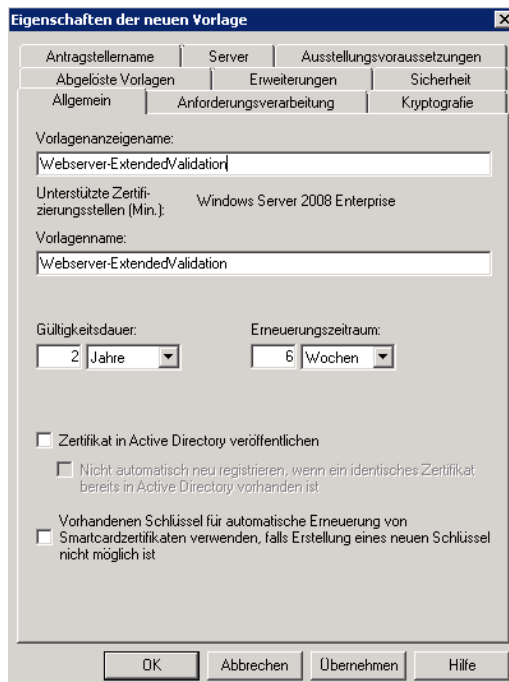


Extended Validation Zertifikate von einer Windows Server 2008 R2 CA ausstellen

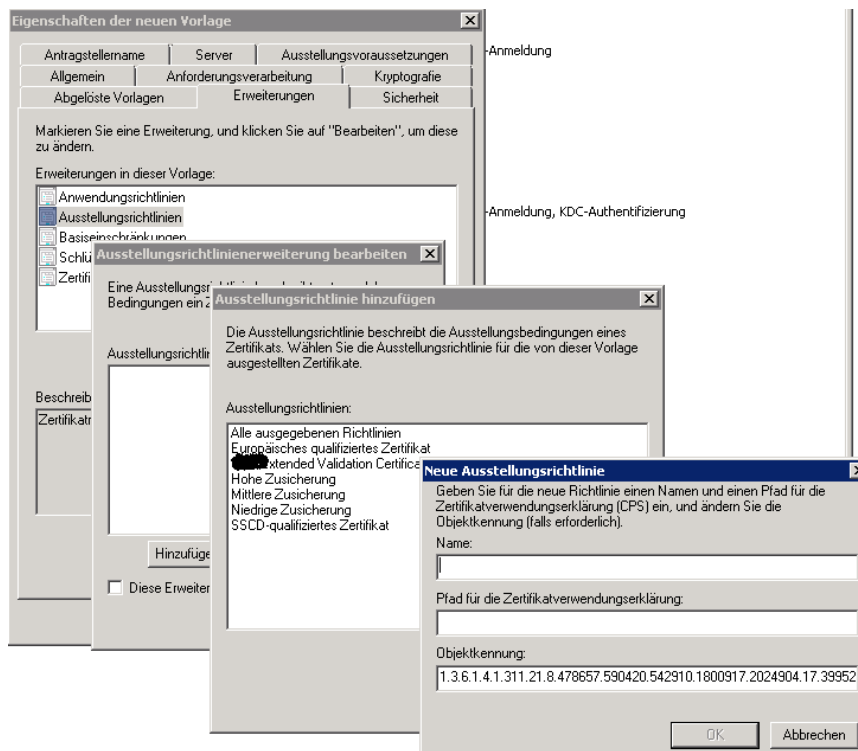
CA Verwaltung starten

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.

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://...ev.pdf

Objektkennung:
1.3.6.1.4.1.311.21.8.478657.590420.542910.1800917.2024904.17.74332

OK Abbrechen

Ausstellungsrichtlinienerweiterung bearbeiten

Eine Ausstellungsrichtlinie beschreibt unter welchen Bedingungen ein Zertifikat ausgestellt werden darf.

Ausstellungsrichtlinien:
Extended Validation Certificate

Hinzufügen... Bearbeiten... Entfernen

Diese Erweiterung als kritisch markieren

OK Abbrechen

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

Eigenschaften von Webserver-EV

Antragstellername Ausstellungsbedingungen

Allgemein Anforderungsverarbeitung Kryptografie

Abgelöste Vorlagen Erweiterungen Sicherheit Server

Gruppen- oder Benutzernamen:

- Authentifizierte Benutzer
- Administrator (administrator@...)
- Domänen-Admins (...)
- Domänencomputer (...)**
- Organisations-Admins (...)
- Domänen-Benutzer (...)
- Domänencomputer (...)

Hinzufügen... Entfernen

Berechtigungen für "Domänencomputer"

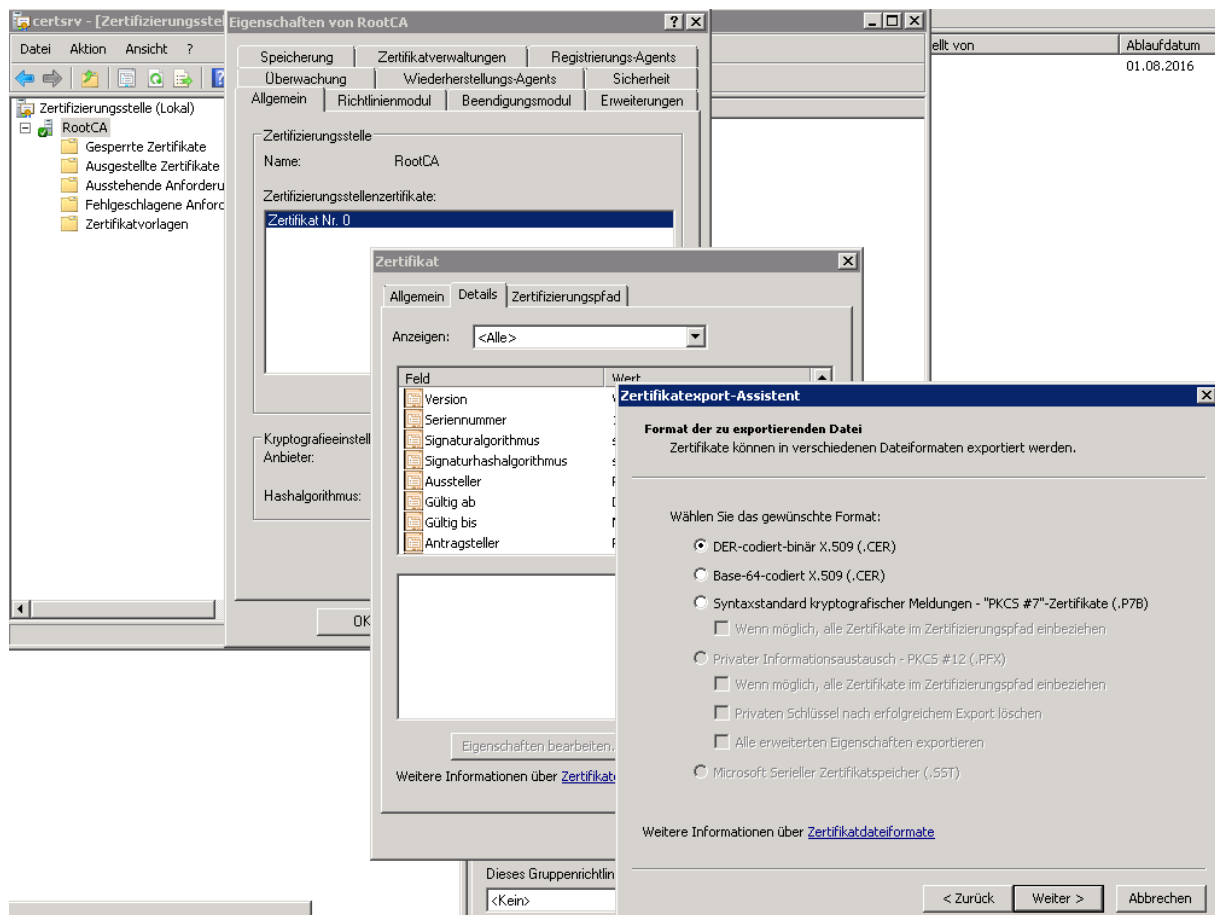
	Zulassen	Verweigern
Vollzugriff	<input type="checkbox"/>	<input type="checkbox"/>
Lesen	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Schreiben	<input type="checkbox"/>	<input type="checkbox"/>
Registrieren	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Automatisch registrieren	<input type="checkbox"/>	<input type="checkbox"/>

Klicken Sie auf "Erweitert", um spezielle Berechtigungen anzuzeigen.

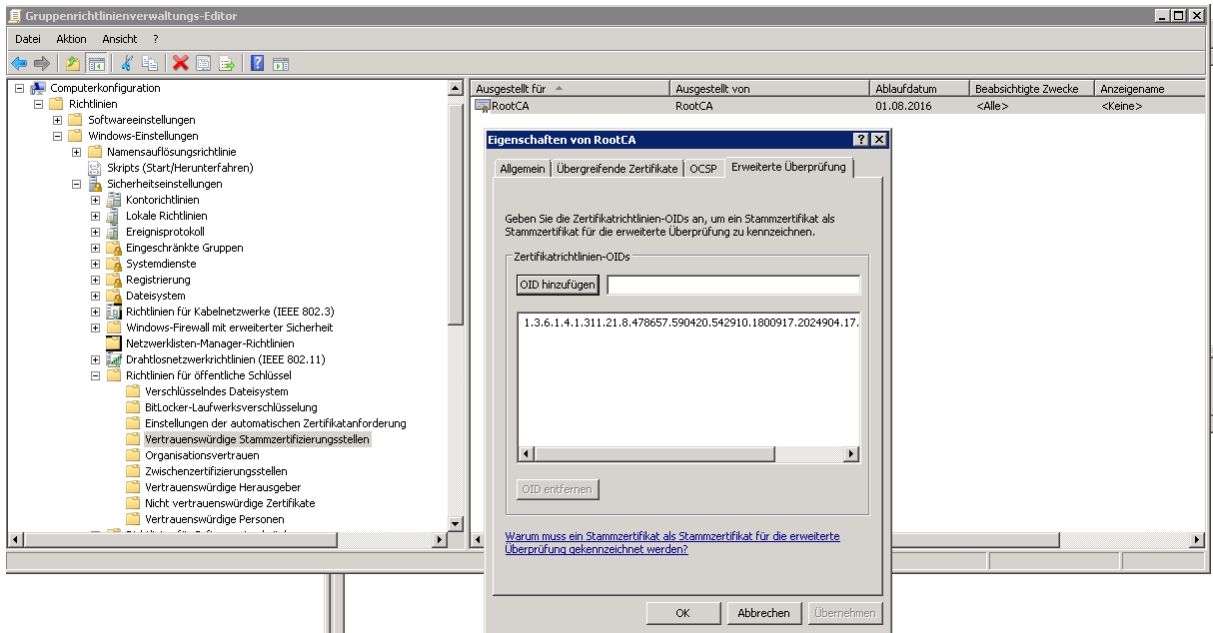
[Weitere Informationen über Zugriffssteuerung und Berechtigungen](#)

OK Abbrechen Übernehmen Hilfe

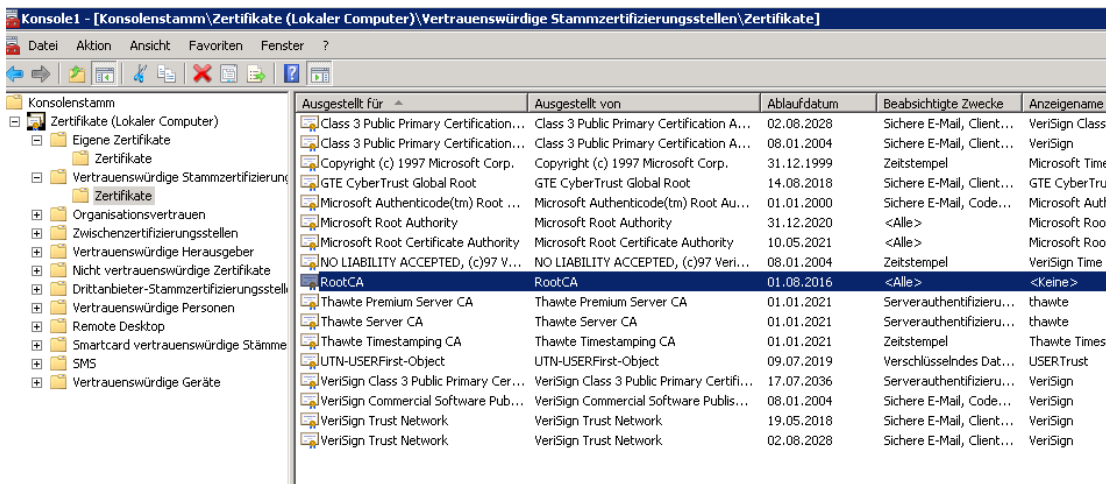
RootCA Zertifikat exportieren, um dieses per GPO neu zu verteilen



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

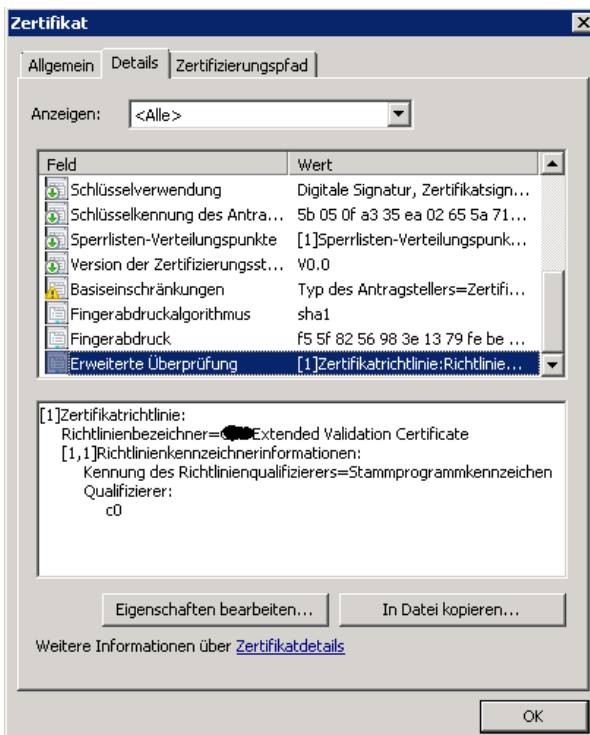


Altes Root CA Zertifikat zum testen entfernen (Zertifikatspeicher Computer)

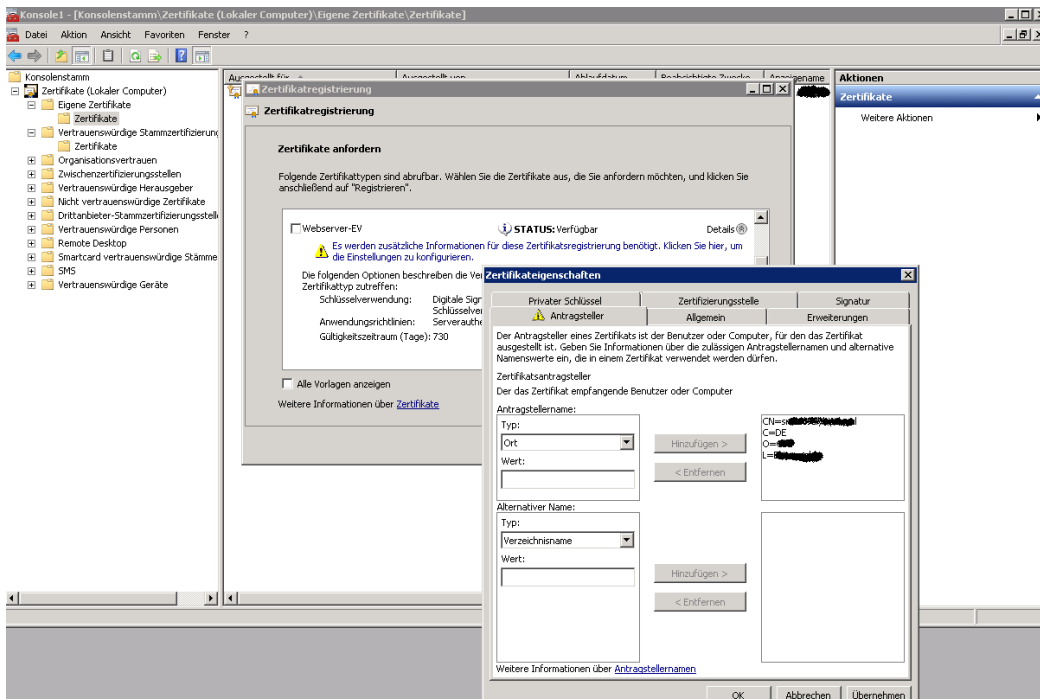


GPUPDATE /FORCE

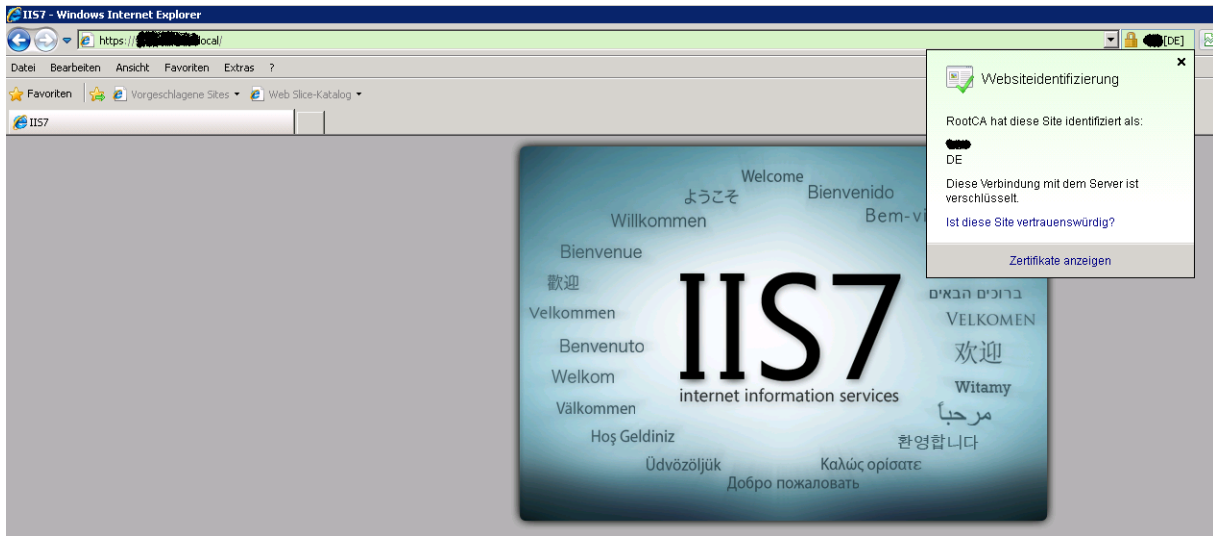
Eigenschaften des „neuen“ Root CA Zertifikats - Erweiterte Ueberpruefung



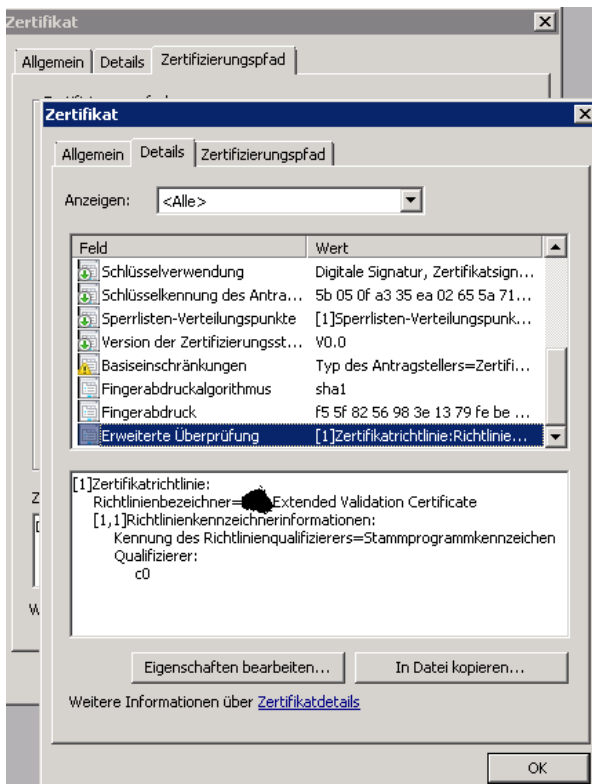
Neues Zertifikat basierend auf der neuen Zertifikatvorlage anfordern
 Neben dem CN (Common Name) sind auch die die X.509 Attribute C (Country) und O (Organisation) wichtig. Diese werden dann vom Webbrowser bei der Validierung des EV Zertifikats verwendet. Ohne diese Werte zeigt der Webbrowser bei der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