

Zertifizierungsstellen mit Microsoft Windows Server 2012R2

Ein PDF von Fabian Niesen, basierend auf einer dreiteiligen Artikelserie zuerst erschienen bei www.fabian-niesen.de

Über den Autor

Fabian Niesen ist seit Jahren beruflich als IT-Consultant unterwegs und arbeitet bei der CONET Solutions GmbH in Hennef. Unter anderem ist er Zertifiziert als MCSA Windows Server 2008 / 2012, MCSA Office 365, MCSE Messaging, MCT und Novell Certified Linux Administrator. Seine Hobby's sind Social Media, Bloggen, Mittelaltermärkte und Historische Lieder.



Sie finden mich bei:

Google+: <https://plus.google.com/+FabianNiesen>

Twitter: http://twitter.com/#!/Fabian_Niesen

LinkedIn: <http://www.linkedin.com/in/fabianniesen/>

Xing: https://www.xing.com/profile/Fabian_Niesen

MS TechNet: <https://social.technet.microsoft.com/profile/fabian%20niesen%20%5Bmct%5D/>

Privater Blog: <https://www.fabian-niesen.de>

Rechtliches / Haftungsausschluss

Dieser Artikel wurden nach bestem Wissen und Gewissen geschrieben und wird ohne Garantie oder Gewährleistung angeboten. Es besteht kein Anspruch auf Support.

Inhaltsverzeichnis

Über den Autor.....	1
Rechtliches / Haftungsausschluss.....	1
Inhaltsverzeichnis	1
Grundlegendes einer Zertifizierungsstellen (CA).....	2
Intern oder Extern? Was sind die Vorteile und was sind die Nachteile?	2
Was ist eine Offline CA?	2
Prüfpunkte für die Gültigkeit von Zertifikaten	3
Welche Arten von Zertifikaten benötigen Sie?.....	3
Welche Menge an Zertifikaten benötigen Sie?	3
Installation einer Offline Root Zertifizierungsstelle unter Windows Server 2012R2.....	3
Die Einrichtung der Offline-CA.....	3
Installation einer unter geordneten Zertifizierungsstelle unter Windows Server 2012R2.....	13
Konfiguration der Wiederherstellbarkeit von Privaten Schlüsseln.....	20
Konfiguration der Zertifikatsvorlagen.....	24
Aktivierung des automatisierten Ausstellen von Zertifikaten (Auto-Enrollment).....	28

Grundlegendes einer Zertifizierungsstellen (CA)

Bevor Sie mal eben schnell eine CA einrichten, sollten Sie vorher über ein paar Dinge nachdenken. Ist eine Interne CA überhaupt das was Sie benötigen? Ergeben sich aus Ihren Sicherheitsanforderungen der Bedarf nach einer Offline Root-CA? Sollen / müssen die Zertifikate im Internet auf Ihre Gültigkeit geprüft werden können? Welche Arten von Zertifikaten benötigen Sie? Welche Menge an Zertifikaten benötigen Sie?

Fangen wir mal an die Fragen zu erörtern.

Intern oder Extern? Was sind die Vorteile und was sind die Nachteile?

Interne CA	Externe CA	Interne Sub-CA einer Externen
Einfach zu erstellen	Zertifikate müssen meistens einzeln Beschafft werden	Wird von wenigen Anbietern angeboten
Es können für alle möglichen Verwendungszwecke Zertifikate erzeugt werden	Die Art der Zertifikate hängt von dem Anbieter ab. Meistens nur SSL, Mail und Softwaresignatur Zertifikate	Es können für alle möglichen Verwendungszwecke Zertifikate erzeugt werden, die die Übergeordnete CA erlaubt.
Kann einfach in ein Active Directory integriert werden	Administration meistens über eine Webseite	Kann einfach in ein Active Directory integriert werden
Zertifikate sind kostenlos	Meistens muss pro Zertifikat bezahlt werden	Zertifikate sind meistens kostenlos, aber hohe Initialkosten
Automatisches erstellen und Verteilen bei Integration in das Active Directory möglich	Manuelle Integration notwendig	Automatisches erstellen und Verteilen bei Integration in das Active Directory möglich
Es können auch Zertifikate für nicht "offizielle" TLDs wie .local oder .intern ausgestellt werden	Nur für Offizielle Domains möglich, die meisten CAs prüfen auch die Inhaberschaft	Es können auch Zertifikate für nicht "offizielle" TLDs wie .local oder .intern ausgestellt werden. Dies kann aber auch durch Vorgaben eingeschränkt sein.
CA muss zu den Vertrauten CAs hinzugefügt werden um Warnung zu verhindern	Wenn der Anbieter in den Listen der Vertrauten CAs der Hersteller enthalten ist, sind keine weiteren Schritte notwendig	Wenn der Anbieter der übergeordneten CA in den Listen der Vertrauten CAs der Hersteller enthalten ist, sind keine weiteren Schritte notwendig

Was ist eine Offline CA?

Bei einer Offline / Stand-Alone Root CA wird zuerst eine Übergeordnete CA erstellt die keine Verbindung zum Netz hat, das bedeutet der Server ist auch kein Domänenmitglied. Typischer weise eine VM die exportiert wird nach den notwendigen Schritten und in einen Tresor gelegt wird. Diese CA hat nur die Aufgabe ein Sub-CA Zertifikat auszustellen und dieses zu gegebener Zeit zu erneuern. Wenn die Sub-CA kompromittiert wird, kann die Übergeordnete CA das Sub-CA Zertifikat widerrufen. Dies ist eigentlich nur notwendig wenn sich andere auf die Zertifikate verlassen können müssen. Dann sollten Sie aber auch noch weiter Schutzmaßnahmen treffen. Für eine rein Intern genutzte CA (z.B. für VPN, oder 802.1x) ist dieser Mehraufwand selten notwendig, aber trotzdem eine Best-Practise Empfehlung.

Prüfpunkte für die Gültigkeit von Zertifikaten

Je nach dem was Sie mit den Zertifikaten vorhaben, verlangen die Dienste dass geprüft werden kann, ob in Zertifikat noch gültig ist. Diese Prüfpunkte werden bei der Erstellung der Zertifikate im Zertifikat hinterlegt. Neben der Möglichkeit diese Listen im Active Directory zu speichern, bietet sich für Systeme die sich nicht innerhalb der eigenen Netzwerkgrenzen befinden ein zusätzlicher Webserver an. Dieser sollte optimaler Weise von überall erreichbar sein. Was genau an Prüfpunkten und Protokollen Sie benötigen, hängt wie so oft von Ihren Anforderungen ab.

Welche Arten von Zertifikaten benötigen Sie?

Wenn Sie noch nicht genau wissen für was Sie alle Zertifikate brauchen, hat eine Interne CA Vorteile. Wichtig ist, diese kann (Ohne Abstriche an der Usability) selten für "externe" Zwecke eingesetzt werden, es sei denn, alle die Zertifikate nutzen fügen Ihre CA zu den Vertrauenswürdigen CAs hinzu. Brauchen Sie hingegen nur ein Zertifikat für Ihre Homepage oder der öffentlichen Adresse Ihres Exchange Servers, so sind Zertifikate von einer Externen CA meistens der beste Weg. Möchten Sie mit S/MIME digital Signierte Mail für alle Ihrer Mitarbeiter zur Kommunikation nach extern umsetzen, dürfte meistens eine Interne Sub-CA einer Externen CA der beste Weg sein.

Welche Menge an Zertifikaten benötigen Sie?

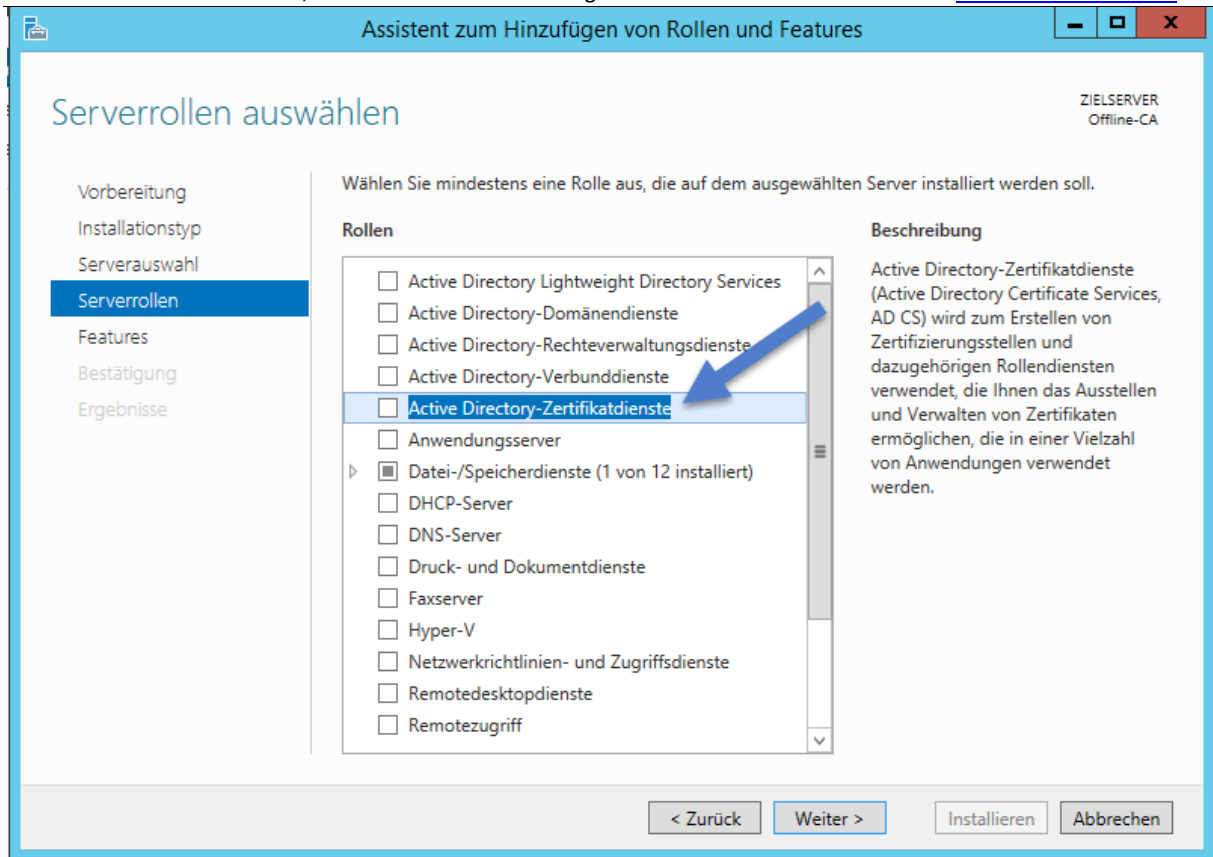
Ab wie vielen Zertifikaten es sich lohnt eine interne CA oder Sub-CA aufzubauen, kann man so nicht sagen. Wenn aber alle 50 Computer ein Zertifikat benötigen, dann sollten Sie definitiv über eine der Internen Lösungen nachdenken.

Installation einer Offline Root Zertifizierungsstelle unter Windows Server 2012R2

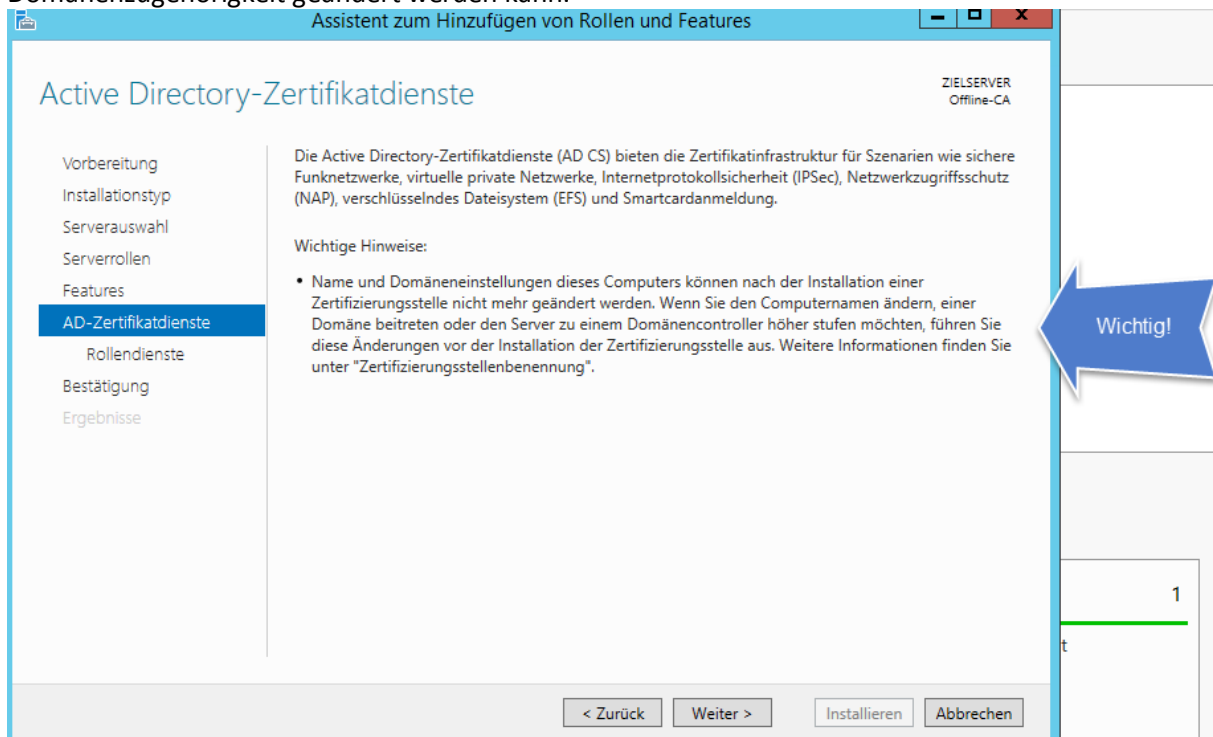
Ich empfehle Ihnen vorher den Artikel "Grundlegendes einer Zertifizierungsstellen (CA)" zu lesen. In diesem Artikel beschreibe ich Ihnen wie Sie eine interne Zertifizierungsstelle unter Windows Server 2012R2 einrichten. Wie in dem Artikel über die Grundlagen von Zertifizierungsstellen beschrieben, richte auch ich zuerst eine Offline Root-CA ein. Dafür wird eine Virtuelle Windows Server 2012R2 Maschine benötigt. Diese sollte unter keinen Umständen Mitglied der Domäne sein.

Die Einrichtung der Offline-CA

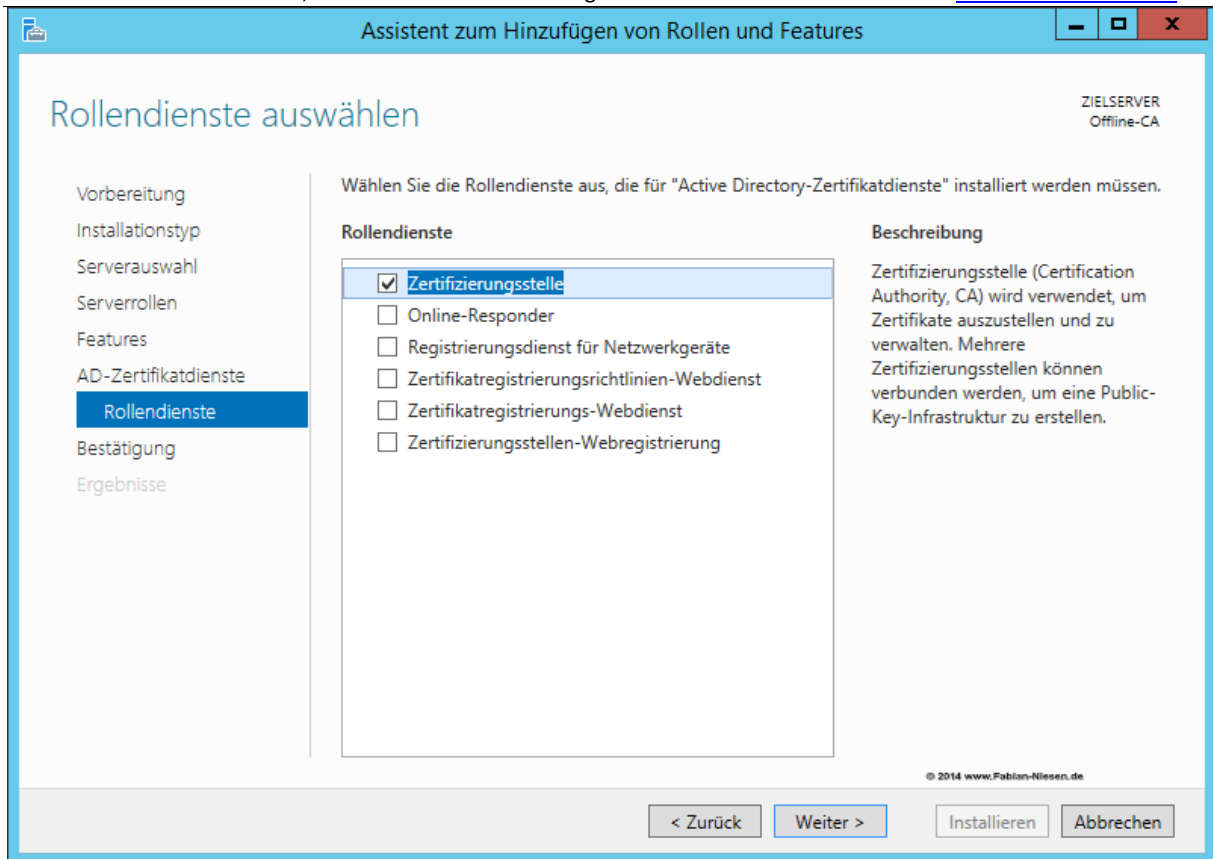
Es schadet nichts die VM auf einen Aktuellen Updatestand zu bringen. Sobald das geschehen ist, kann die Installation beginnen. Als erstes wird die Rolle "Active Directory-Zertifikatdienste" installiert.



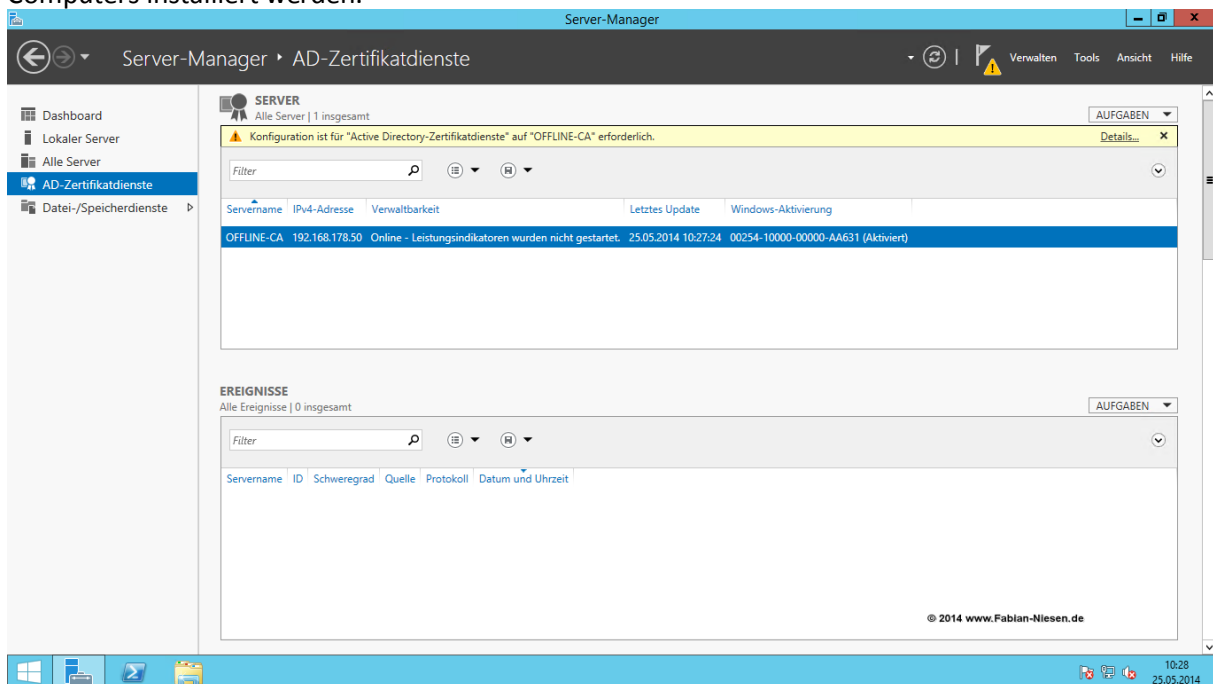
Wichtig ist das nach der Installation der Zertifizierungsstelle weder der Computernamen noch die Domänenzugehörigkeit geändert werden kann.



Die benötigten Rollendienste sind bei der Root-CA lediglich die Rolle "Zertifizierungsstelle"



Nach der Installation der Zertifikatsdienste kann die Zertifizierungsstelle ohne Neustart des Computers installiert werden.



Als Anmeldeinformation für die Rollendienste der Offline CA muss das lokale Administrator Konto verwendet werden. Der zu konfigurierende Rollentyp ist hierbei die Zertifizierungsstelle selber.

The screenshot shows the 'AD CS-Konfiguration' window at the 'Rollendienste' step. The left sidebar lists steps: Anmeldeinformationen, Rollendienste (selected), Installationstyp, ZS-Typ, Privater Schlüssel, Kryptografie, ZS-Name, Gültigkeitsdauer, Zertifikatdatenbank, Bestätigung, Status, and Ergebnisse. The main area is titled 'Wählen Sie die zu konfigurierenden Rollendienste aus.' and contains a list of services with checkboxes: ☒ Zertifizierungsstelle, ☐ Zertifizierungsstellen-Webregistrierung, ☐ Online-Responder, ☐ Registrierungsdienst für Netzwerkgeräte, ☐ Zertifikatregistrierungs-Webdienst, and ☐ Zertifikatregistrierungsrichtlinien-Webdienst. At the bottom, there are buttons for '< Zurück', 'Weiter >', 'Konfigurieren', and 'Abbrechen'. The top right corner indicates 'ZIELSERVER Offline-CA'.

Da wir gewollter Weise über keine Active Directory Mitgliedschaft verfügen, bleibt nur eine "Eigenständige Zertifizierungsstelle" übrig. Eine "Unternehmenszertifizierungsstelle" wird später als die untergeordnete Zertifizierungsstelle erstellt.

The screenshot shows the 'AD CS-Konfiguration' window at the 'Setuptyp' step. The left sidebar lists steps: Anmeldeinformationen, Rollendienste, Installationstyp (selected), ZS-Typ, Privater Schlüssel, Kryptografie, ZS-Name, Gültigkeitsdauer, Zertifikatdatenbank, Bestätigung, Status, and Ergebnisse. The main area is titled 'Geben Sie den Installationstyp der Zertifizierungsstelle an.' and contains two options: ☐ Unternehmenszertifizierungsstelle (with a description about AD DS) and ☒ Eigenständige Zertifizierungsstelle (with a description about offline operation). At the bottom, there are buttons for '< Zurück', 'Weiter >', 'Konfigurieren', and 'Abbrechen'. The top right corner indicates 'ZIELSERVER Offline-CA'.

Die Offline-CA wird als "Stammzertifizierungsstelle" eingerichtet. Für den privaten Schlüssel sollte ein neuer erstellt werden, und nicht ein vorhandener verwendet werden.

Die Schlüssellänge sollte möglichst hoch sein. Als Standard wird 2048 Bit vorgegeben, aber es kann auch 4096 Bit ausgewählt werden. Da der Hashalgorithmus "SHA1" nicht mehr als sicher gilt, verwende ich in meiner Umgebung "SHA512" aus der Algorithmus Familie "SHA2". Auch der MD5 Algorithmus der vielen aus der Linux Welt für Prüfsummen bekannt ist, ist nicht mehr sicher. Mehr dazu im [Golem Artikel "Hash-Verfahren"](#).

AD CS-Konfiguration

ZIELSERVER
Offline-CA

Kryptografie für Zertifizierungsstelle

Anmeldeinformationen
Rollendienste
Installationstyp
ZS-Typ
Privater Schlüssel
Kryptografie
ZS-Name
Gültigkeitsdauer
Zertifikatdatenbank
Bestätigung
Status
Ergebnisse

Geben Sie die Kryptografieoptionen an.

Kryptografieanbieter auswählen: RSA#Microsoft Software Key Storage Provider Schlüssellänge: 4096

Wählen Sie den Hashalgorithmus aus, mit dem Zertifikate dieser Zertifizierungsstelle signiert werden sollen:

- SHA256
- SHA384
- SHA512**
- SHA1

☐ Administratorinteraktion bei jedem Zertifizierungsstellenzugriff auf den privaten Schlüssel zulassen

[Weitere Informationen zur Kryptografie](#)

© 2014 www.Fabian-Niesen.de

< Zurück Weiter > Konfigurieren Abbrechen

Als nächstes sollte für die Offline CA ein vernünftiger Name gefunden werden, diesen sehen hinterher alle Clients in ihrem Zertifikatsspeicher. Sinnvoll wäre hier zum Beispiel "Unternehmensname Root-CA" oder vergleichbares.

Bei der Gültigkeitsdauer ist zu beachten, spätestens nach diesem Zeitraum benötigen sie die Offline-CA zu erneuern der Zertifizierungsstelle. Wichtig ist auch, je länger der Zeitraum, desto grösser ist die Gefahr wenn die Sub-CA kompromittiert wird und die Anwendung das Zertifikat nicht auf Gültigkeit überprüft. Hier sollten Sie genau überlegen wie das Risiko ist, und was Sie mit Ihrer CA vorhaben. Bei mir zuhause, kann ich bei den 5 Jahren die Standard sind bleiben.

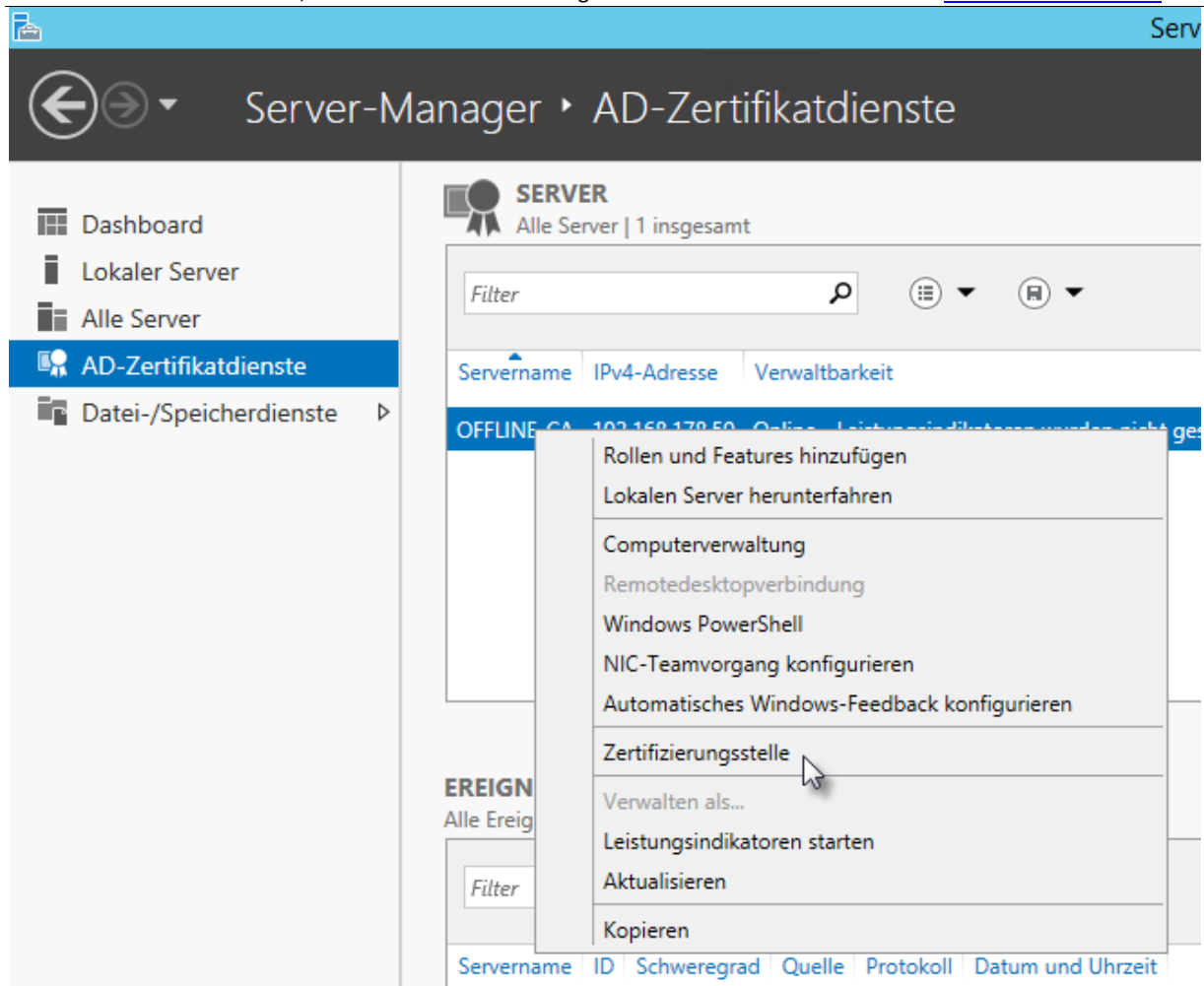
Die Datenbankorte können ohne Probleme an dem vorgeschlagenen Ort belassen werden. Zum Schluss kann alles nochmal geprüft werden, bevor die Zertifizierungsstelle eingerichtet wird. Prüfen Sie es sorgfältig, danach gibt es keinen Weg zurück, außer von vorne anzufangen.

The screenshot shows the 'AD CS-Konfiguration' console window. The title bar includes the text 'AD CS-Konfiguration' and standard window controls. The main area is titled 'Bestätigung' (Confirmation). On the left, a navigation pane lists steps: 'Anmeldeinformationen', 'Rollendienste', 'Installationstyp', 'ZS-Typ', 'Privater Schlüssel', 'Kryptografie', 'ZS-Name', 'Gültigkeitsdauer', 'Zertifikatdatenbank', 'Bestätigung' (highlighted), 'Status', and 'Ergebnisse'. The main content area contains the text: 'Klicken Sie zum Konfigurieren der folgenden Rollen, Rollendienste oder Features auf "Konfigurieren".' Below this is a section titled 'Active Directory-Zertifikatdienste'. Under 'Zertifizierungsstelle', the following configuration details are listed: 'ZS-Typ: Eigenständige Stammzertifizierungsstelle', 'Kryptografieanbieter: RSA#Microsoft Software Key Storage Provider', 'Hashalgorithmus: SHA512', 'Schlüssellänge: 4096', 'Administratorinteraktion zulassen: Deaktiviert', 'Gültigkeitsdauer des Zertifikats: 25.05.2019 10:30:00', 'Distinguished Name: CN=Root CA Fabian-Niesen.de', 'Ort der Zertifikatdatenbank: C:\Windows\system32\CertLog', and 'Ort des Zertifikatdatenbankprotokolls: C:\Windows\system32\CertLog'. At the bottom right, there is a copyright notice '© 2014 www.Fabian-Niesen.de'. The bottom of the window features four buttons: '< Zurück', 'Weiter >', 'Konfigurieren', and 'Abbrechen'.

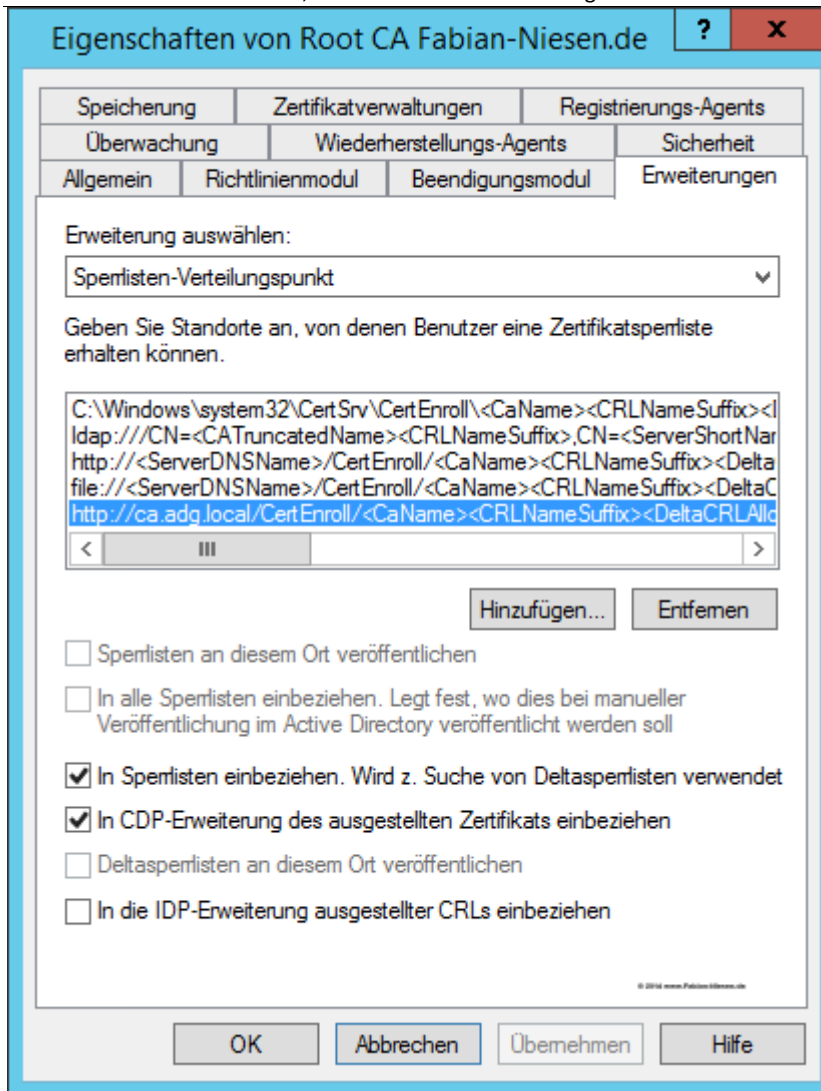
Nach einem kurzen Moment ist die Zertifizierungsstelle eingerichtet.

The screenshot shows the 'AD CS-Konfiguration' console window at the 'Ergebnisse' (Results) step. The title bar is the same. The navigation pane on the left now has 'Ergebnisse' highlighted. The main content area displays the text: 'Die folgenden Rollen, Rollendienste oder Features wurden konfiguriert:'. Below this is the 'Active Directory-Zertifikatdienste' section. Under 'Zertifizierungsstelle', there is a green checkmark icon followed by the text 'Erfolgreiche Konfiguration'. Below this, a link reads 'Weitere Informationen zur Konfiguration der Zertifizierungsstelle'. The copyright notice '© 2014 www.Fabian-Niesen.de' is still present. The bottom buttons are now '< Zurück', 'Weiter >', 'Schließen', and 'Abbrechen'.

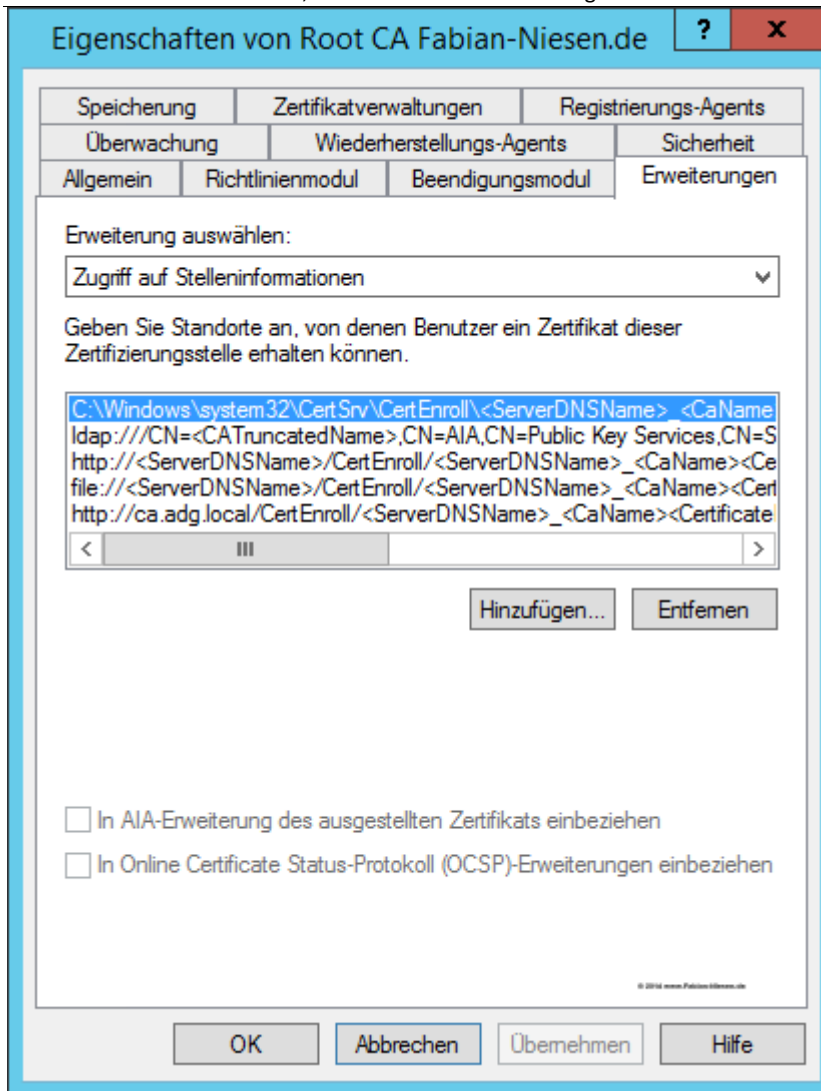
Nach der Einrichtung der CA müssen noch ein paar Einstellungen in der Zertifizierungsstelle vorgenommen werden. Dazu starten Sie die "Zertifizierungsstelle"-Konsole aus dem Server-Manager.



In den Eigenschaften der Root-CA sollten jetzt die "Certificate Revocation Lists (CRL)" bzw. im Deutschen die "Zertifikatssperrlisten" und die "Authority Information Access (AIA)" bzw. im Deutschen der "Zugriff auf Stelleninformationen" (Ich lasse die Übersetzung mal unkommentiert) gepflegt werden. Hier sollten Sie gut überlegen in welche Sperrlisten eingetragen werden, so mal ja der Server der Offline CA Offline sein wird. Sinnvoll ist es für die Root-CA dieselben Veröffentlichungspunkte zu Nutzen wie für die Untergeordnete CA. Dafür sollte man sich jetzt schon für einen Computernamen / DNS-Namen für die Sub-CA entscheiden. In kleinen Umgebungen wäre es möglich die Untergeordnete CA auf einen Domänen Controller zu installieren. Dieser würde aber bis zu einer Migration der CA auf seinem Betriebssystem Stand verbleiben und könnte auch nicht heruntergestuft werden. Dies könnte in Zukunft dazu führen das der Domänen Funktion Ebene nicht weiter angehoben werden kann. Ich werde in meiner Umgebung den DNS-Alias "CA" für die untergeordnete Zertifizierungsstelle verwenden, und trage ihn auch direkt in den DNS ein. Entsprechend trage ich als Veröffentlichungspunkt "<http://ca.adg.local/CertEnroll/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crt>" und Aktiviere für den hinzugefügten Punkt die Checkboxes "in Sperrlisten einbeziehen. Wird z. Suche von Deltasperrlisten verwendet" und "In CDP-Erweiterung des ausgestellten Zertifikats einbeziehen".

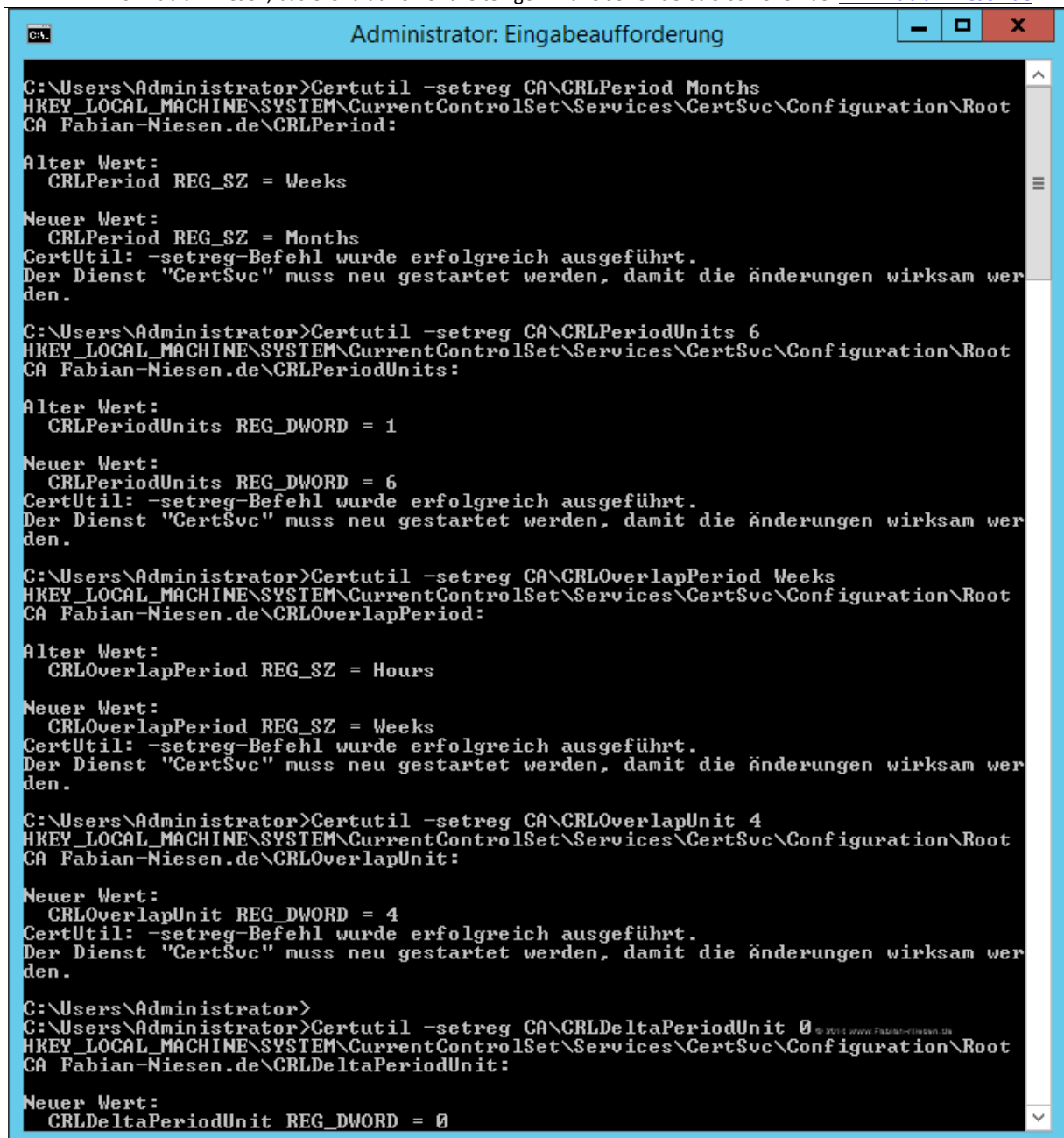


Für den "Zugriff auf Stelleninformationen" trage ich entsprechend "<http://ca.adg.local/certEnroll/<ServerDNSName> <CaName><CertificateName>.crl>" und aktiviere die Option "In AIA-Erweiterung des ausgestellten Zertifikats einbeziehen".



Damit die Offline-CA nicht jede Woche zur Erzeugung einer neuen Sperrliste gestartet werden muss, müssen die folgenden Befehle in eine Eingabeaufforderung die im Administrativen Modus gestartet wurde:

```
Certutil -setreg CA\CRLPeriod Months
Certutil -setreg CA\CRLPeriodUnits 6
Certutil -setreg CA\CRLOverlapPeriod Weeks
Certutil -setreg CA\CRLOverlapUnit 4
Certutil -setreg CA\CRLDeltaPeriodUnit 0
```



```
C:\Users\Administrator>Certutil -setreg CA\CRLPeriod Months
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\Root
CA Fabian-Niesen.de\CRLPeriod:

Alter Wert:
    CRLPeriod REG_SZ = Weeks

Neuer Wert:
    CRLPeriod REG_SZ = Months
CertUtil: -setreg-Befehl wurde erfolgreich ausgeführt.
Der Dienst "CertSvc" muss neu gestartet werden, damit die Änderungen wirksam wer-
den.

C:\Users\Administrator>Certutil -setreg CA\CRLPeriodUnits 6
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\Root
CA Fabian-Niesen.de\CRLPeriodUnits:

Alter Wert:
    CRLPeriodUnits REG_DWORD = 1

Neuer Wert:
    CRLPeriodUnits REG_DWORD = 6
CertUtil: -setreg-Befehl wurde erfolgreich ausgeführt.
Der Dienst "CertSvc" muss neu gestartet werden, damit die Änderungen wirksam wer-
den.

C:\Users\Administrator>Certutil -setreg CA\CRLOverlapPeriod Weeks
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\Root
CA Fabian-Niesen.de\CRLOverlapPeriod:

Alter Wert:
    CRLOverlapPeriod REG_SZ = Hours

Neuer Wert:
    CRLOverlapPeriod REG_SZ = Weeks
CertUtil: -setreg-Befehl wurde erfolgreich ausgeführt.
Der Dienst "CertSvc" muss neu gestartet werden, damit die Änderungen wirksam wer-
den.

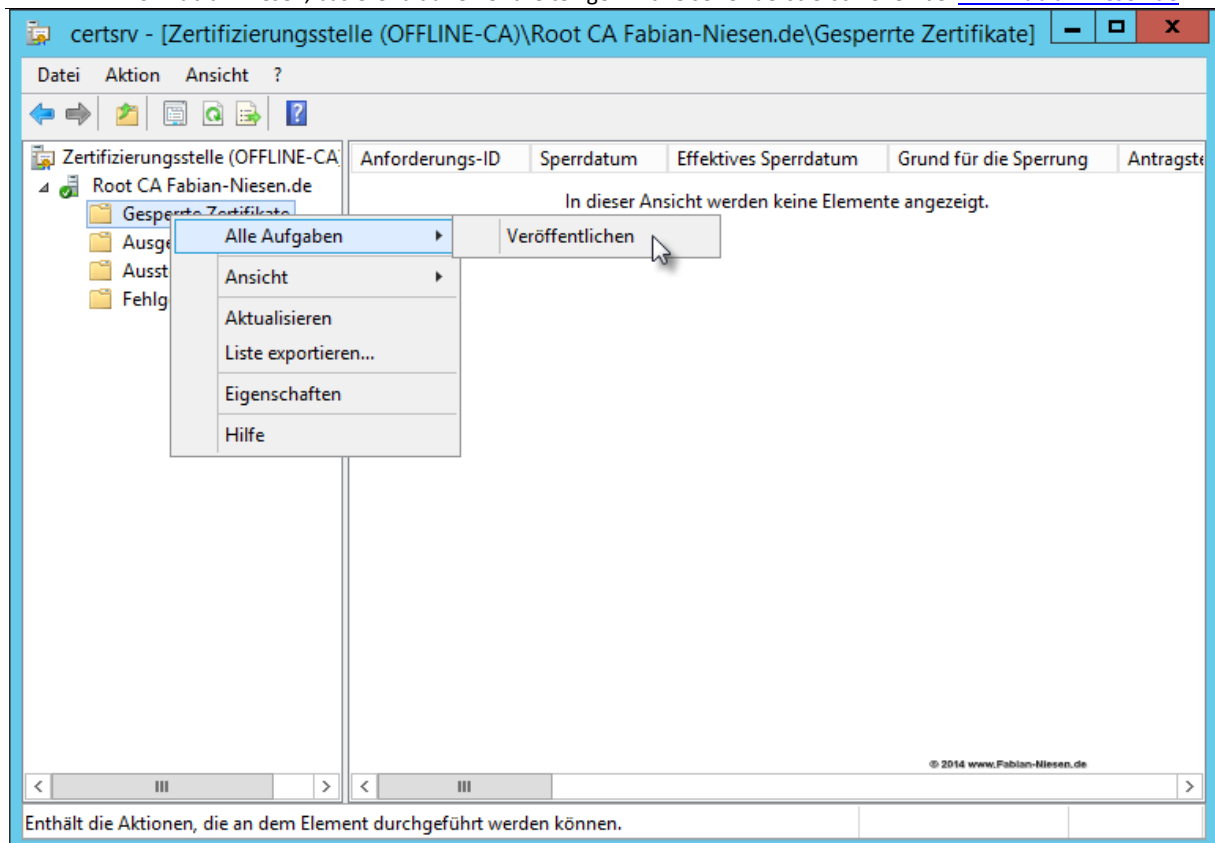
C:\Users\Administrator>Certutil -setreg CA\CRLOverlapUnit 4
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\Root
CA Fabian-Niesen.de\CRLOverlapUnit:

Neuer Wert:
    CRLOverlapUnit REG_DWORD = 4
CertUtil: -setreg-Befehl wurde erfolgreich ausgeführt.
Der Dienst "CertSvc" muss neu gestartet werden, damit die Änderungen wirksam wer-
den.

C:\Users\Administrator>
C:\Users\Administrator>Certutil -setreg CA\CRLDeltaPeriodUnit 0
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\Root
CA Fabian-Niesen.de\CRLDeltaPeriodUnit:

Neuer Wert:
    CRLDeltaPeriodUnit REG_DWORD = 0
```

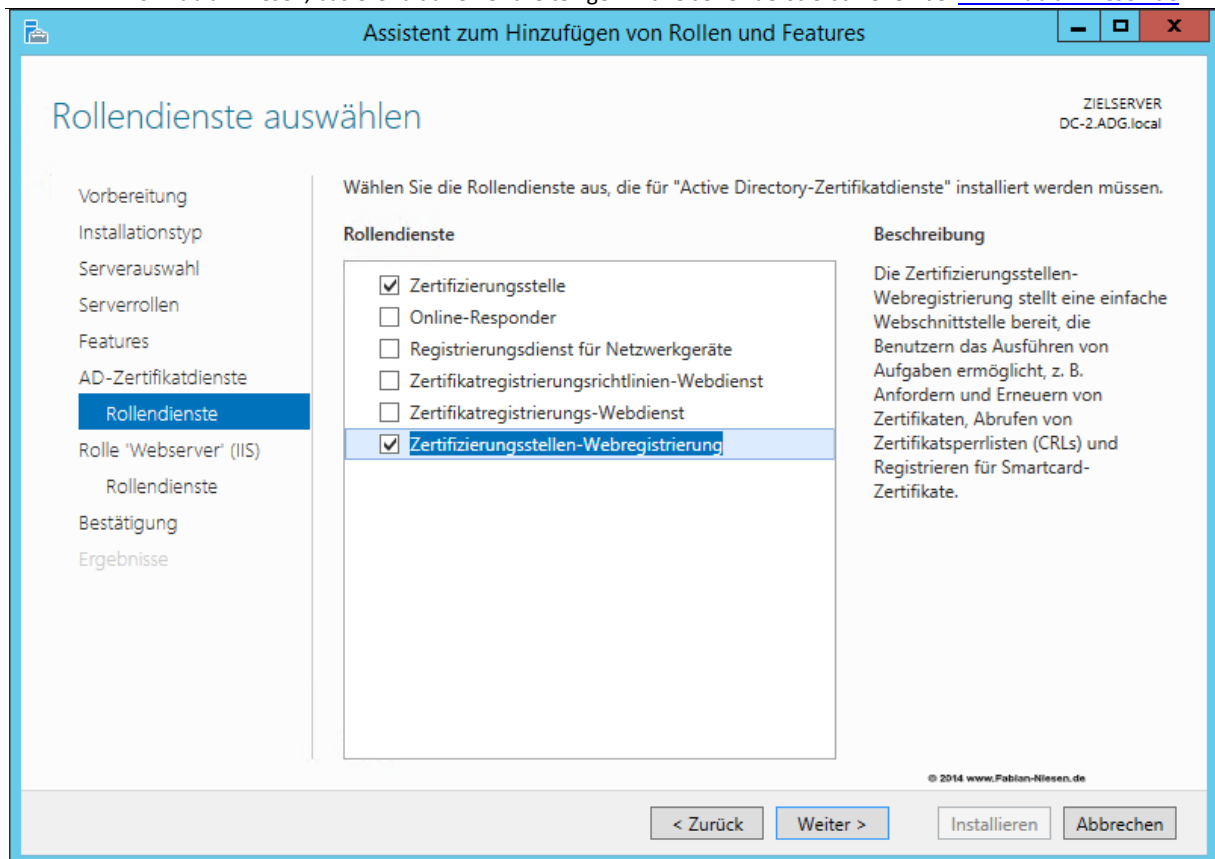
Als nächstes sollte die Liste der Gespeicherten Zertifikate veröffentlicht werden. Tragen Sie sich die Erneuerung der Sperrliste am besten direkt in den Kalender ein. Ohne eine Gültig Sperrliste verweigert die SUB-CA ihren Dienst.



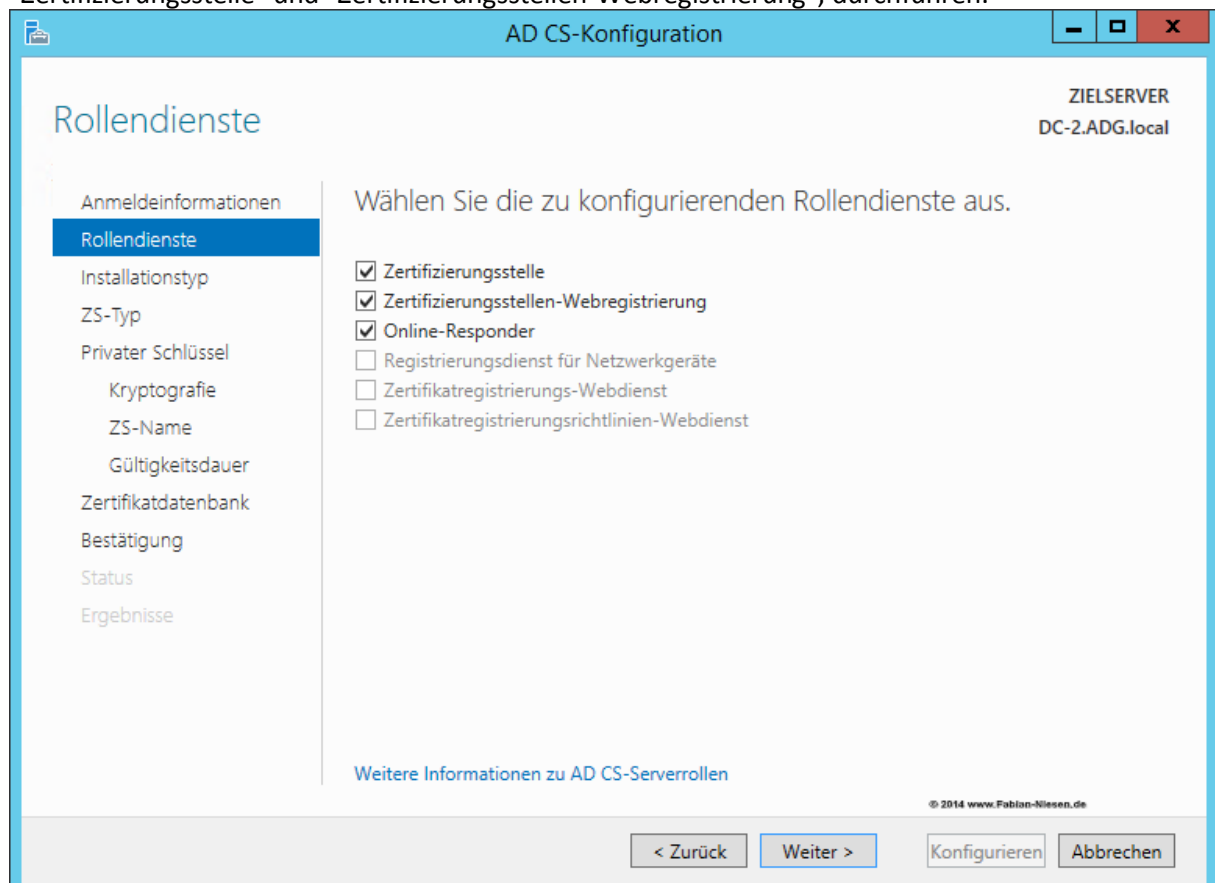
Als nächstes solle der Inhalt des Ordners "C:\Windows\System32\Certsrv\CertEnroll" zusammen mit einem Export des Persönlichen Zertifikates (Ohne privaten Schlüssel) der Root-CA in einen Ordner, zur vereinfachten Einrichtung kann er auch über Netzwerk freigegeben werden.

Installation einer unter geordneten Zertifizierungsstelle unter Windows Server 2012R2

Die Installation der Zertifizierungsstelle ist ähnlich, nur das diesmal auch zusätzlich die Zertifizierungsrolle "Zertifizierungsstellen-Webregistrierung" mit installiert werden muss.



Die bringt auch den Internet Information Server (IIS) mit, leider wird noch der Kompatibilitätsmodus für den IIS 6 benötigt. Nach der Installation der Active Directory Zertifizierungsstelle erfolgt wieder die Konfiguration. Die Konfiguration möchten wir direkt für die beiden Rollendienste, "Zertifizierungsstelle" und "Zertifizierungsstellen-Webregistrierung", durchführen.



Dieses Mal soll allerdings eine "Unternehmenszertifizierungsstelle" eingerichtet werden, um die Integration in das Active Directory zu nutzen.

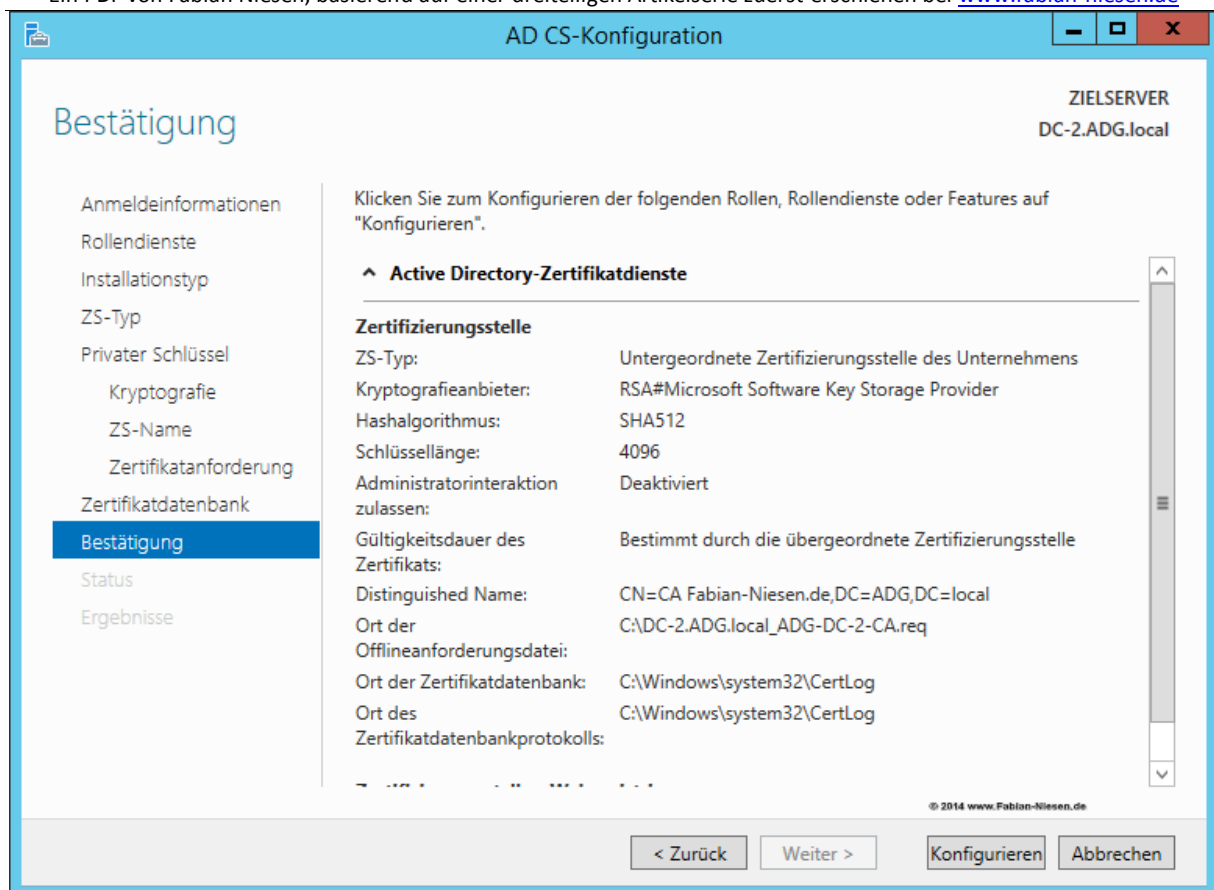
Der Zertifizierungsstellen-Typ ist diese Mal auch ein anderer, es wird eine "Untergeordnete Zertifizierungsstelle" eingerichtet.

Auch hier sollte wieder ein neuer Privater Schlüssel erzeugt werden. Die Kryptografie Einstellungen würde ich genauso wie bei der Übergeordneten CA konfigurieren. Der Name der Zertifizierungsstelle sollte wieder für Ihre Umgebung passend sein.

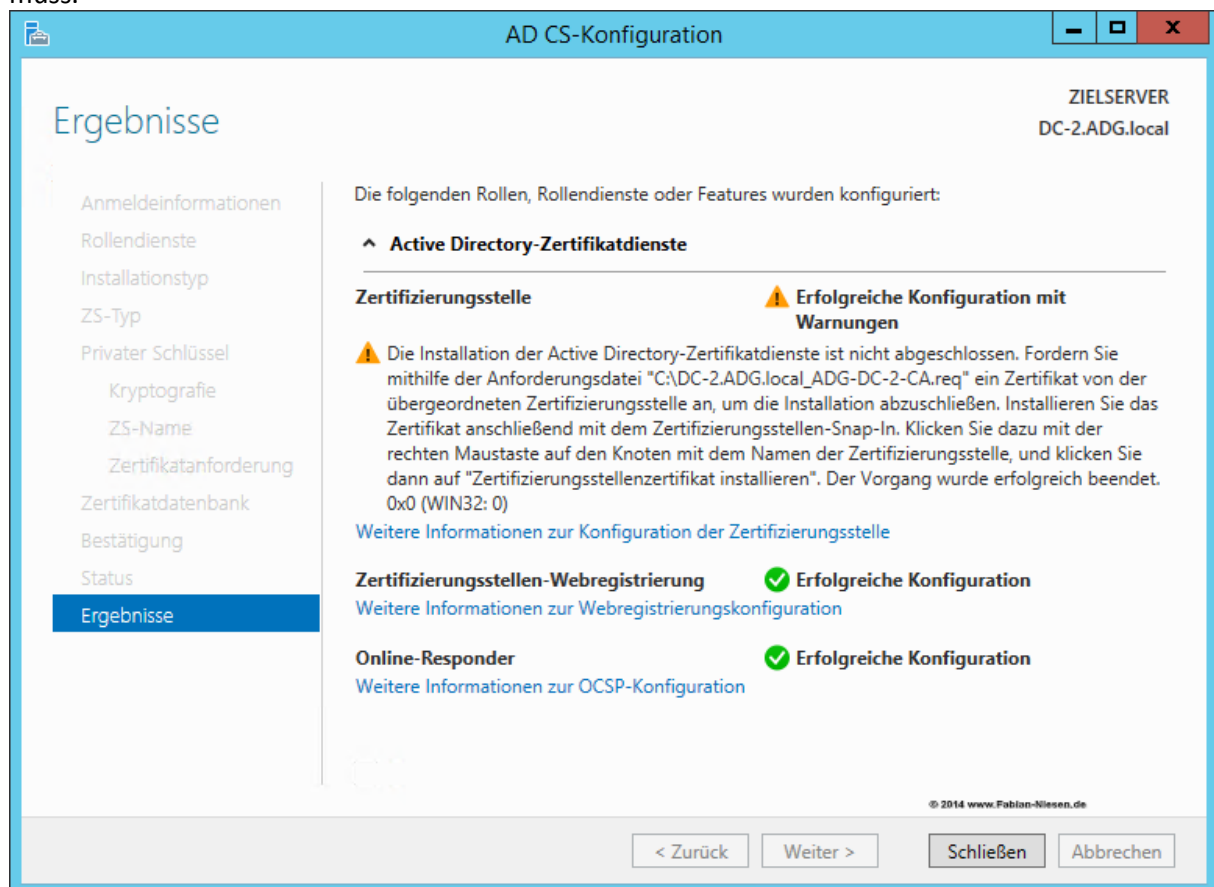
Da die Übergeordnete CA keine automatisierten Schnittstellen hat, exportieren wir den Zertifikatsanforderung für die untergeordnete Zertifizierungsstelle. Diese Anforderung muss anschließend in das Transferverzeichnis, in dem schon die anderen Daten der Übergeordneten CA liegen, kopiert werden.

Die Datenbankeinstellungen übernehme ich auch hier wieder.

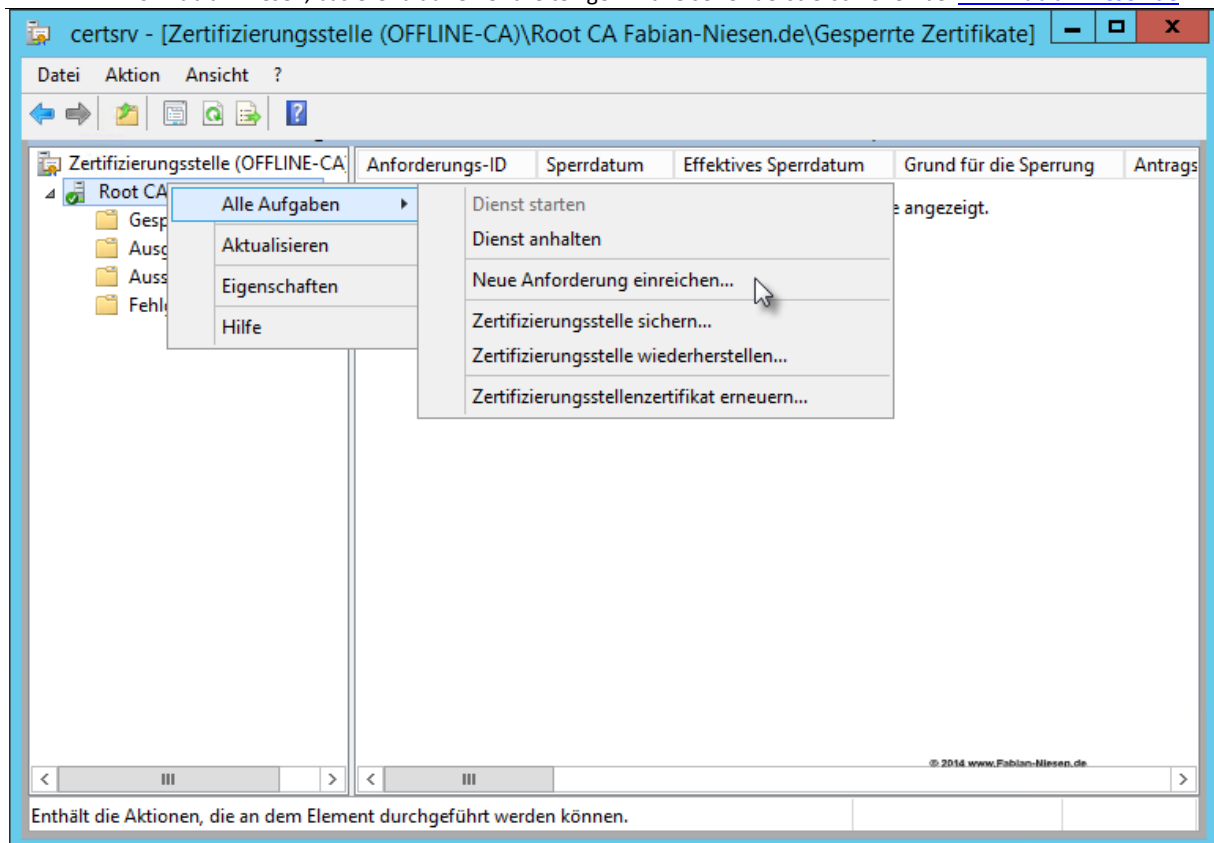
Die Zusammenfassung sollte auch hier geprüft werden, da sich im Nachhinein nichts mehr ändern lässt.



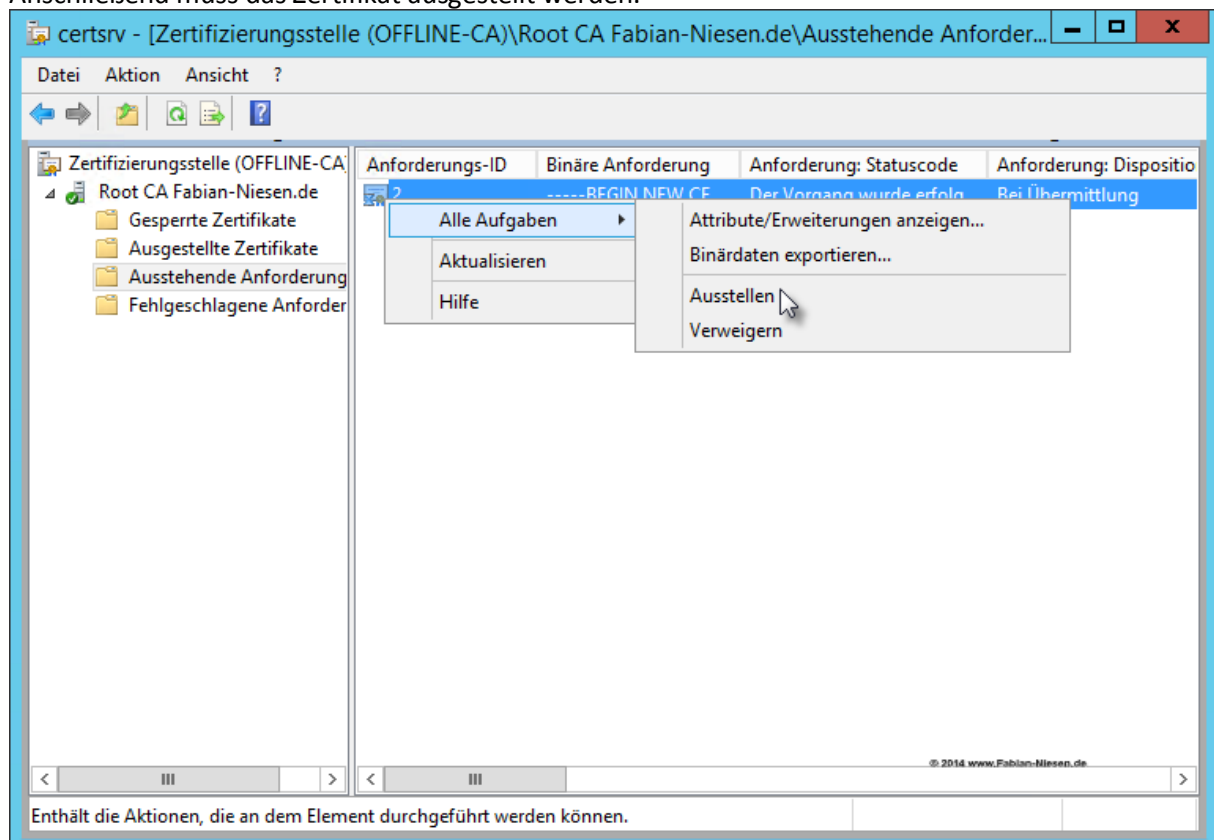
Die Installation erfolgt mit einer Warnung, da das Zertifikat noch von der Root-CA signiert werden muss.



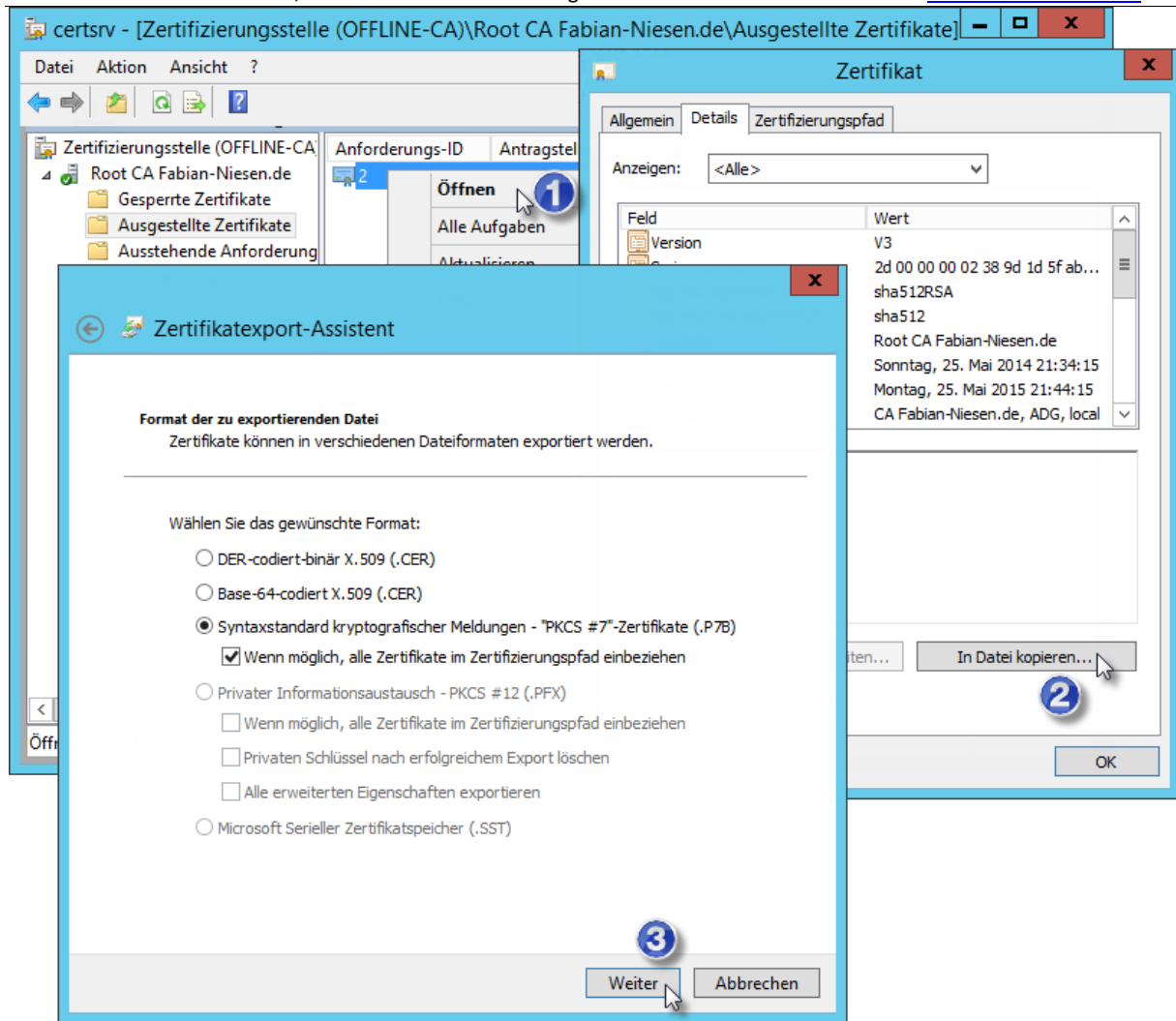
Nun kann in die Offline-Zertifizierungsstelle die Zertifikate Anforderung der Untergeordneten Zertifizierungsstelle importiert werden.



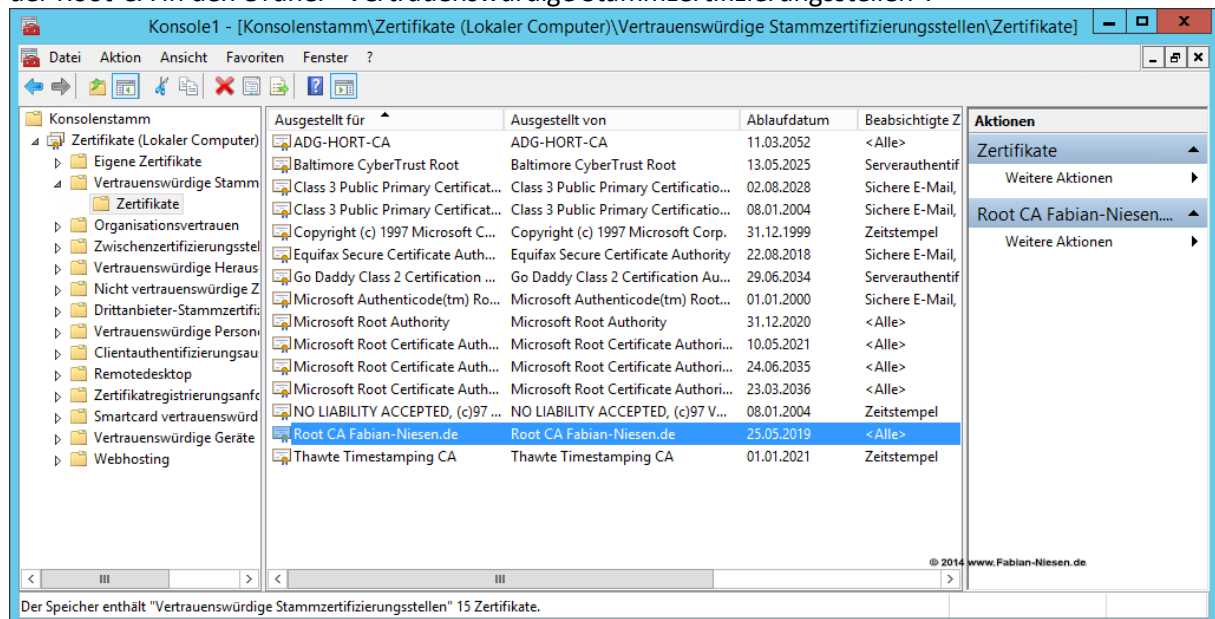
Anschließend muss das Zertifikat ausgestellt werden.



Nun kann unter den Ausgestellten Zertifikaten das neue Zertifikat exportiert werden.

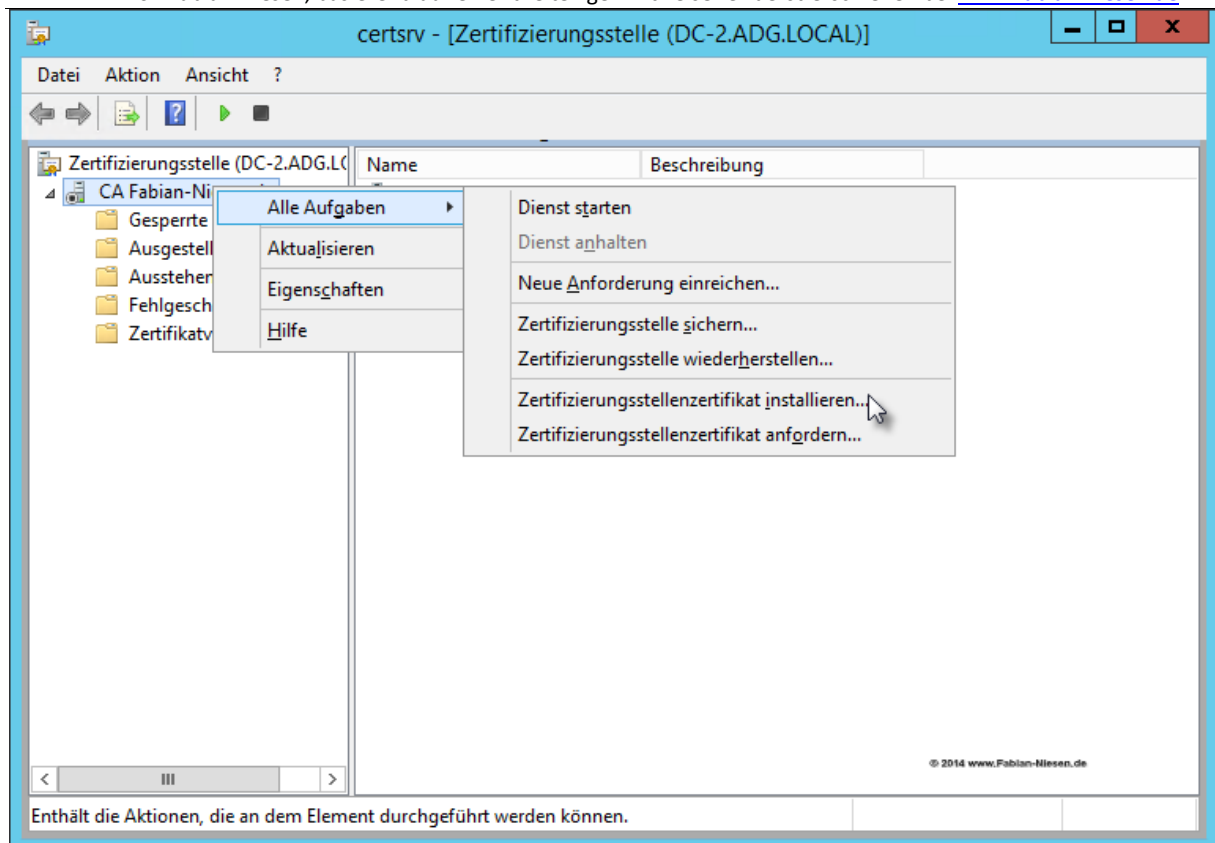


Anschließend wird auf der Untergeordneten Zertifizierungsstelle die MMC geestartet. Fügen Sie dort das Zertifikate Snap-In für das Lokale Computerkonto hinzu. Importieren Sie das Exportierte Zertifikat der Root-CA in den Ordner "Vertrauenswürdige Stammzertifizierungsstellen".



Als nächstes müssen die CRL und CRT Dateien nach "C:\Windows\System32\certsrv\CertEnroll" kopiert werden, damit die Revokation Liste der Root-CA geprüft werden kann.

Anschließend können Sie in der Konsole "Zertifizierungsstelle" das Zertifizierungsstellenzertifikat installiert.



Nach der Installation kann die Zertifizierungsstelle gestartet werden. Nach dem Start kann die Root-CA heruntergefahren werden und exportiert werden. Sinnvoll wären 1-2 Exporte an verschiedenen Stellen, optimaler Weise verschlüsselt.

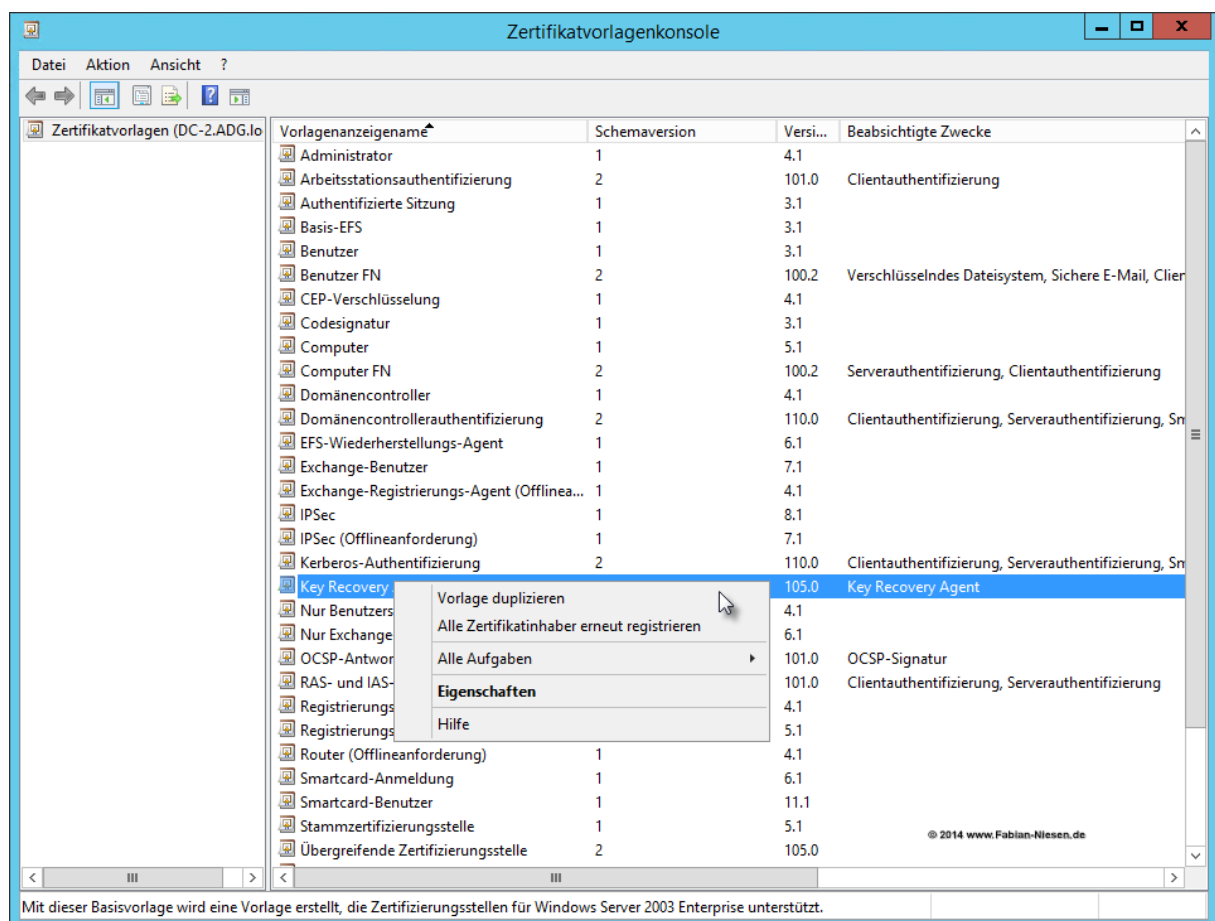
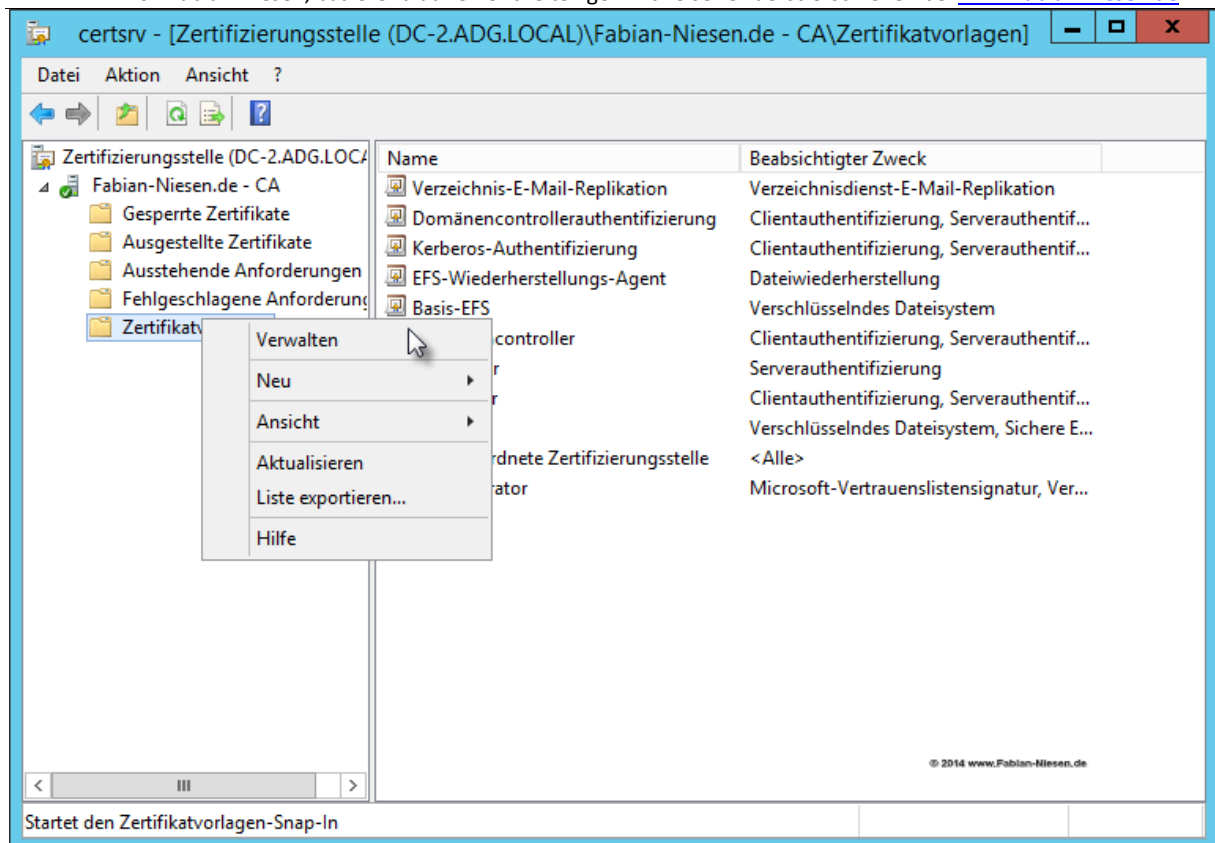
Konfiguration der Wiederherstellbarkeit von Privaten Schlüsseln

Damit auch mal der Private Schlüssel wiederhergestellt werden kann, wenn er mal verloren geht, muss noch etwas Arbeit getan werden.

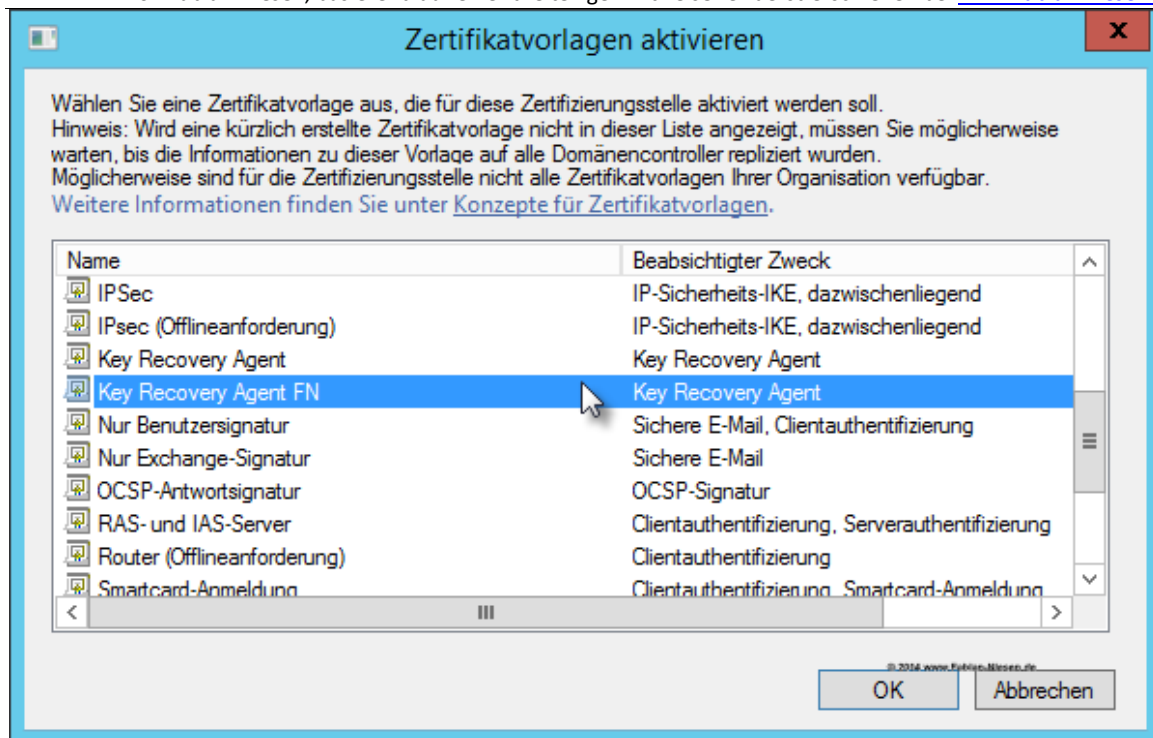
Zuerst muss das "Key Recovery Agent" (KRA) Zertifikat veröffentlicht werden. Dazu Verwalten Sie die Zertifikatsvorlagen und Duplizieren dort die KRA-Vorlage.

Zertifizierungsstellen mit Microsoft Windows Server 2012R2

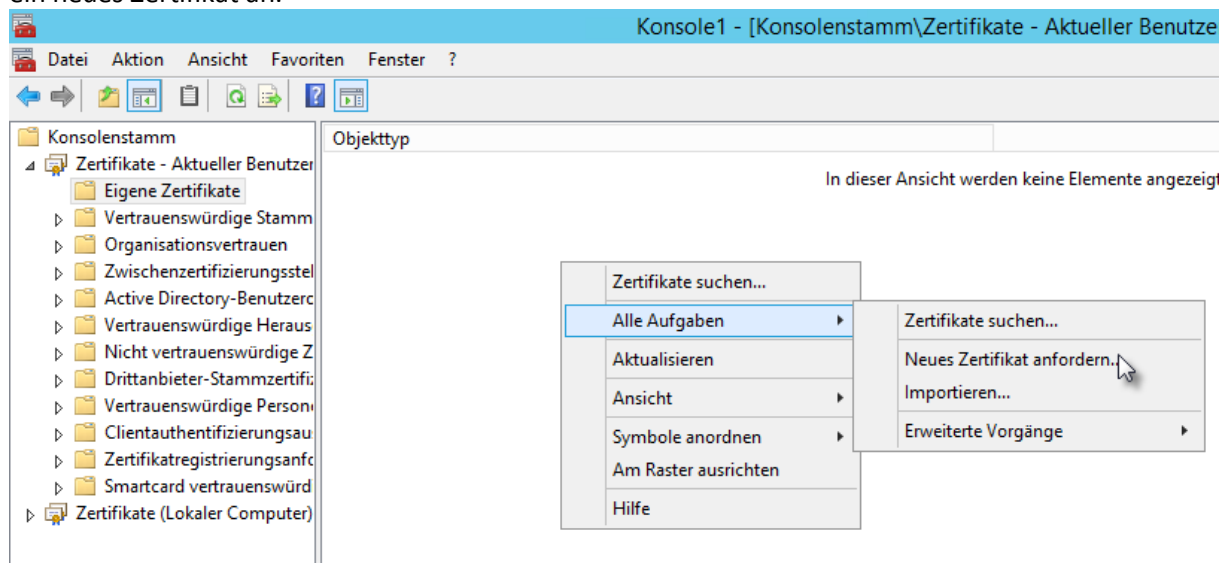
Ein PDF von Fabian Niesen, basierend auf einer dreiteiligen Artikelserie zuerst erschienen bei www.fabian-niesen.de



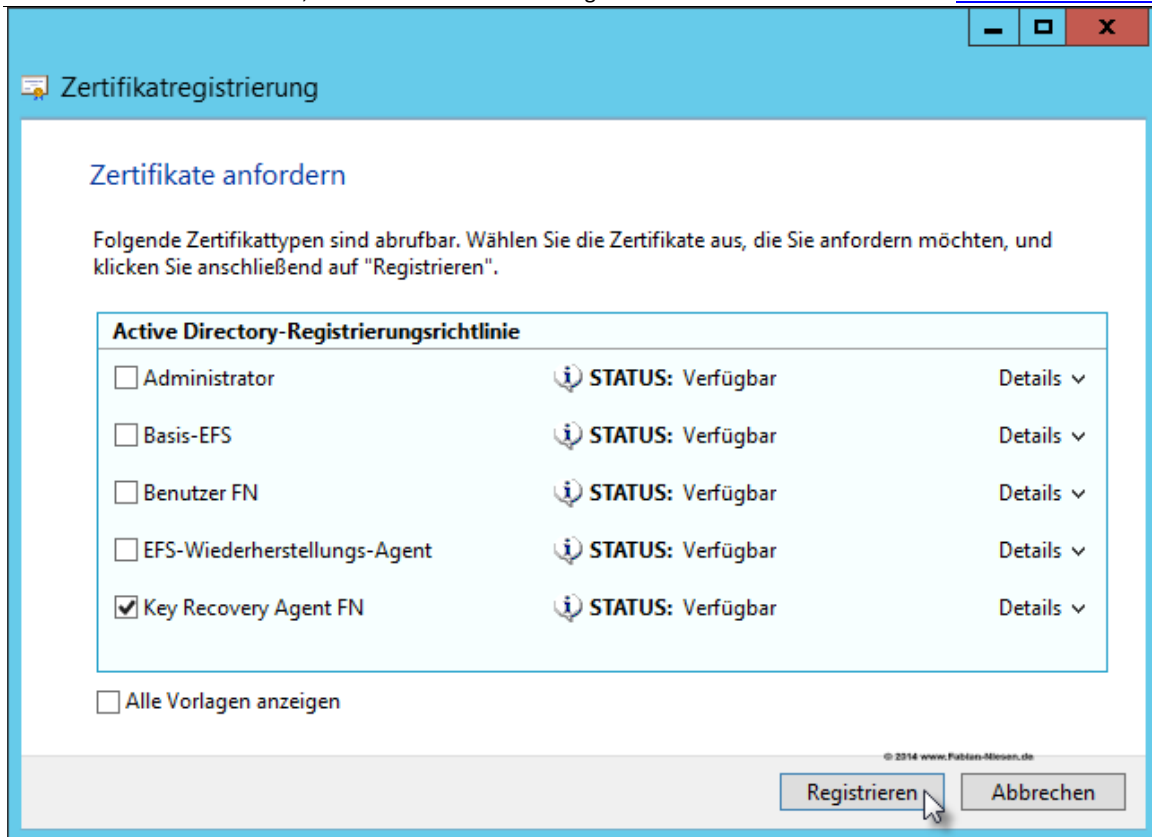
Veröffentlichen Sie nun die angepasste Vorlage.



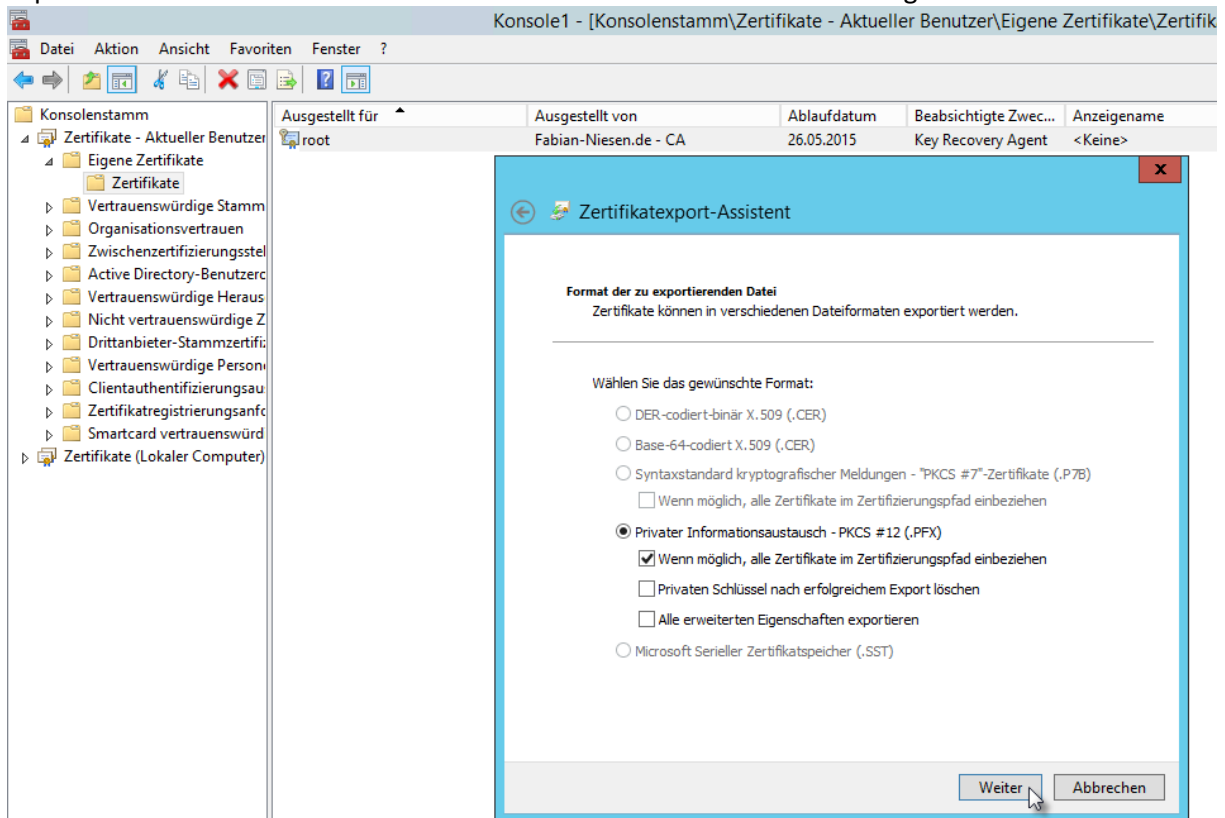
Nun müssen Sie das entsprechende Zertifikat beantragen. Melden Sie sich dazu auf einem Computer mit einem Domänen-Administrator Konto an. Öffnen Sie den lokalen Zertifikatsspeicher, und fordern ein neues Zertifikat an.



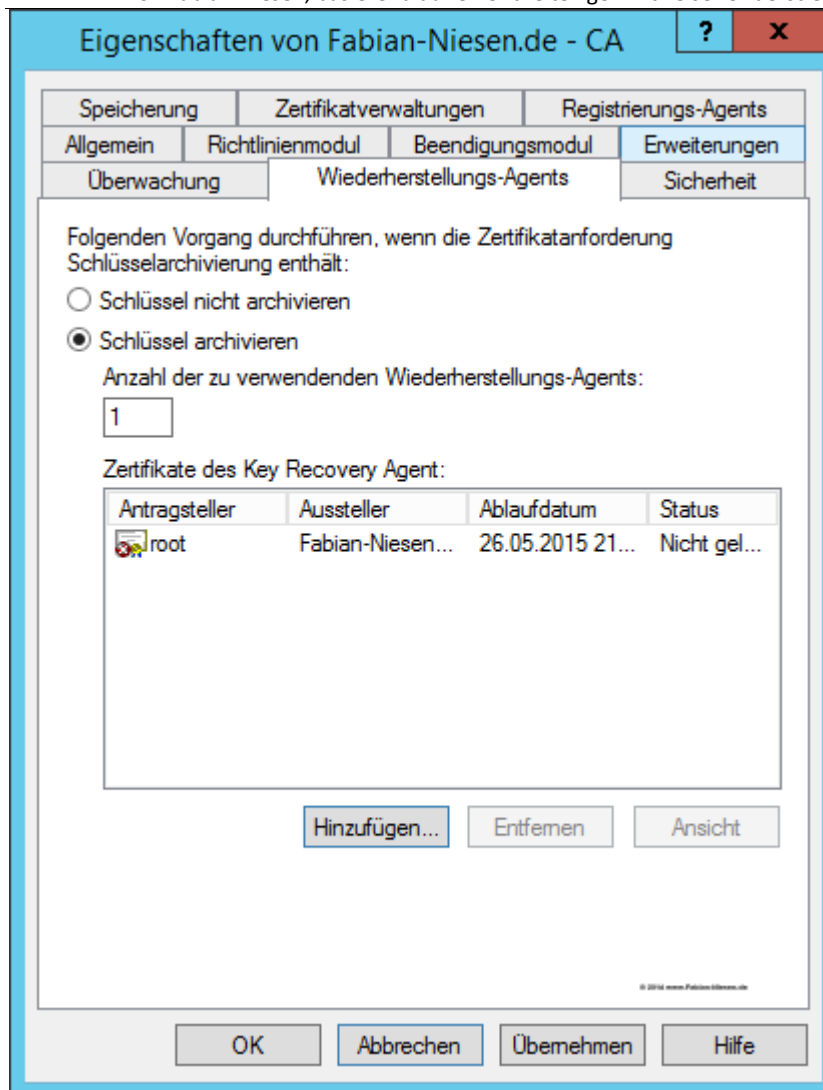
Fordern Sie das "Key Recovery Agent" Zertifikat an.



Exportieren Sie das Zertifikat mit dem Privaten Schlüssel und sichern Sie es gut.



Jetzt muss dieses Zertifikat noch der in der Zertifizierungsstelle entsprechend hinterlegt werden. In den Eigenschaften der Zwischenzertifizierungsstelle muss der Wiederherstellungs-Agent eingetragen werden.



Im Anschluss müssen die Dienste der Zertifizierungsstelle neu gestartet werden.

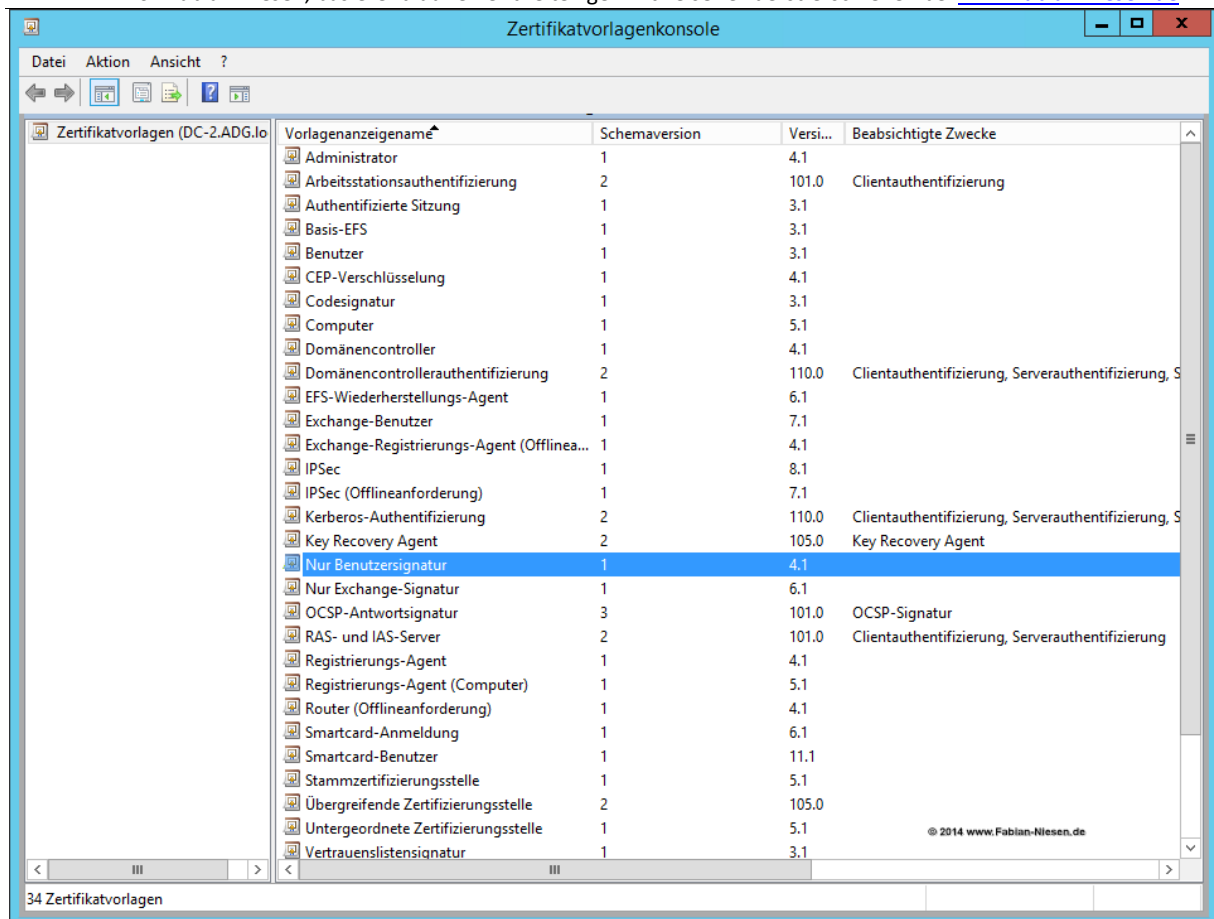
Konfiguration der Zertifikatsvorlagen

Damit die Zertifizierungsstelle auch Ihre Arbeit aufnehmen kann, müssen noch die Vorlagen für die Zertifikate konfiguriert werden die im Unternehmen genutzt werden sollen.

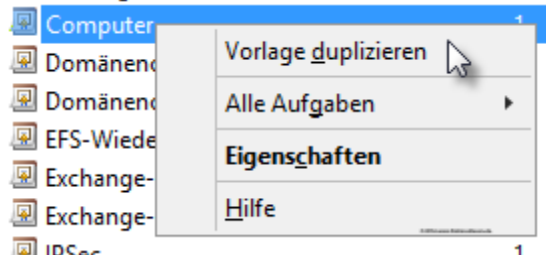
Vorlagen gibt es viele, wichtig ist die rauszusuchen und zu konfigurieren die im Unternehmen (oder wie in meinem Fall, zu Hause) gebraucht werden.

Zertifizierungsstellen mit Microsoft Windows Server 2012R2

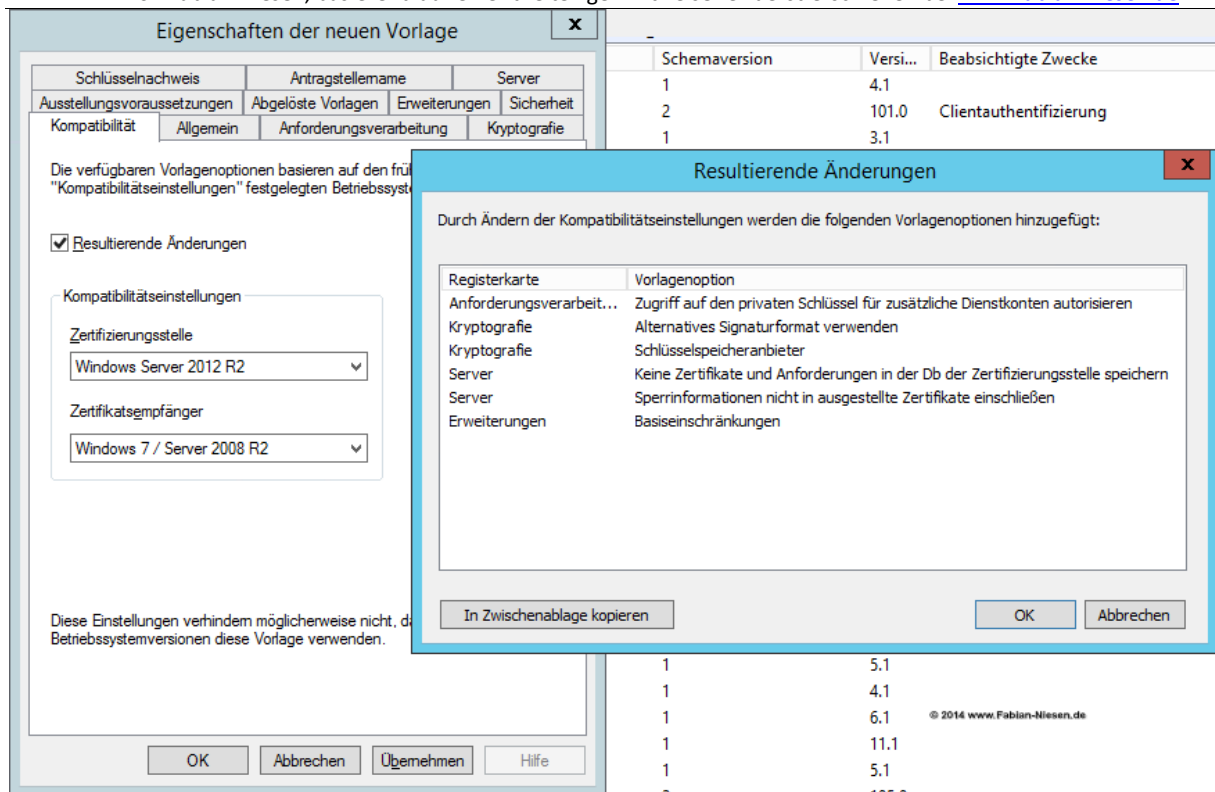
Ein PDF von Fabian Niesen, basierend auf einer dreiteiligen Artikelserie zuerst erschienen bei www.fabian-niesen.de



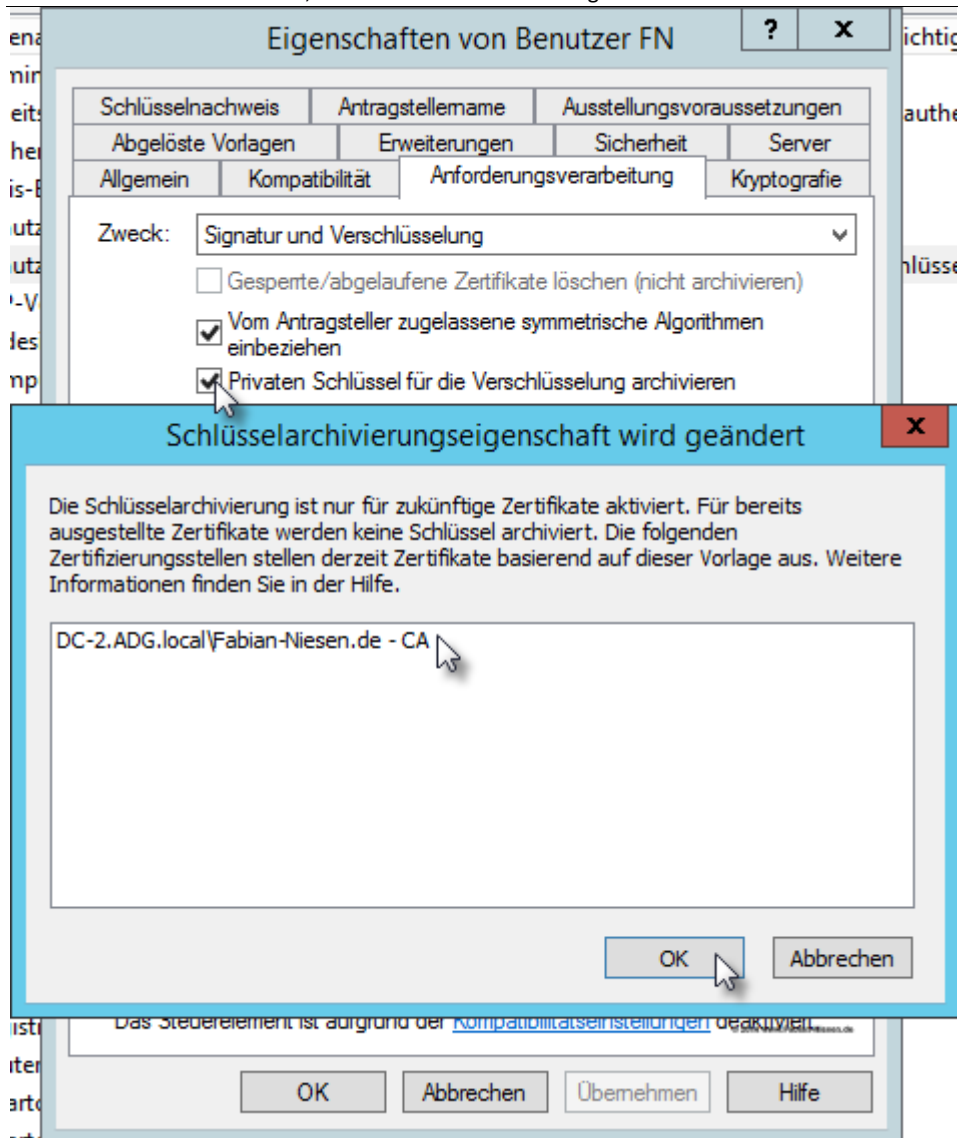
Wenn Sie Anpassungen an den Vorlagen vornehmen möchten, müssen Sie diese duplizieren.



Es empfiehlt sich beim duplizieren entspricht der Umgebung die Kompatibilität zu konfigurieren. Daraus resultieren neue Funktionen, Algorithmen etc. die mit den alten Betriebssystem Versionen noch nicht kompatibel waren.

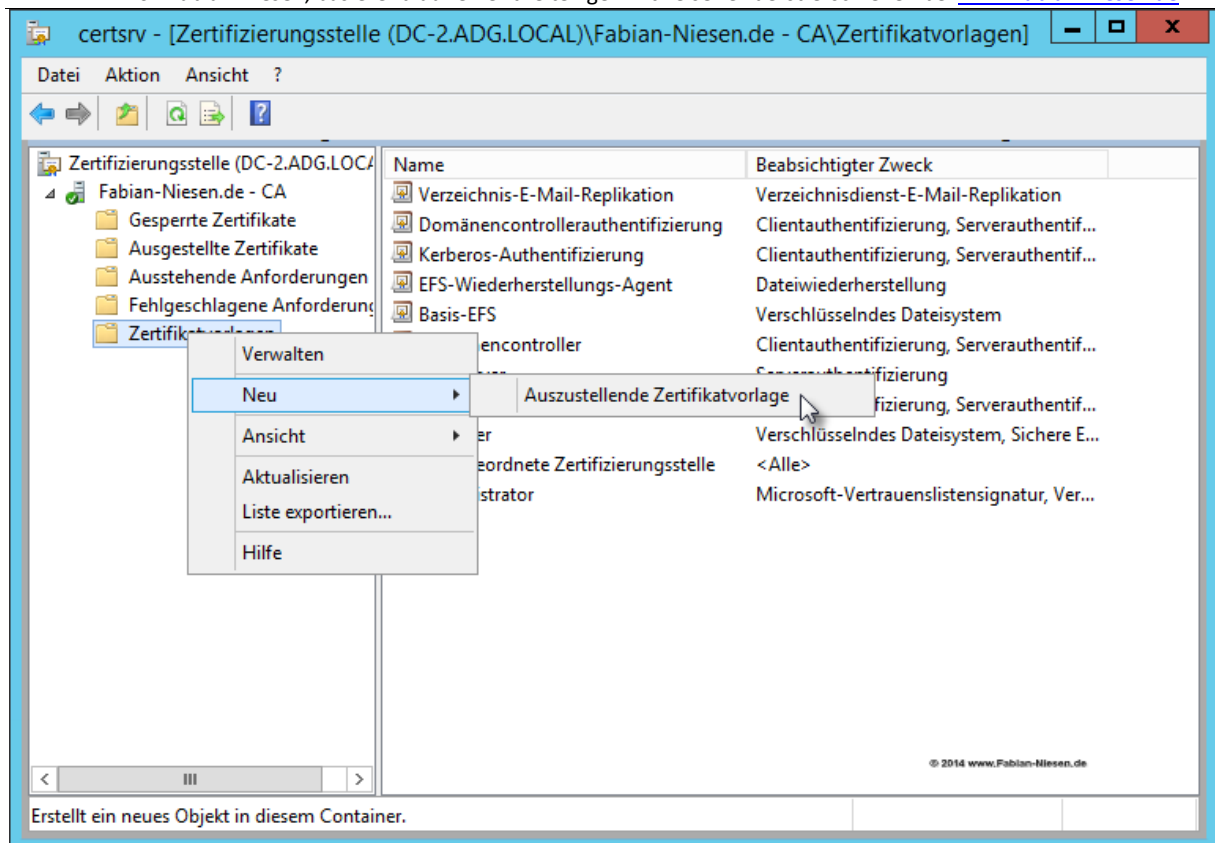


Wenn der Private Schlüssel wiederherstellbar sein soll, muss noch der entsprechende "Wiederherstellungs-Agent" konfiguriert werden.

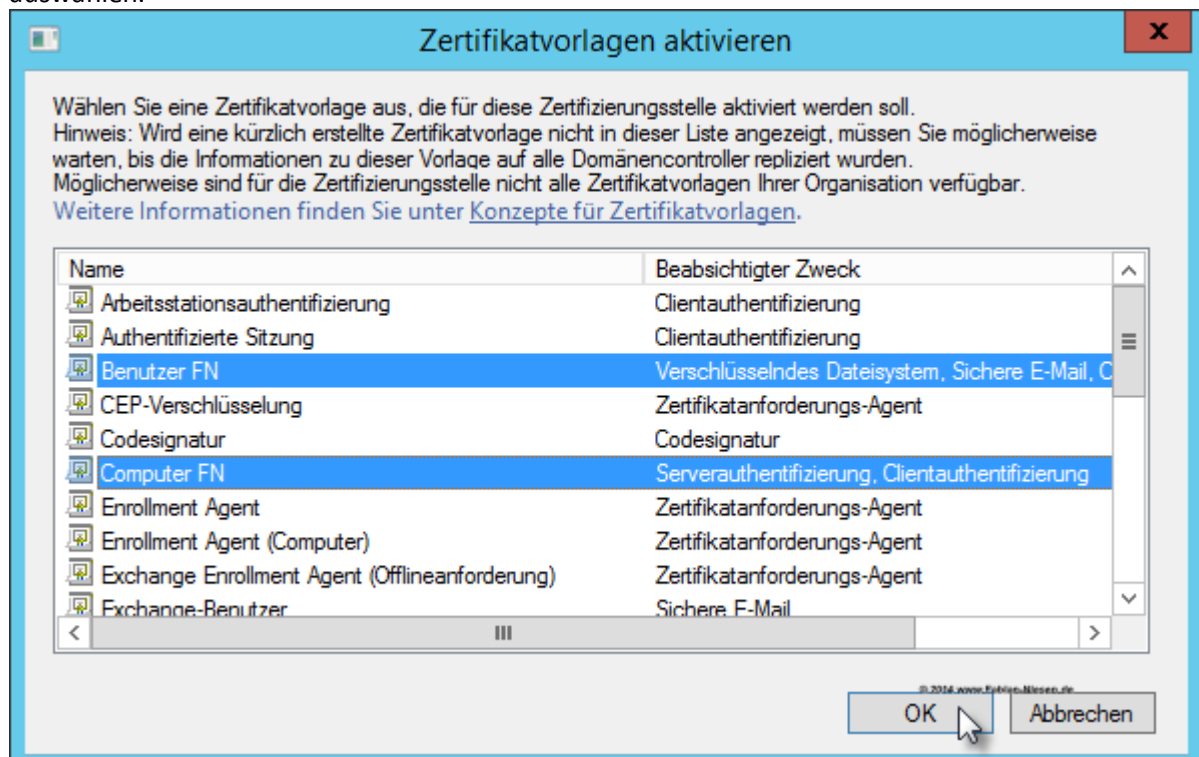


Da die Konfiguration der einzelnen Zertifikatsvorlagen abhängig vom Zweck ist, gehe ich hier nicht weiter drauf ein.

Nach der Konfiguration muss die Zertifikatsvorlage noch als "Auszustellende Zertifikatsvorlage" konfiguriert werden.



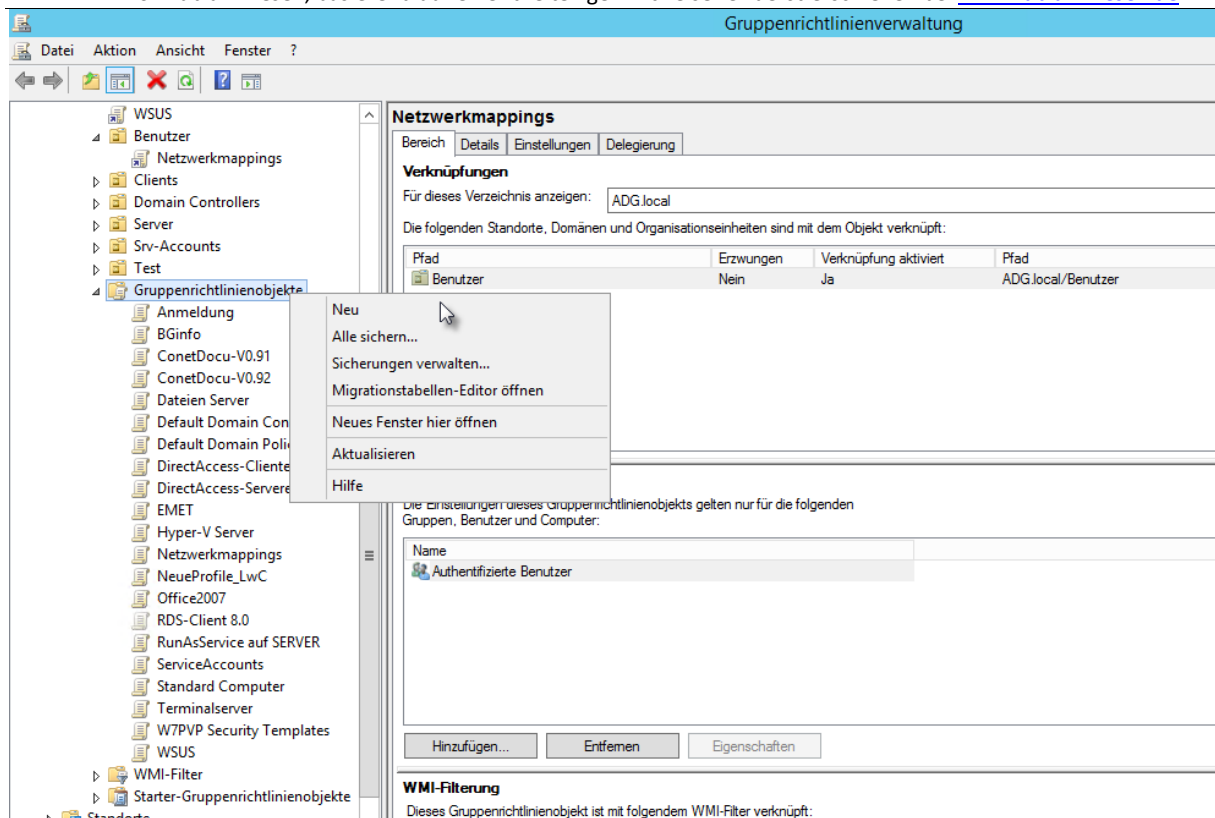
In diesen Dialog können Sie die Zertifikatsvorlagen die Sie veröffentlichen möchten einfach auswählen.



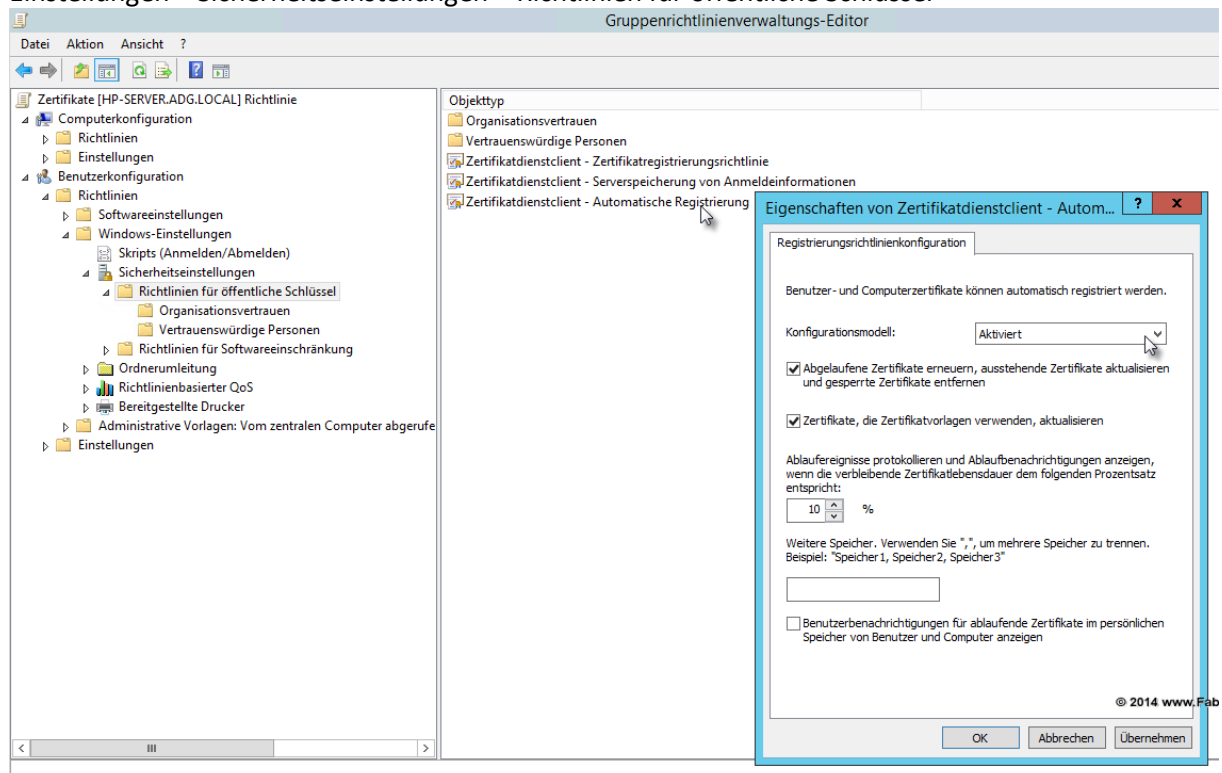
Aktivierung des automatisierten Ausstellen von Zertifikaten (Auto-Enrollment)

Um die Zertifikate automatisch auszurollen nutzen wir eine Gruppenrichtlinie, da die CA auch noch bei den Clients als vertrauenswürdige Zertifizierungsstelle eingetragen werden muss.

Dazu legen wir eine neue Gruppenrichtlinie an.



Für Benutzer finden sich die Einstellungen unter: Benutzerkonfiguration > Richtlinien > Windows Einstellungen > Sicherheitseinstellungen > Richtlinien für öffentliche Schlüssel



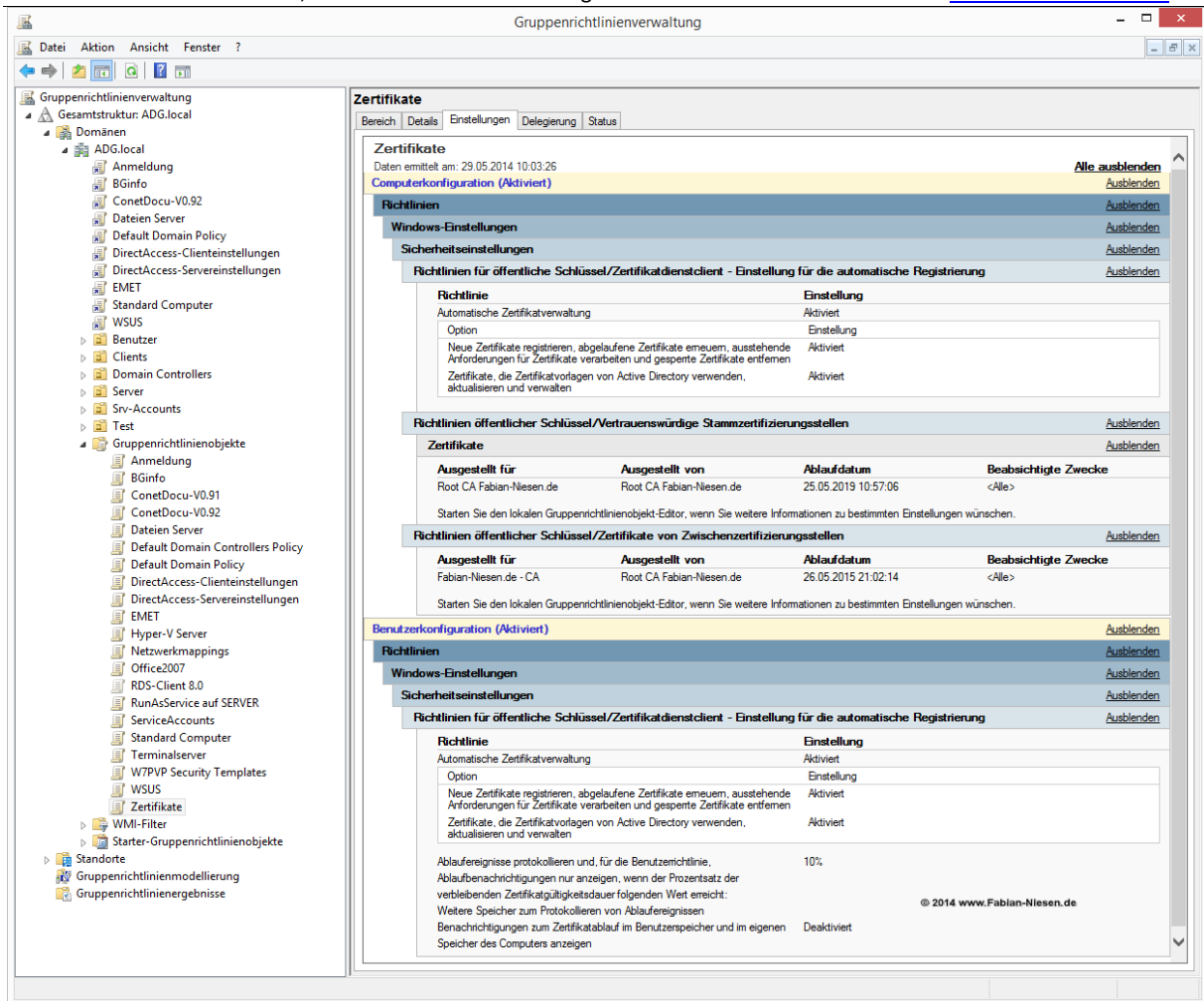
Für Computer findet sich dieselbe Einstellung unterhalb der Computerkonfiguration.

Zusätzlich sollten hier noch das Zertifikat der Root-CA unter "Vertrauenswürdige Stammzertifizierungsstellen" und das Zertifikat der Sub-CA in "Zwischenzertifizierungsstellen", beide allerdings OHNE den privaten Schlüssel!

Die Zusammenfassung der Gruppenrichtlinie sieht dann ungefähr so aus:

Zertifizierungsstellen mit Microsoft Windows Server 2012R2

Ein PDF von Fabian Niesen, basierend auf einer dreiteiligen Artikelserie zuerst erschienen bei www.fabian-niesen.de



Wenn die Gruppenrichtlinie entsprechend verknüpft ist, sollten mit dem nächsten Update der Gruppenrichtlinien die ersten Computer und Benutzer Zertifikate ausgestellt werden, die Domänencontroller haben schon automatisch welche nach der Erstellung der CA erhalten. Wenn die Gruppenrichtlinie auch auf die OU der Domänen Controller angewandt wird, beantragen diese sich automatisch weitere Zertifikate, abhängig von den passenden Vorlagen die sich veröffentlicht haben.

certsrv - [Zertifizierungsstelle (Lokal)\Fabian-Niesen.de - CA\Ausgestellte Zertifikate]

DateiAktionAnsicht?

Zertifizierungsstelle (Lokal)

Fabian-Niesen.de - CA

Gesperrte Zertifikate

Ausgestellte Zertifikate

Ausstehende Anforderung

Fehlgeschlagene Anforderung

Zertifikatsvorlagen

Anforderungs-ID	Antragstellername	Binäres Zertifikat	Zertifikatsvorlage	Seriennummer	Anfangsdatum des Zertifikats	Ablaufdatum des Zertifikats	Ausgestellt
3	ADG\HP-SERVERS	-----BEGIN CERTI...	Domänencontroller (DomainController)	1d00000003d06...	27.05.2014 02:02	26.05.2015 21:02	
4	ADG\DC-25	-----BEGIN CERTI...	Domänencontroller (DomainController)	1d00000004129...	27.05.2014 03:19	26.05.2015 21:02	
5	ADG\FABIAN-WS2...	-----BEGIN CERTI...	Computer FN (1.3.6.1.4.1.311.21.8.8459972.394974...	1d00000005017...	29.05.2014 09:57	26.05.2015 21:02	
6	ADG\Fabian	-----BEGIN CERTI...	Benutzer FN (1.3.6.1.4.1.311.21.8.8459972.3949747...	1d0000000682f...	29.05.2014 09:58	26.05.2015 21:02	
7	ADG\DC-25	-----BEGIN CERTI...	Domänencontrollerauthentifizierung (1.3.6.1.4.1.3...	1d0000000780...	29.05.2014 09:58	26.05.2015 21:02	
8	ADG\DC-25	-----BEGIN CERTI...	Kerberos-Authentifizierung (1.3.6.1.4.1.311.21.8.84...	1d000000085a0...	29.05.2014 09:58	26.05.2015 21:02	
9	ADG\DC-25	-----BEGIN CERTI...	Verzeichnis-E-Mail-Replikation (1.3.6.1.4.1.311.21...	1d00000009f6b...	29.05.2014 09:58	26.05.2015 21:02	
10	ADG\HP-SERVERS	-----BEGIN CERTI...	Domänencontrollerauthentifizierung (1.3.6.1.4.1.3...	1d0000000a316...	29.05.2014 09:58	26.05.2015 21:02	
11	ADG\HP-SERVERS	-----BEGIN CERTI...	Kerberos-Authentifizierung (1.3.6.1.4.1.311.21.8.84...	1d0000000b347...	29.05.2014 09:58	26.05.2015 21:02	
12	ADG\HP-SERVERS	-----BEGIN CERTI...	Verzeichnis-E-Mail-Replikation (1.3.6.1.4.1.311.21...	1d0000000ce2e...	29.05.2014 09:58	26.05.2015 21:02	
13	ADG\Fabian	-----BEGIN CERTI...	Benutzer FN (1.3.6.1.4.1.311.21.8.8459972.3949747...	1d0000000d136...	29.05.2014 09:58	26.05.2015 21:02	

© 2014 www.Fabian-Niesen.de