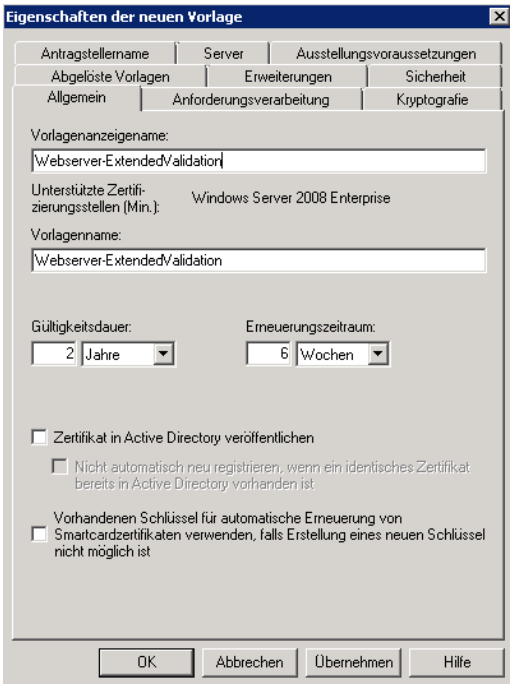
Extended Validation Zertifikate von einer Windows Server 2008 R2 CA ausstellen

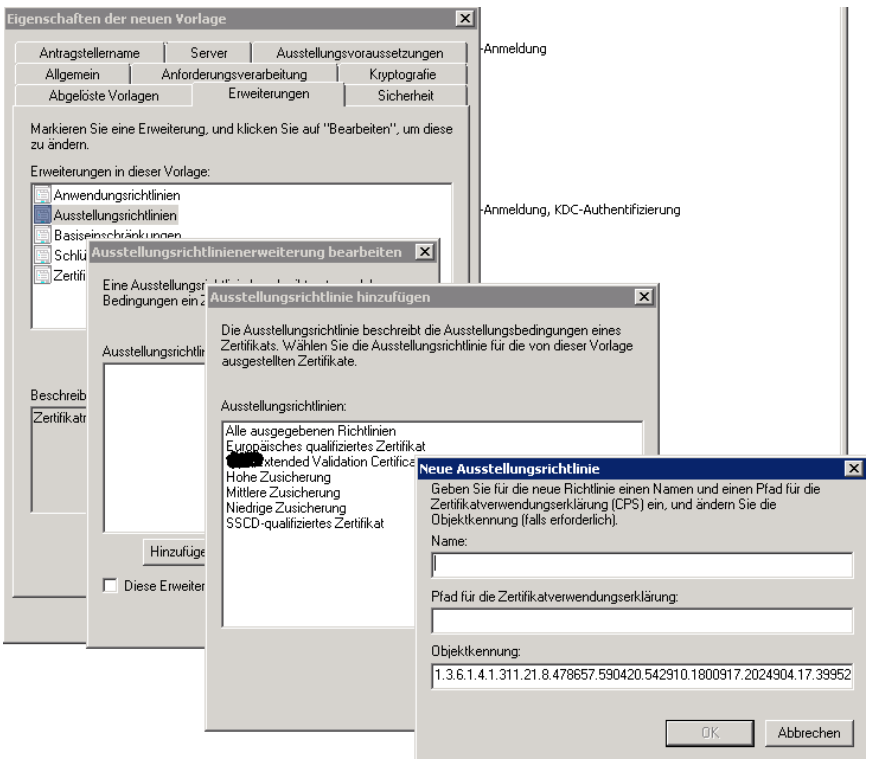
CA Verwaltung starten

Doppelte Zertifikatvorlage von der Zertifikatvorlage Webserver

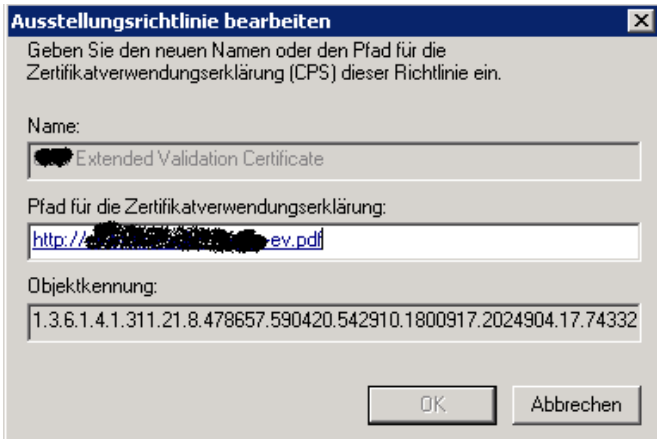
Name fuer die Vorlage waehlen



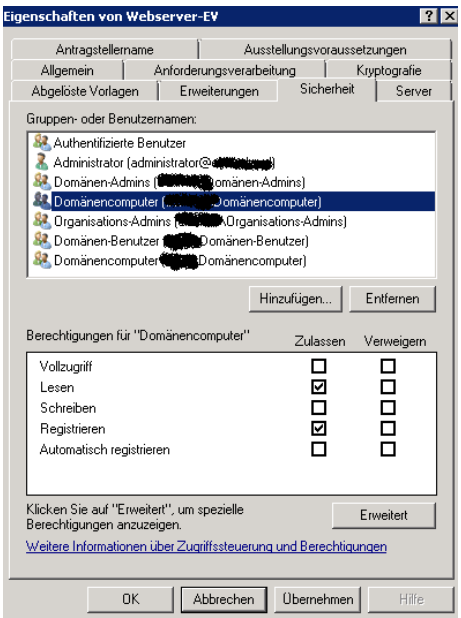
Erweiterungen – Ausstellungsrichtlinien – Neue Ausstellungsrichtlinie



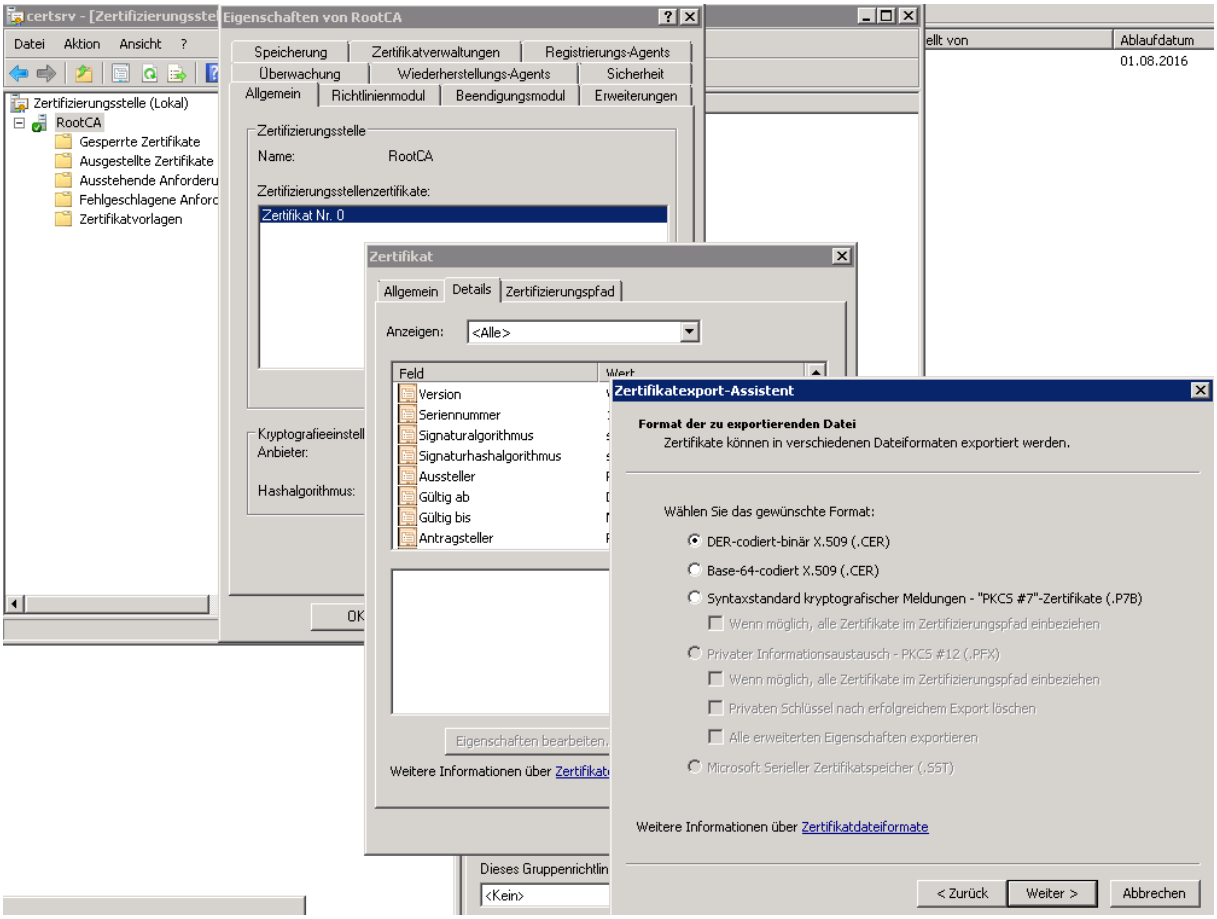
Namen vergeben, Pfad fuer die Zertifikatverwendungserklaerung angeben und die Objektkennung in die Zwischenablage kopieren.



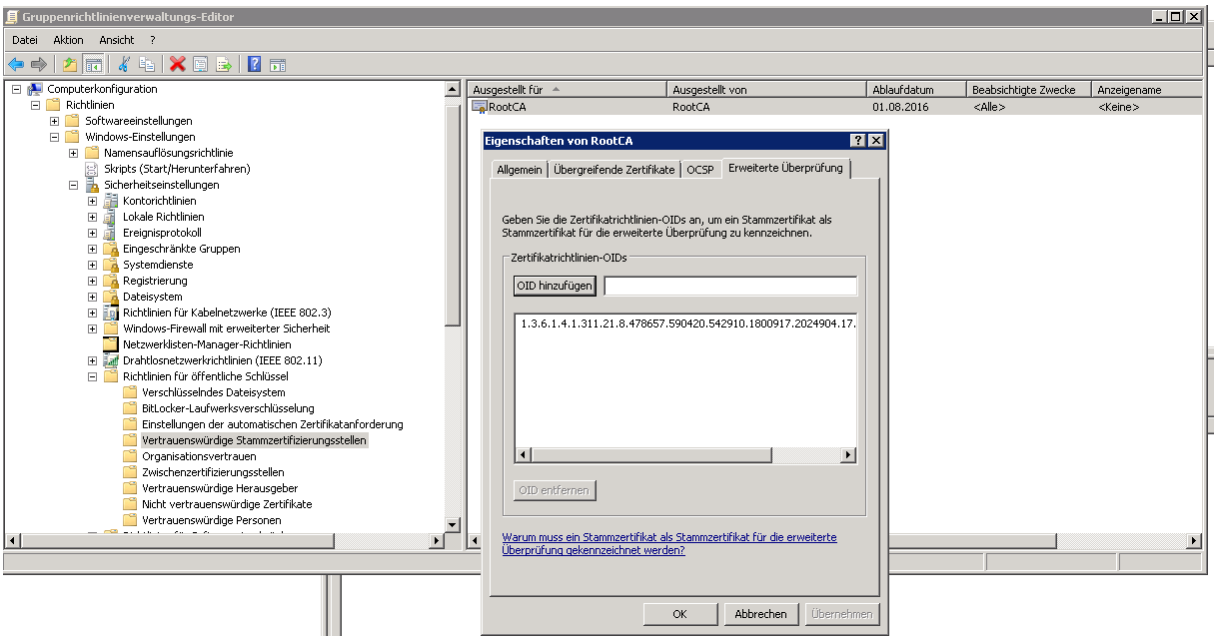
Diese Erweiterung als kritisch markieren NICHT aktivieren.
Berechtigungen fuer Domaenen-Computer zum Einschreiben des Zertifikats setzen



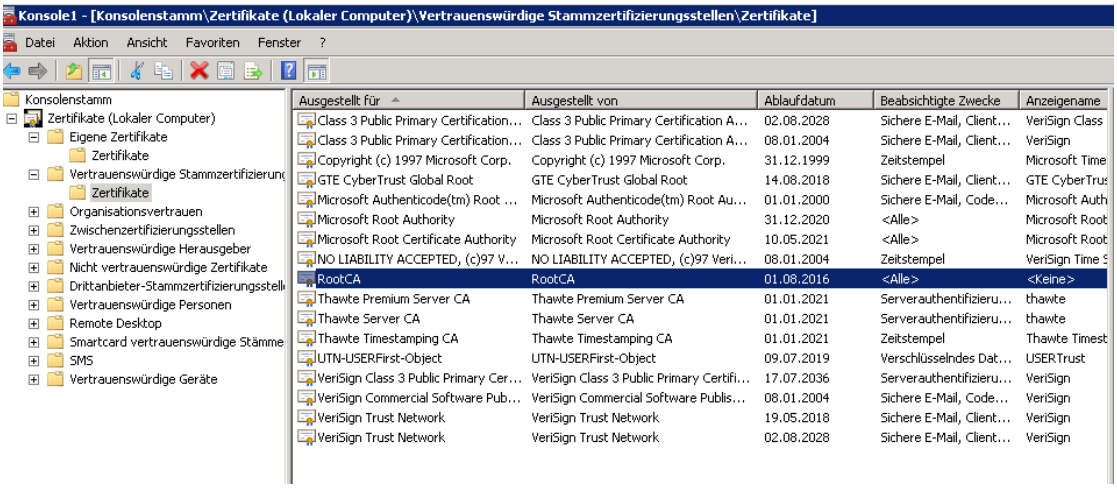
RootCA Zertifikat exportieren, um dieses per GPO neu zu verteilen



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.

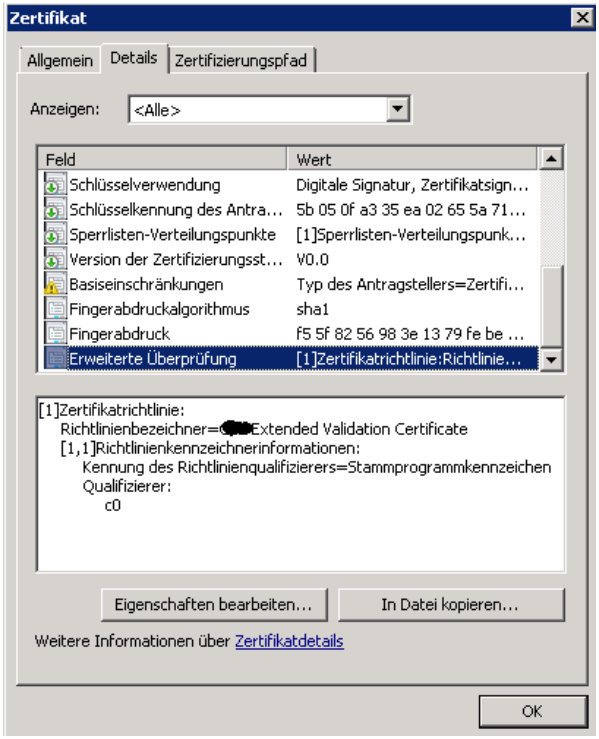


Altes Root CA Zertifikat zum testen entfernen (Zertifikatspeicher Computer)

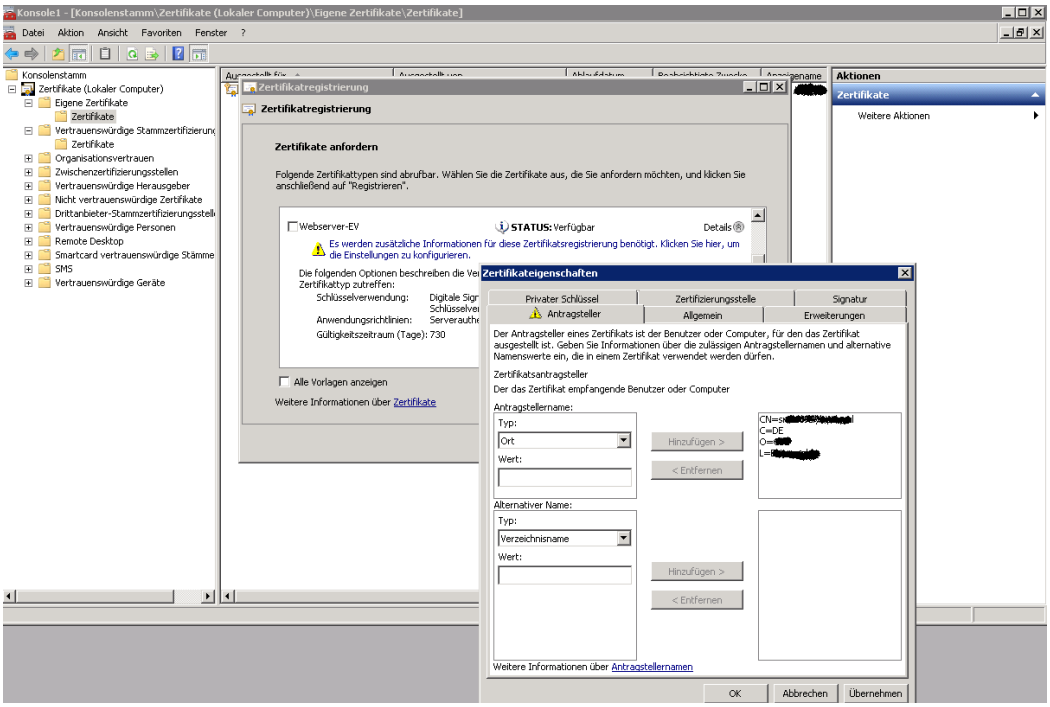


GPUPDATE /FORCE

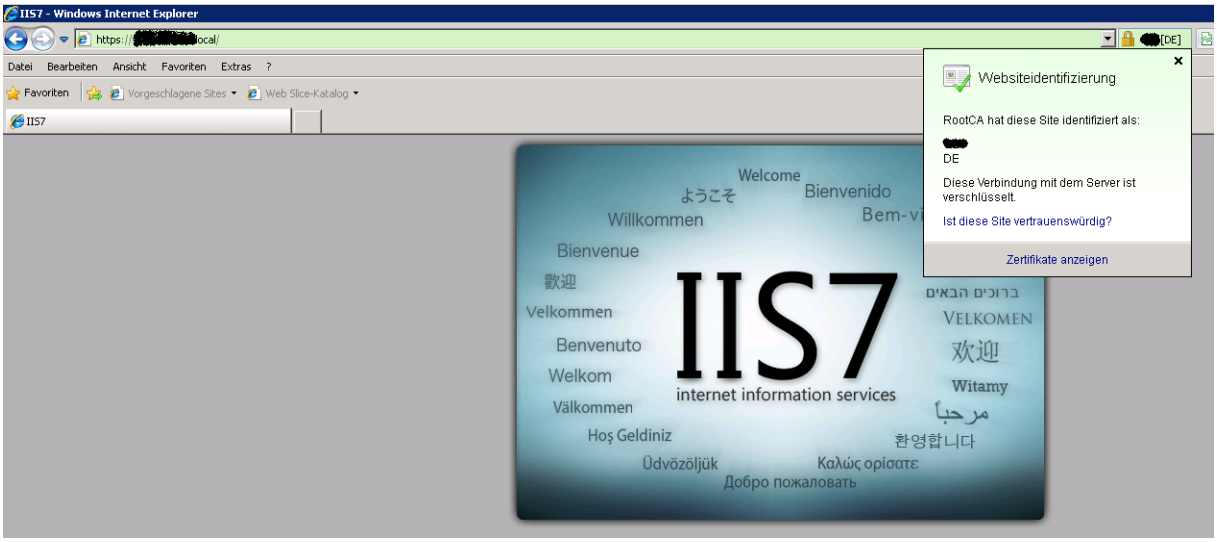
Eigenschaften des „neuen“ Root CA Zertifikats - Erweiterte Ueberpruefung



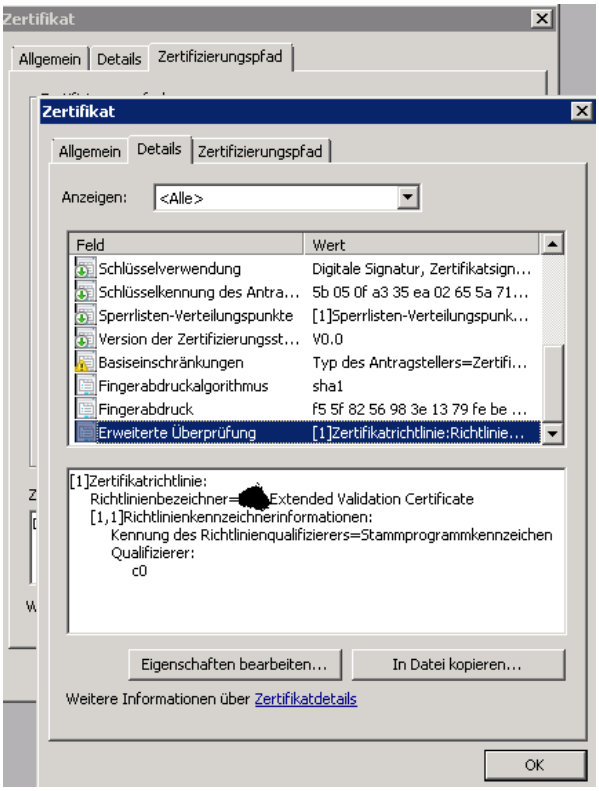
Neues Zertifikat basierend auf der neuen Zertifikatvorlage anfordern
Neben dem CN (Common Name) sind auch die die X.509 Attribute C (Country) und O (Organisation) wichtig. Diese werden dann vom Webbrowser bei der Validierung des EV Zertifikats verwendet. Ohne diese Werte zeigt der Webbrowser bei der EV-Validierung „Unbekannt“ an.



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