

ANLEITUNG: ZERTIFIKATSERSTELLUNG WINDOWS AD



Ziel:

Erstellung und Signatur eines Zertifikats in einer Windows-AD-Umgebung für einen Webserver.

Schritt 1

Zunächst kann, wenn die Zertifizierungsstelle nicht bekannt ist, die Applikation **"Zertifizierungsstelle"** gestartet werden:



Schritt 2

Anschließend ist die Zertifizierungsstelle zu sehen, hier EKGLab-SVR-02-CA:

certsrv - [Zertifizierungsstelle (Lok Datei Aktion Ansicht ?	s[)]		-	٥	×
(* *) 🗟 🛛 🕨 🖿					
 Tertifizierungistelle (Loka) Zertifizierungistelle (Loka) Esperitz Zertifikate Ausgertellte Zertifikate Ausstehende Anforderung Feligischlagene Anforder Zertifikatvorlagen 	Name	Beschreibung Zertifizierungsstelle			



Schritt 3

Dann muss das Konsolen-Snap-In **"Zertifikate"** in der Microsoft Management Console ausgewählt werden und dort unter **"Eigene Zertifikate → Zertifikate → Alle Aufgaben → Erweiterte Vorgänge → Benutzerdefinierte** Anforderung erstellen..." gewählt werden:

Konsolenstamm	Ausgestell	lt für	Ausgestellt von	Ablaufdatum	Beabsichtigte Zwec	Anzeigename	Status	Aktionen	
 Zertifikate (Lokaler Computer) Eigene Zertifikate 	EKGLab	-SVR-02-CA	EKGLab-SVR-02-CA	24.01.2028	<alle></alle>	<keine></keine>		Zertifikate	-
 Zertifica Vertrauenty Organisatic Ansisht 	n >	Neues Zertifikat and Importieren	EKOLob SVR 02-CA fordern	24.01.2028	«Alle»	<keine></keine>		Weitere Aktionen	,
> Zwischenze Neues Fenst	er hier öffnen	Enweiterte Vorgänge	e >	Benutzerdefinierte Anforderun	g erstellen				
> Nicht vertra Neue Aufga	enblockansicht			Registrierungsrichtlinien verwa	lten				
> 20 Drittanbietx > 20 Vertrauenav Aktualisierer > 20 Clientauthe Liste exporti	ren								
> Stammelen > Stamme te: Hilfe									
 Remoted bittage Zertöfikaregistnerungsanfordu Smartcard vertrauenswürdige Vertrauenswürdige Geräte Webhosting Windows Live ID Token Issuer Zertöfikatvorlagen Zertöfizierungsstelle (Lokal) 	rungen Kämme								

Schritt 4

Anschließend muss dem Assistenten gefolgt werden:

🗢 🔿 🙍 💼 🛍 🔯 👘								
Konsienstamm Eigene Zertifikate Eigene Zertifikate Certifikate Ce	Ausgestellt für LEKSLab-SVR-02-CA LEKSLab ore m cn Vorbereitu Beachten Sie Anschluss von Stellen Sie verfügen (kann.	Ausgestellt von EKGLSb-SVR-02-CA EKGLSb-SVR-02-CA EKGLSb-SVR-02-CA EKGLSb-SVR-02-CA EKGLSb-SVR-02-CA Ing Jagende Schritte, wenn Sie Zertifik Unahtlosnetzwerken, Schutz des J ogener Aufgaben sind. Anforderung eins Zertifikats Fol- ist mit dem Netzwerk verbunden ber Anmeldeinformationen, mit o	Ablaufdatum 24.01.2028 34.01.2028 34.01.2020 ate installieren, die digital nhalts, Einrichten der Iden iendes sicher: enen Ihr Recht, das Zertifi	Beabsichtigte Zwec cAlle> Alle> Alle> e Anmeldeinformationer titst, und Ausführen and kat zu erhalten, überprüf	Anzeigename (Keine) //wiewa wiewa twerden brechen	Status	Aktionen Zerbfikate Weitere Aktionen	• •



Schritt 5

Im nächsten Schritt sollte "Active-Directory-Registrierungsrichtlinie" gewählt werden, wenn vorhanden, sonst "Den Vorgang ohne Registrierungsrichtlinie fortsetzen":

 Konsolenstamm Zertifikate (Lokaler Computer) Eigene Zertifikate 	Ausgestellt für	Ausgestellt von EKIGLab-SVR-02-CA	Ablaufdatum 24.01.2028 24.01.2029	Beabsichtigte Zwec	Anzeigename <keine></keine>	Status	Aktionen Zertifikate	•
Zertifikäte Organisationzvertrauen Organisationzvertrauen Zvischenzertifizierungsstellen Zvischenzertifizierungsstellen Vertrauenzwürdig ersonen Organisationzvertrauenzurfür Organisationzvertrausenzurfür Organisationzvertrausenzurfür Organisationzvertrausenzurfür Organisationzvertrausenzurfür Stamme testen Remotedesktop Zertifikatregistrierungsanforderungen Werbusenzwürdig erste Werbusenzwürdig erste Werbusenzwürdig erste Werbusenzwürdig erste Werbusenzwürdig erste Werbusenzwürdig erste Werbusenzwürdig (Lokal)	Zertifikatregi Zertifika Mrthilfe d Zertifika Konfigurie Vom Adm Active D Von Inner Benutzer Den Von	strierung r Zertifikatregistrierungsrichtlinie aus r Zertifikatregistrierungsrichtlinie kö ohlgen registriert werden. Die Zertifi t. inistrator konfiguriert inistrator konfiguriert definierte Anforderung gang ohne Registrierungsrichtlinie fo	wählen nnen Zertifikate basierend isatregistrierungsrichtlinie i rtsetzen	- [auf vordefinierten st möglicherweise bereit: Neue hin Weiter Ab	a für Sie vurfügen brechen		Weitere Aktionen	,

Schritt 6

Im nächsten Schritt wird die Standard-Vorlage "Webserver" ausgewählt:

🖀 Datei Aktion Ansicht Favoriten Fenster ?								- 8 ×
🗢 🔿 📶 📋 🗟 🕞 📓 📷								
Konsolenstamm	Ausgestellt für	Ausgestellt von	Ablaufdatum	Beabsichtigte Zwec	Anzeigename	Status	Aktionen	
 Zertifikate (Lokaler Computer) 	EKGLab-SVR-02-CA	EKGLab-SVR-02-CA	24.01.2028	<alle></alle>	<keine></keine>		Zertifikate	
Zertifikate	EKGLab SHE M CA	ENGLAR GID AD CA	24 M 2020	- [Wainas X		Weitere Aktionen	•
> 2 Vertrauenswürdige Stammzertifizierungsstelle								
> Organisationsvertrauen	Zertifikatregistrierung							
> Zwischenzerünzlerungsstellen								
Nicht vertrauen swürdige Zertifikate	Benutzerdefini	erte Anforderung						
> Drittanbieter-Stammzertifizierungsstellen								
> 🔛 Vertrauenswürdige Personen	Wählen Sie aus der	folgenden Liste eine Option au	is, und konfigurieren Sie	die Zertifikatoptionen n	ach			
> 🛄 Clientauthentifizierungsaussteller	Bedarf.							
> 🛄 Stammelemente der Vorabversion								
> Stämme testen	Vorlage:	Arbeitsstationsauthe	ntifizierung		~			
> Remotedesktop		Arbeitsstationsauthe	ntifizierung					
Zertifikätregistrierungsanforderungen Smartcard vertrauen pwürdige Stämme	Anfordeninger	Computer						
Vertrauen swürdige Geräte	Antorderungsr	Domänencontroller						
> Webhosting		Domänencontrollera	uthentifizierung					
> 🔛 Windows Live ID Token Issuer	Hinweis: Die Schlü	sselarchix IPSec	omputery					
> 🛃 Zertifikatvorlagen	Zertifikatanforder	ang basier IPsec (Offlineanforde	rung)					
> 🙀 Zertifizierungsstelle (Lokal)	ist).	Kerberos-Authentifiz	ierung					
		RAS- und IAS-Server	ur					
		Router (Offlineanfor	derung)					
		Stammzertifizierung: Übergreifende Zertifi	stelle					
		Untergeordnete Zert	fizierungsstelle					
		Verzeichnis-E-Mail-F	eplikation		en			
		Webserver 1 Jahr						
		Webserver test						
		Zertifizierungsstellen	austausch					
< >	<					>		



Schritt 7

Daraufhin muss unter "Alternativer Name" der DNS-Name des Servers bzw. die IP-Adresse angegeben werden:

Prostycene run	Ausgestellt von	Ablaufdatum	Beabsichtigte Zwec	Anzeigename	Status	Aktionen	
EKGLab-SVR-02-C/	A EKGLab-SVR-02-CA	24.01.2028	<alle></alle>	<keine></keine>		Zertifikate	
EKGLab-SVD_MD_C	A EVGL 36.500.02.CA	24.01.2029	Alles	Noines		Million Alations	
Zeptication EKGLab-SVR-02-C/ EKGLab-SVR-02-C/ EKGLab-SVR-02-C/ Zetrif Zetrif Sie Sie	Ausgetent von Ausgetent von EVRLab-QVE.02-CA EVRLab-QVE.02-CA ikatregistrierung	Abilufbasum 24.01.2028 24.01.2028 24.01.2028 24.01.2028 24.01.2028 sint der Benutzer oder Computer, abionen über die zulässigen Akras ei in einem Zerbfikät verwendet we Benutzer oder Computer Hinzufügen > < Entfernen Chaese 20.045 servern servern	Besbischtigte Zwec cAlles rAlls rAlls für den das Zertifikkt gstellernarnen und erden dürfen. ebserver cAG dürfen. ver ebserver rAG stellernarnen und erden dürfen.	Anzeigename dicines	Status	Kkuonen Zertriikate Weitere Aktionen	
<		Hinzufügen > 192166	sbrechen Übernehmen	rechen	>		
	EKOLab-SVR-02-C.	Certifikateigenschaften Certifikateigenschaften Certifikateigenschaften Kick Certifikate	EXSLab-SVR-02-CA EXSLab-SVR-02-CA 24.01.2028 EXSLab-SVR-02-CA EXSLab-SVR-02-CA 24.01.2028 EXSLab-SVR-02-CA EXSLab-SVR-02-CA 24.01.2028 E	C EKGLab-SR-02-CA EKGLab-SR-02-CA 24.01.2028 <alle> EKGLab-SR-02-CA EVGLab-SR-02-CA 24.01.2028 <alle> Zetrifikatergistrierung </alle></alle>	Center Construction of the second se	Certofikationseinheit Fyp: Poddesse (vd) Vert Hinzufügen > Poddesse (vd) Vert Ken CK Abbrechen Ubernehmen Vert CK Abbrechen Vert CK CK Abbrechen Vert CK CK Abbrechen Vert CK CK Abbrechen Vert CK CK CK CK CK C CK C CK C C	 ENGLAD-SMR-02-CA Englad-Smr-02-CA

Schritt 8

Im nächsten Schritt wird die Standard-Vorlage "Webserver" ausgewählt:

Datel Aktion Ansicht Favoriten Fenster :									= 0' X
💠 🔶 🙍 💼 🗈 🔒 🖬 📷									
Consolenstamm	Ausgestellt für		Ausgestellt von	Ablaufdatum	Beabsichtigte Zwec	Anzeigename	Status	Aktionen	
 Zertifikate (Lokaler Computer) Einana Zastifikata 	EKGLab-SVR-02-CA		EKGLab-SVR-02-CA	24.01.2028	<alle></alle>	<keine></keine>		Zertifikate	-
 Eigen Zertifikate Vertrauenswördige Stammzertifizierungsstelle Organisationsvertrauen Organisationsvertrauen Vertrauenswördige Herauggeber Nicht vertrauensvärdige Zertifikate Orittanbieter-Stammzertifizierungsstellen Vertrauenswördige Zertifikate Orittanbieter-Stammzertifizierungsstellen Orittanbieter-Stammzertifizierungsstellen Stamme testen Stammetemente der Vorabversion Stammetesten Stammetesten Vertrauenswördige Stämme Vertrauenswördige Stämme Vertrauenswördige Stämme Vertrauenswördige Stämme Stertifikate Stammetestelle (Lokal) 	EKSLab COUR.D.C.A Zertifi Zer Kic Sie	Zertifikatei Anzeigen Zertifikat Anzeigen Webserv Beschreit	Exclusion Support	24 Att 3AD2	nd Verwendung eines	kiicken f. ails a sen ten		Weitere Aktionen	,
				OK ADD	reuren [ubernehmen]		,		



Schritt 9

Unter "Privater Schlüssel" muss die Option "Privaten Schlüssel exportierbar machen" gewählt werden:

Konsolenstamm	Ausgestellt für	Ausgestellt von	Ablaufdatum Beabsichtigte Zwec	Anzeigename	Status	Aktionen	
 Zertifikate (Lokaler Computer) 	EKGLab-SVR-02-CA	EKGLab-SVR-02-CA	24.01.2028 <alle></alle>	<keine></keine>		Zertifikate	
Vertrauenswindige Personalier Vertrauenswindige Stammzertifizierungssteller Vertrauenswindige Stammzertifizierungsstellen Vertrauenswindige Herausgeber Wertrauenswindige Herausgeber Wittauenswindige Personen Vertrauenswindige Personen Vertrauenswindige Personen Vertrauenswindige Personen Stammelemente der Vorsbversion Stamme teiten Remotedesktop Zenfikategistrierungsanforderungen	Aurgestellt tur Gelfstüb-SvR-02-CA Gelfstüb-AusmCA Gelfstüb-AusmCA Zertifik Zertifik Klict	Ausgezeitt von EKSLab-SVR-02-CA EKSLab-SVR-02-CA EKSLab-SVR-02-CA Stragsteler Algemein Erweiterunger Kryptografiedienstanbieter Schlüsseloptionen Legen Sie die Schlüssellsneu und die Expo Schlüsseloptionen	Ablaufdatum Beabichtigte Zwec 24 01:2028 cAlles 24 01:2028 cAlles Privater Schlüssel * rtoptionen für den privaten Schlüssel fest.	Kline> Kline> Kline> klicken r. ails ^ sen	Status	Zertöfikste Weitere Aktionen	,
 > (iii) Vertrauenswürdige Gerste > (iii Windows Live ID Token Issuer > (iiii Zertrifikatvorlagen > (iiiii Zertrifikatvorlagen) 		Collig Privaten Schlüssel ergondierbar machen Archivierung des privaten Schlüssels zu Verstärkter Schutz für den privaten Schl Schlüsselbyp Schlüsselberechtigungen	lassen üssel v	ten			
< >	٢		OK Abbrechen Übernehmen		>		

Schritt 10

Daraus wird eine Datei ausgegeben, diese muss in einem Editor geöffnet und der Inhalt kopiert werden:

CAtemplrequest/webserver-request - Notepad + + [Administrator]	-	Ø	×
Datei Bearbeiten Suchen Ansicht Codierung Sonache Einstellungen Werkzeuge Makros Ausführen Plugins Fenster ?		+ 1	• ×
🖮 webserver-request 🖸			
1BEGIN NEW CERTIFICATE REQUEST			^
2 MIIEFTCCAv0CAQAwTjELMAkGA1UECwwCaXQxDjAMBgNVBAoNBWRpbUFHNQ4wDAYD			- 11
3 VQQHDAVhZG9yZjELMAKGA1UECAwCZGUXEjAQBqNVBAMMCXd1YnN1cnZ1cjCCASIw			
4 DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKwoZx6XPBwHSWUVjHjwwmDepPBQ			
S YV1/L3VdvAuPoLgsCjq2vuf0oYt1gyj2+RmeenRL6kWev04WyZX6yTfV9msqjIEk			
6 yghRyeL8urMerReHfeGbwsq30L5r0/ptdyCEzTnYKhVb/fldzm531oa0ENIe18C4			
7 pasybyrCcQDJN)TO/UFTUATU7CgSDJIdHamMnnICNC2XV2+OaTgUSSTNU+3hrnw			
 ywcub / yokalica/Pookaki kgiwcub y ysabky bi // or zwojnobpub/kd2ka/shr y ybicka http://doi.org/10.1002/jite/			
10 AACCAYUHAYAWAINGCASOFOWNKCAULSINYELJUNGUJUNGUJUNGUJUNGUJUNG			
11 NTwwOgIBBOwWU125LTAVLUNELKVLROxhY15#b2NhbAwURUtHTEFCXGFkbWluaXNO			
12 cmF0b3IHB01NQy5FWEUwcgYKKwYBBAGCNw0CAjFkHGICAQEeWgBNAGkAYwByAG8A			
13 CWBVAGYAdAAgaFIAUWBBACAAUWBDAGgAYQBUAG4AZQBSACAAQWBYAHKACABDAG8A			
14 ZubyAGEAcABoAGkAYuAgAFAAcgBvAHYAAQBkAGUAcgHBADCBoAYJKoZIhvcNAQKO			
15 NYGSMIGPMCEGCS#GAQQBgjcUAgQUHhIAV#BIAGIAU#BIAHIAdgBIAHI#E#YDVRO1			
16 BAWWCGYIKWYBBQUHAWEUDGYDVROPAQH/BAQDAGWGRCYCAIUdEQQTHB2CCNNich21			
1/ CmshabwcCkalinnichzicoceuxgaszkadgwidyłejegdwkiwitasaji fwinobuluja			
10 ISENCE TANGUNAN TA			
20 hkm/s/ky/WS/kz/CM/6N/s/RC/6N/s/RC/6N/s/RC/60/LG/21/20/2/tD/Rio			
21 N200PMH40zenM4KmGEL40YR4ASuSFuu8Tm2e93Ab6IJGg12I836F43ue49vXDdv4			
22 WWcrFczky1SfMAHwJDtnn2Ixu3Eba91g69NdrFncr1Ke/t92u0G2LDpDxFq++285			
23 3jqHbHNtpDxRXEzW5dHqEXFa1/0xKtOeiGKv73GyShH2tPK8HwNBRgo=			
24END NEW CERTIFICATE REQUEST			
			_



Schritt 11

Anschließend müssen die Active-Directory-Zertifikatsdienste im Browser geöffnet werden:

Microsoft-Active Directory-Zertif ×	+																	v		-	L	1	~
← → C ③ localhost/certsrv/	/																	Ŀ	☆	0			:
Microsoft-Active Directory-Zertifikatdienst	ste – E	EKGLa	ab-SVF	/R-02-0	2-CA	A																Start	seite
Willkommen																							
Auf diese Website können Sie ein Z einem Zertifikat können Sie Ihre Ide bestätigen, E-Mail-Nachrichten sign angeforderten Zertifikattyp, durchfüh	Zertifil entität nieren uhren.	kat für geger 1 oder	ir den inübei r versi	n Web er and schlüs	lebbr Indere	brov eren seln	en L In u	wse n Le i uno	er, E eute nd w	E-M en, r veite	lail- mit ere	Clie den Sicl	ent hen her	ode Sie rheit	er and übe tsauf	dere r da gab	Prog s We en, a	gram eb ko bhàn	me a mmu igig v	infor inizi∉ ∕om	dei ere	m. N n,	/lit
Sie können diese Website auch zur Zertifikatssperrliste verwenden, ode	um Dov ler Sie	wnloa könne	ad ein nen de	nes Zo den St	Zerti Statu	ertifiz atus	ifizie Is ei	zien ein/	erung ner a	gsst aus	telle stel	enze hen	ertif ider	fikat n Ar	ts, ei nford	ner 3 erun	Zertif g an	ikatk zeige	ette (en.	oder	r ei	ner	
Weitere Informationen zu Active Dir Zertifikatdienstedokumentation.	irectory	y-Zerti	tifikato	atdiens	enste	te ei	erh	rhal	alten	n Si	e ur	nter	Ac	ctive	Dire	ector	y₌						
Wählen Sie eine Aufgabe: Ein Zertifikat anfordem	anzeio	Gen																					

Schritt 12

Dort muss "Ein Zertifikat anfordern" und dort "Erweiterte Zertifikatanforderung" gewählt werden:

Microsoft-Active Directory-Zertifix +	~	-	(×
← → C ③ localhost/certsrv/certrqus.asp	Ŀ	☆		٤	:
Microsoft-Active Directory-Zertifikatdienste EKGLab-SVR-02-CA			- 3	Starts	eite
Zertifikat anfordern					_
Wählen Sie den Zertifikattyp: Benutzerzertifikat oder senden Sie eine enweiterte Zertifikatanforderung ein.					



Schritt 13

In das Feld **"Base-64-codierte Zertifikatanforderung"** muss der zuvor kopierte Inhalt eingefügt werden, die restlichen Felder können leer bleiben:

Microsoft-Active Directory-Zertifikatdienste EKGLab-SVR-02-CA	Startseite
Zertifikat- oder Erneuerungsanforderung einreichen	
Fügen Sie eine Base-64-codierte CMC- oder PKCS #10-Zertifikatanforderung oder eine PKCS #7- Erneuerungsanforderung, die von einer externen Quelle (wie z.B. einem Webserver) generiert wurde, in das Fel "Gespeicherte Anforderung" ein, um eine gespeicherte Anforderung bei der Zertifizierungsstelle einzureichen.	d
Gespeicherte Anforderung:	
Base-64-codierte Zertifikatanforderung (CMC oder PKCS #10 oder PKCS #7):	
Zertifikatvorlage:	
Benutzer V	
Zusätzliche Attribute:	
Attribute:	
Einsenden >	

Schritt 14

Nach einem Klick auf **"Einsenden"** kann das signierte Zertifikat heruntergeladen werden. Dieses muss dann im Explorer durch Doppelklick geöffnet werden:

Name	Änderungsdatum	Тур	Größe
	24.01.2023 16:18	Dateiordner	
🔄 certnew (1).cer	24.01.2023 16:36	Sicherheitszertifikat	2 KB
🔄 certnew (1).p7b	24.01.2023 16:36	PKCS #7-Zertifikate	6 KB



Schritt 15

Im darauf folgenden Dialog muss **"Zertifikat installieren"** gewählt werden und dem Assistenten gefolgt:

Zeronkat	~
gemein Details Zertifizierungspfad	
Zertifikatsinformationen	
Dieses Zertifikat ist für folgende Zwecke beabsichtigt: • Gwantiet die Identifikt eines Remotercomputers	_
Ausoestellt für: webserver	-
Ausgestellt von: EKGLab-SVR-02-CA	
Gültig ab 24.01.2023 bis 23.01.2025	
Zertifikat installeren Ausstellererkla	rung
	ж

Schritt 17

Dies muss mit einem Klick auf **"Fertig stellen"** bestätigt werden:

100		×
Zertifikatimport-Assisten	at in the second se	
Fertigstellen des	Assistenten	
Das Zertifikat wird importie	ort, nachdem Sie auf "Fertig stellen" gokäckt haben.	
Sie haben folgende Einstel	lungen ausgewählt:	1
Yom Benutzer gewahlter Inhalt	Zertifikat	

Schritt 16

Im nächsten Schritt wird ein Zertifikatspeicher gewählt, hier sollte **"Eigene Zertifikate"** gewählt werden:

Zertifikatimport-Assistent	
Zertifikatspeicher	
Zertifikatspeicher sind Systembereiche, in	denen Zertifikate gespeichert werden.
Windows kann automatisch einen Zertfikal Speicherort für die Zertfikate angeben. Zertfikatspeicher automatisch ausw	tspeicher auswählen, oder Sie können einen vählen (auf dem Zertäfikattyp basierend) er speichern
Zertifikatspeicher:	[ensurements of the second sec
Eigene Zertifikate	Durchsuchen
	Weiter Abbreck

Schritt 18

Dies wird bestätigt:





Schritt 19

Anschließend erscheint das Zertifikat in der Liste und kann über "Alle Aufgaben -> Exportieren" exportiert werden:

Konsolenstamm	Ausgestellt	tfür ^	Ausgestellt von	Ablaufdatum	Beabsichtigte Zwec	Anzeigename	Status	Aktionen				
 Zertifikate (Lokaler Computer) Eigene Zertifikate 	EKGLab-SVR-02-CA		EKGLab-SVR-02-CA	24.01.2028	8 <alle></alle>	<keine></keine>		Zertifikate	-			
C Zertifikate	E EKGLab	-SVR-02-CA	EKGLab-SVR-02-CA EKGLab-SVR-02-CA	23.01.2028	<alle></alle>	<keine></keine>		Weitere Aktionen	,			
> 2 Vertrauenswürdige Stammzertifizierungsstelle > 2 Organisationsvertrauen		Öffnen						webserver				
> Zwischenzertifizierungsstellen		Alle Aufgaben	> Öffnen					Weitere Aktionen	,			
 Vertrauenswürdige Herausgeber Nicht vertrauenswürdige Zertifikate Drittanbieter-Stammzertifizierungsstellen 	A K L E				Ausschneiden Kopieren	Zertifikat mit neuem Zertifikat mit neuem	Schlüssel anfordern Schlüssel erneuern					
 Vertrauenswürdige Personen Clientauthentifizierungsaussteller Stammelemente der Vorabversion 		Löschen Eigenschaften	Private Schlüssel ver Enweiterte Vorgänge	walten	>							
> 🛄 Stämme testen > 🛄 Remotedesktop		Hilfe	Exportieren									
Zertöfikätregisthierungsanforderungen Smattard vertrauen würdige Stämme Webhosting Webhosting Webhosting Webhosting Zertöfikatvorlagen Zertöfikatvorlagen												

Schritt 20

Auch hier muss wieder einem Assistenten gefolgt werden:

🗢 🔿 🙍 📷 🔏 🗞 🗙 🗟 🔒 🖬 📷								1
Konsolenstamm	Ausgestellt für	Ausgestellt von	Ablaufdatum	Beabsichtigte Zwec	Anzeigename	Status	Aktionen	
 Zertifikate (Lokaler Computer) 	EKGLab-SVR-02-				× Seine>		Zertifikate	
 Eigene Zertifikate Zertifikate 	SVR-02- SVR-02-	🚱 Zertifikatexport-Assistent			leine> :bserver		Weitere Aktionen	•
Organisationsvertrauen							webserver	-
Vertrauensvürdige Stammærtfrüerungsstelle Organisationvertrauen Zvisichenzentfrüerungsstellen Vertrauensvürdige Zertifikate Drittanbieter-Stammærtfrüerungsstellen Vertrauensvürdige Zertifikate Oritanbieter-Stammærtfrüerungsstellen Vertrauensvürdige Sersite Stammelemente der Vorabversion Stamme teisten Remotedeiktop Zvisifikategistrierungsanforderungen Vertrauensvürdige Gerste Vertrauensvördige Gerste Vertrauensvördige Losal Zertifizierungsstelle (Lokal)		Willkommen Deser Assistent hift Ihnen bein Kopi und zertifikelsoperitaten von zertifik Ein von einer Zertifizierungsstelle aus sen schaft Informationen für den Dek Netzwerkverbeindungen. Ein Zertifikels gespeichert werden.	sren von Zertfikaten, Zertfik stopicher auf den Datonträg gestelltes Zertfikat dent der roschutz oder für den Aufba speicher ist der Systembereic ang fortzusetzen.	atvertrauenslisten er. IdentRitsbestAbigung. sicherer h, in dem Zertifikate			Weitere Aktionen	,
< >	<					>		



Schritt 21

Im nächsten Schritt muss "Ja, privaten Schlüssel exportieren" gewählt werden:

	Ausgestellt für		Ausgestellt von	Ablaufdatum	Beabsichtigte Zwec	Anzeigename	Status
	EKGLab-SVR-02-					× leine>	
	EKGLab-SVR-02-					(eine>	
igsstelle	webserver	4	F Zertifikatexport-Assistent			:bserver	
			Printen Critikal synodiates				
			Sie können den privaten Schlüssel mit d	em Zertifikat exportieren.			
llen							
			Private Schlüssel sind kennwortgeschütz	at. Wenn Sie den privaten	Schlüssel mit dem		
			Seiten ein Kennwort eingeben.	uncen, mussen sie dur eine	r der rolgenden		
			Möchten Sie mit dem Zertifikat auch den	privaten Schlüssel export	eren?		
			Ia. privaten Schlüssel exportien	00			
e							
			Orien, privaten schussel nicht es	porceren			

Schritt 22

Daraufhin muss die Option "PKCS #12" gewählt werden:

	CHOCAD . SAM. OF.			seme >	Weiter
mmzertifizierungsstelle	webserver	4	Zertifikatexport-Assistent	:bserver	
1					webserver
sstellen					Weiter
ausgeber			Format der zu exportierenden Datei		
ge Zertifikate			Zertitikate konnen in verschiedenen Dateiformaten exportiert werden.		
rtifizierungsstellen				-	
sonen			Wiklen Sie der neurünschte Format:		
saussteller					
rapversion			O DER-codiert-binär X.509 (.CER)		
			Base-64-codiert X.509 (.CER)		
anforderungen			 Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P78) 		
ürdige Stämme			Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen		
Ste			Privater Informationsaustausch - PKCS #12 (.PFX)		
Issuer			Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen		
			Privaten Schlüssel nach erfolgreichem Export löschen		
			Alle erweiterten Eigenschaften exportieren		
			Zertifikatdatenschutz aktivieren		
			O Microsoft Serieller Zertifikatspeicher (.SST)		
			Weiter Abbrechen		
				-	



Schritt 23

Im nächsten Schritt muss das Zertifikat mit einem **Passwort** geschützt werden, hier kann ein Dummy-Passwort gewählt werden, ein leeres Passwort oder kein Passwort wird aber u.U. abgelehnt:

	COLLOCOD-SALLAS.				X terriez	2.eronicate
Zertifikate	EKGLab-SVR-02-				(eine>	Weitere Aktionen
ifikate	webserver	4	Zertifikatexport-Assistent		bserver	Weitere Aktionen
enswürdige Stammzertifizierungsstelle						webserver
ationsvertrauen						Million Alations
enzertifizierungsstellen						Weitere Aktionen
enswürdige Herausgeber			Sicherheit	the field of the state		
ertrauenswürdige Zertifikate			Zur Gewähnleistung der Sicherheit mussen sie den prin Sicherheitsnrinzinal oder mithilfe eines Kennworts schi	aten Schlussel mit einem		
ieter-Stammzertifizierungsstellen				na sta		
inswürdige Personen			Gruppen- oder Benutzernamen (empfohlen)			
thentifizierungsaussteller				Mar Kines		
elemente der Vorabversion				Hinzurügen		
e testen				Entheman		
desktop				LINGTON		
tregistrierungsanforderungen						
rd vertrauenswürdige Stämme						
enswürdige Geräte						
ting						
is Live ID Token Issuer						
rlagen			Kennwort:			
asstelle (Lokal)			••••			
ground (const)			Kannungh hard blinger.	·		
			Reinmore bestaugen.	6		
			•••••			
			Verschlusslung: TrislaDEC.Gub1			
			rescription of the second seco			
				<u>_</u>		
				Weiter Abbrecher	a	
					and a second sec	

Schritt 24

Die daraus resultierende **.pfx-Datei** muss nun auf den **Server** übertragen werden. Bei IIS kann diese direkt verwendet werden, zur Verwendung mit nginx oder dem Apache httpd muss eine .crt- und eine .key-Datei erzeugt werden. Dies geht mit openssl:

openssl pkcs12 -in beispiel.pfx -clcerts -nokeys -out beispiel.crt openssl pkcs12 -in beispiel.pfx -nocerts -nodes -out beispiel.key Wurde zuvor ein Passwort gesetzt, kann es von der .key-Datei entfernt werden: openssl rsa -in beispiel.key -out beispiel-unlocked.key Dazu muss einmalig das Passwort eingegeben werden.