18.02.2020 22:46 03.02.2021 09:46 11.01.2022 16:56	~	



\$cert = (Get-ChildItem -path cert:\LocalMachine\Request)

Nun wechsel ich wieder zurück zum Client-System und setzen den 2. Befehl ab. Dieser Befehl fragt nun auf Basis der Zertifiksananforderung das Zertifikat ab.



Es wird sofort in den angegebenen Speicher abgelegt.

Konsole1 - [Konsolenstamm\Zertifikate (Lokaler C	Computer)\Eigene Zertifikate\Ze	rtifikate]						- 🗆 X
🚘 Datei Aktion Ansicht Favoriten Fenster	?							_ 8 ×
🗢 🔿 🙍 📷 🔏 ங 🗙 🖾 🔒 🖬 📷								
<ul> <li>Konsolenstamm</li> <li>Zertifikate (Lokaler Computer)</li> <li>Compose Zertifikate</li> </ul>	Ausgestellt für Â	Ausgestellt von SRVSUBCA	Ablaufdatum 18.04.2022	Beabsichtigte Zwecke Clientauthentifizierung, Serverauthentifizierung	Anzeigename <keine></keine>	Status	Zertifikatvorlage WEBSHA256	Aktionen Zertifikate
Certifikate     Certifikate     Vertrauenswürdige Stammzertifizierungsste	SRVTOOLS.dwp.local	SRVSUBCA SRVSUBCA	21.04.2022 21.04.2022	Clientauthentifizierung, Serverauthentifizierung Serverauthentifizierung, Clientauthentifizierung	<keine> <keine></keine></keine>		WEBSHA256 WEBSHA384	Weite 🕨
Criganisationsvertrauen     Criganisationsvertrauen     Criganisationsvertrauen	🕼 SRVTools.dwp.local	SRVSUBCA	14.12.2020	Remote Desktop Authentication	<keine></keine>		RDPAuth	SRVTOOLS A Weite >
Avischenzentrizerungsstellen     Vertrauenswürdige Zertfikate     Drittanbieter-Stammzeitige Zertfikate     Drittanbieter-Stammzeitfizierungsstellen     Vertrauenswürdige Personen     Clientauthentfizierungsaussteller     Stammetement der Vorabversion     Stämme testen     Remotelesktop     Zertfikatregistrierungsanforderungen     Smartcard vertrauenswürdige Stämme     Vertrauenswürdige Geräte     Webhosting     Windows Live ID Token Issuer								•rene •