# Extended Validation Zertifikate von einer Windows Server 2008 R2 CA ausstellen

## CA Verwaltung starten

Doppelte Zertifikatvorlage von der Zertifikatvorlage Webserver

Name fuer die Vorlage waehlen

Eigenschaften der neuen Vorlage 🛛 🛛 🛛				
Antragstellername Server Ausstellungsvoraussetzungen Abgelöste Vorlagen Erweiterungen Sicherheit Allgemein Anforderungsverarbeitung Kryptografie				
Vorlagenanzeigename:				
Webserver-ExtendedValidation				
Unterstützte Zertifi- zierungsstellen (Min.): Windows Server 2008 Enterprise				
Vorlagenname:				
Webserver-ExtendedValidation				
Gültigkeitsdauer: Erneuerungszeitraum:				
Zettitikat in Active Directory veroftentlichen     Nicht automatisch neu registrieren, wenn ein identisches Zertifikat     bereits in Active Directory vorhanden ist				
Vorhandenen Schlüssel für automatische Erneuerung von Smattcardzertifikaten verwenden, falls Erstellung eines neuen Schlüssel nicht möglich ist				
OK Abbrechen Übernehmen Hilfe				

Erweiterungen – Ausstellungsrichtlinien – Neue Ausstellungsrichtlinie

Eigenschaften der neuen Vorlage	X
Antragstellername Server Ausstellungsvoraussetzur	ngen   Anmeldung
Allgemein Anforderungsverarbeitung Kryptogra	afie
Abgelöste Vorlagen Erweiterungen Sicherh	heit
Markieren Sie eine Erweiterung, und klicken Sie auf "Bearbeiten", um zu ändern.         Erweiterungen in dieser Vorlage:         Anwendungsrichtlinien         Basiseinschrächtinien         Schtil Ausstellungsrichtlinien         Schtil Ausstellungsrichtlinien         Bedingungen ein Zertifikat	Anmeldung, KDC-Authentifizierung Anmeldung, KDC-Authentifizierung en K die Ausstellungsbedingungen eines ungsrichtlinie für die von dieser Vorlage
Alle ausgegebenen Richtlinien Europisches qualifiziertes Zertifizet Hinzufüge Hinzufüge Diese Erweiter	At           Neue Ausstellungsrichtlinie         X           Geben Sie für die neue Richtlinie einen Namen und einen Pfad für die Zettifikatverwendungserklärung (CPS) ein, und ändern Sie die Dbjektkennung (falls erforderlich).         Name:           I         Pfad für die Zettifikatverwendungserklärung:         Dbjektkennung:           I         Dijektkennung:         Dijektkennung:           I         Markenung:         Dijektkennung:           I         Dijektkennung:         Dijektkennung:           Dijektkennung:         Dijektkennung:         Dijektkennung:

Namen vergeben, Pfad fuer die Zertifikatverwendungserklaerung angeben und die Objektkennung in die Zwischenablage kopieren.

Ausstellungsrichtlinie bearbeiten       ×         Geben Sie den neuen Namen oder den Pfad für die       Zertifikatverwendungserklärung (CPS) dieser Richtlinie ein.
Name: Extended Validation Certificate
Pfad für die Zertifikatverwendungserklärung: http://
Objektkennung:           1.3.6.1.4.1.311.21.8.478657.590420.542910.1800917.2024904.17.74332
0K Abbrechen
Ausstellungsrichtlinienerweiterung bearbeiten 🛛 💌
Eine Ausstellungsrichtlinie beschreibt unter welchen Bedingungen ein Zertifikat ausgestellt werden darf.
Ausstellungsrichtlinien:
Hinzufügen Bearbeiten Entfernen
OK Abbrechen

Diese Erweiterung als kritisch markieren NICHT aktivieren. Berechtigungen fuer Domaenen-Computer zum Einschreiben des Zertifikats setzen

		?
Antragstellername A	usstellungsvora	ussetzungen
Allgemein Anforderungsvera	rbeitung	Kryptografie
Abgelöste Vorlagen Erweiterunge	n Sicherł	neit Server
Gruppen- oder Benutzernamen:		
🍇 Authentifizierte Benutzer		
🤱 Administrator (administrator@dittation		
Somänen-Admins (	n-Admins)	
Somänencomputer (States Domär	encomputer)	
🚜 Organisations-Admins 🛲 Orga	nisations-Admin	s)
🚜 Domänen-Benutzer 🗰 Domäner	-Benutzer)	
Momänencomputer Domäner	computer)	
	Uissufiliass	Entformon
	minzulüden	
"Berechtigungen für "Domänencomputer	Zulanna	Nerweigern
Berechtigungen für "Domänencomputer"	Zulasse	n Verweigern
Berechtigungen für "Domänencomputer" Vollzugriff	Zulasse	n Verweigern
Berechtigungen für "Domänencomputer" Vollzugriff Lesen	Zulasse	n Verweigern
Berechtigungen für "Domänencomputer" Vollzugriff Lesen Schreiben	Zulasse	
Berechtigungen für "Domänencomputer" Vollzugriff Lesen Schreiben Registrieren		n Verweigern
Berechtigungen für "Domänencomputer" Vollzugriff Lesen Schreiben Registrieren Automatisch registrieren		n Verweigern
Berechtigungen für "Domänencomputer" Vollzugriff Lesen Schreiben Registrieren Automatisch registrieren		n Verweigern
Berechtigungen für "Domänencomputer" Vollzugriff Lesen Schreiben Registrieren Automatisch registrieren	Zulasse D D D D	n Verweigern
Berechtigungen für "Domänencomputer" Vollzugriff Lesen Schreiben Registrieren Automatisch registrieren Klicken Sie auf "Erweitert", um spezielle Berechtigungen anzuzeigen.	Zulasse U U U	n Verweigem
Berechtigungen für "Domänencomputer" Vollzugriff Lesen Schreiben Registrieren Automatisch registrieren Klicken Sie auf "Erweitert", um spezielle Berechtigungen anzuzeigen.	Zulasse	Verweigern     Verweigern     Erweitert tigungen
Berechtigungen für "Domänencomputer" Vollzugriff Lesen Schreiben Registrieren Automatisch registrieren Klicken Sie auf "Erweitert", um spezielle Berechtigungen anzuzeigen. Weitere Informationen über Zugriffssteuer	Zulasse	Verweigern     Verweigern     Erweitert tigungen
Berechtigungen für "Domänencomputer" Volzugriff Lesen Schreiben Registrieren Automatisch registrieren Klicken Sie auf "Erweitert", um spezielle Berechtigungen anzuzeigen. Weitere Informationen über Zugriffssteuer	Zulasse	Criterion     Verweigern     Constant     Constant

#### RootCA Zertifikat exportieren, um dieses per GPO neu zu verteilen



Gruppenrichtlinie erstellen um das RootCA Zertifikat erneut auf die betreffenden Clients/Server zu importieren. Das RootCA Zertufukat wurde ja bereits bei Domaenenbeitritt der Clients/Server per Enterprise Cert Store in den Zertifikatspeicher der vertrauenswuerdigen Stammzertifizierungsstellen importiert und muss jetzt ausgetauscht werden, damit die erweiterte Zertifikatpruefung auch die OID des Zertifikats basierend auf der neuen EV-Zertifikatvorlage enthaelt. Nach dem Import auf der Registerkarte "Erweiterte Ueberpruefung" die OID aus der vorher erstellten Zertifikatvorlage kopieren.



#### Altes Root CA Zertifikat zum testen entfernen (Zertifikatspeicher Computer)

Konsole1 - [Konsolenstamm\Zertifikate (Lokaler Computer)\Vertrauenswürdige Stammzertifizierungsstellen\Zertifikate]							
Datei Aktion Ansicht Favoriten Fenster ?							
Konsolenstamm	Ausgestellt für 🔺	Ausgestellt von	Ablaufdatum	Beabsichtigte Zwecke	Anzeigename		
🖃 🔜 Zertifikate (Lokaler Computer)	🔄 Class 3 Public Primary Certification	Class 3 Public Primary Certification A	02.08.2028	Sichere E-Mail, Client	VeriSign Class		
🖃 🚞 Eigene Zertifikate	🔄 Class 3 Public Primary Certification	Class 3 Public Primary Certification A	08.01.2004	Sichere E-Mail, Client	VeriSign		
🔛 Zertifikate	🔄 Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	31.12.1999	Zeitstempel	Microsoft Time		
Vertrauenswürdige Stammzertifizierung	🔄 GTE CyberTrust Global Root	GTE CyberTrust Global Root	14.08.2018	Sichere E-Mail, Client	GTE CyberTrus		
Zertihkate	🔄 Microsoft Authenticode(tm) Root	Microsoft Authenticode(tm) Root Au	01.01.2000	Sichere E-Mail, Code	Microsoft Auth		
Urganisationsvertrauen	🔄 Microsoft Root Authority	Microsoft Root Authority	31.12.2020	<alle></alle>	Microsoft Root		
🛨 🔛 Zwisu ienzerunzierungsstellen	🔄 Microsoft Root Certificate Authority	Microsoft Root Certificate Authority	10.05.2021	<alle></alle>	Microsoft Root		
Vertrauenswurdige Herdusgeber     Micht vertrauenswürdige Zertifikate	NO LIABILITY ACCEPTED, (c)97 V	NO LIABILITY ACCEPTED, (c)97 Veri	08.01.2004	Zeitstempel	VeriSign Time S		
Drittanbieter-Stammzertifizierungsstellu	RootCA	RootCA	01.08.2016	<alle></alle>	<keine></keine>		
Vertrauenswürdine Personen	🔄 Thawte Premium Server CA	Thawte Premium Server CA	01.01.2021	Serverauthentifizieru	thawte		
Remote Desktop	🔄 Thawte Server CA	Thawte Server CA	01.01.2021	Serverauthentifizieru	thawte		
The second seco	🔄 Thawte Timestamping CA	Thawte Timestamping CA	01.01.2021	Zeitstempel	Thawte Timest		
🕀 🧮 SMS	🔄 UTN-USERFirst-Object	UTN-USERFirst-Object	09.07.2019	Verschlüsselndes Dat	USERTrust		
표 🚞 Vertrauenswürdige Geräte	🔄 VeriSign Class 3 Public Primary Cer	VeriSign Class 3 Public Primary Certifi	17.07.2036	Serverauthentifizieru	VeriSign		
	🔄 VeriSign Commercial Software Pub	VeriSign Commercial Software Publis	08.01.2004	Sichere E-Mail, Code	VeriSign		
	🔄 VeriSign Trust Network	VeriSign Trust Network	19.05.2018	Sichere E-Mail, Client	VeriSign		
	🔄 VeriSign Trust Network	VeriSign Trust Network	02.08.2028	Sichere E-Mail, Client	VeriSign		

**GPUPDATE /FORCE** 

Eigenschaften des "neuen" Root CA Zertifikats - Erweiterte Ueberpruefung

ertifikat	Ē			
Allgemein Details Zertifizierungspf	ad			
Feld	Wert  Digitale Signatur, Zertifikatsign 5b 05 0f a3 35 ea 02 65 5a 71			
<ul> <li>Sperrlisten-Verteilungspunkte</li> <li>Version der Zertifizierungsst</li> <li>Basiseinschränkungen</li> <li>Fingerabdruckalgorithmus</li> </ul>	[1]Sperrlisten-Verteilungspunk V0.0 Typ des Antragstellers=Zertifi sha1			
Erweiterte Überprüfung	[1]Zertifikatrichtlinie:Richtlinie			
[1]Zertifikatrichtlinie: Richtlinienbezeichner= Informationen: [1,1]Richtlinienkennzeichnerinformationen: Kennung des Richtlinienqualifizierers=Stammprogrammkennzeichen Qualifizierer: c0				
Eigenschaften bearbeiten         In Datei kopieren           Weitere Informationen über Zertifikatdetails				
	ОК			

Neues Zertifikat basierend auf der neuen Zertifikatvorlage anfordern

Neben dem CN (Common Name) sind auch die die X.509 Attribute C (Country) und O (Organisation) wichtig. Diese werden dann vom Webbrowser bei der Validierung des EV Zertifikats verwendet. Ohne diese Werte zeigt der Webbrowser bei der EV-Validierung "Unbekannt" an.

🛜 Konsole1 - [Konsolenstamm\Zertifikate (L	.oka	aler Computer)\Eigene Zertifikate\Ze	rtifikate]					_ 🗆 ×						
🚡 Datei Aktion Ansicht Favoriten Fenste	er	?						_ 8 ×						
🗢 🔿 🙍 🖬 📋 🧟 😹 🚺														
Consolenstamm	Aur	panetallt frie 🔺 🛛 Aura	actallt uan	Ablaußdabum	Doshrichtista Zuarka	^gename	Aktionen							
🖃 🔜 Zertifikate (Lokaler Computer)	۴,	Zertifikatregistrierung					Zertifikate	<b>A</b>						
E Eigene Zertifikate				ſ	1 1			📮 Zertifikatregistrierung					Weitere Aktionen	•
Zertrinate     Vertrauenswürdige Stammzertifizierung		[					Welcere Ancionen	,						
Zertifikate		Zertifikate anfordern												
Organisationsvertrauen														
Zwischenzerünzerungsstellen     Vertrauenswürdige Herausgeber		Folgende Zertifikattypen sind abru anschließend auf "Registrieren".	bar. Wählen Si	e die Zertifikate aus, die Sie anforder	'n möchten, und klicken Sie									
🗉 🧮 Nicht vertrauenswürdige Zertifikate														
Drittanbieter-Stammzertifizierungsstell		Webserver-EV		CTATHE Verführer	Detaile (18)									
Centradenswardige Personen		Es werden zusätzliche	Informationen	für diese Zertifikatsregistrierung ben	ötigt. Klicken Sie bier, um									
🗉 🧮 Smartcard vertrauenswürdige Stämme		🐴 die Einstellungen zu k	onfigurieren.											
🗄 🦲 SMS		Die folgenden Optionen besc	nreiben die Vei	Zertifikateigenschaften			×							
		Schlüsselverwendung:	Digitale Sign	Privater Schlüssel	Zertifizierungsstelle	1	Signatur							
		Anwendungsrichtinien:	Schlüsselver Serverauthe	🔥 Antragsteller	Allgemein	Erweit	erungen							
		Gültigkeitszeitraum (Tage	): 730	Der Antragsteller eines Zertifikats i	ist der Benutzer oder Computer	, für den das Ze	rtifikat							
				ausgestellt ist. Geben Sie Informat Namenswerte ein, die in einem Zer	tionen über die zulässigen Antra tifikat verwendet werden dürfe	igstellernamen i n.	ind alternative							
		E a a a		Zertifikatsantragsteller			I							
		I Alle vorlagen anzeigen		Der das Zertifikat empfangende Be	enutzer oder Computer									
		Weitere Informationen über Zertifi	<u>cate</u>	Antragstellername:										
				Тур:	c	N=snamedseksing =DE								
				Ort 💌	Hinzufügen > 0									
				Wert:	< Entfernen									
					< Likromon									
				Alternativer Name:										
				Тур:										
				Verzeichnisname 💌										
				Wert:										
					Hinzufügen >									
	•				< Entformon									
					< uniforment									
	_							,						
				Weitere Informationen über Antrac	gstellernamen									
					OK	Abbrechen	Übernehmen							
						need conton								

Test des neu erstellten Zertifikats im Webbrowser



## Zertifikat Eigenschaften



#### **Issuance Policies fuer eine Enterprise Subordinate CA**

Wenn EV Zertifikate oder andere CPS von einer Sub CA ausgestellt werden ist darauf zu achten, dass die Issurance Policies entsprechend in der CAPOLICY.INF gesetzt sind. Ist keine CAPOLICY.INF vorhanden muss diese erstellt werden und anschließend das Sub CA Certificate Offline gegen die Offline Root CA erneuert werden. Wie das geht steht hier:

http://www.it-training-grote.de/download/Issuance-Policies-SubCA.pdf