**Windows: Automatische Zertifikatverteilung (Certificate Autoenrollment) einrichten**

Veröffentlicht am [**9. Januar 2012**](http://www.andysblog.de/windows-automatische-zertifikatverteilung-certificate-autoenrollment-einrichten) von **[andy](http://www.andysblog.de/author/andy" \o "Zeige alle Artikel von andy)**

Verwendet man im Windows-Netzwerk mit Active Directory die Zertifikatdienste und möchte die Zertifikatverteilung als auch Erneuerung nicht per Hand durchführen, bietet sich die automatische Zertifikatverteilung an.

Anbei eine Beispiel-Konfiguration der Gruppenrichtlinie als auch der Zertifizierungsstelle unter Windows Server 2008 R2.

**Allgemein**

Um den Mechanismus der automatischen Zertifikatverteilung nutzen zu können, muss eine Gruppenrichtlinie konfiguriert werden:

*Computer- ODER Benutzerkonfiguration – Richtlinien – Windows-Einstellungen – Sicherheitseinstellungen – Richtlinien für öffentliche Schlüssel – Zertifikatdienst-Automatische Registrierung*

Das Konfigurationsmodell setzt man auf *„Aktiviert“*.

Nun kann man die Einstellungen

*Abgelaufene Zertifikate erneuern, ausstehende Zertifikate aktualisieren und gesperrte Zertifikate entfernen*

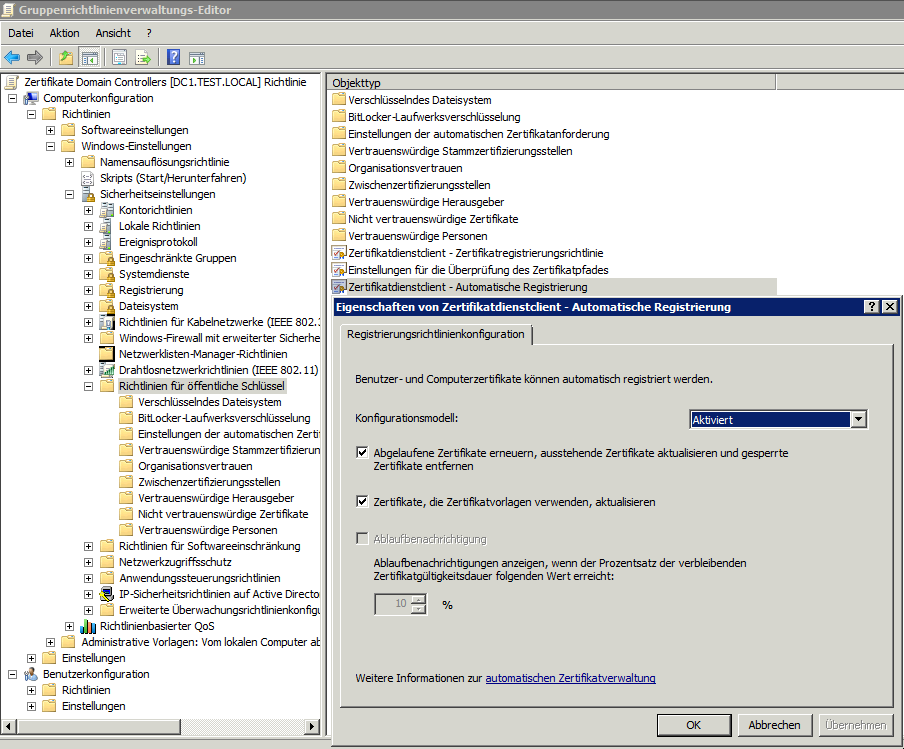
und

*Zertifikate, die Zertifikatvorlagen verwenden, aktualisieren*

für Benutzerzertifikate zusätzlich noch die Einstellung

*Ablaufbenachrichtigung*

aktivieren.

[](http://www.andysblog.de/wp-content/uploads/2012/01/Bildschirmfoto-2012-01-06-um-21.28.08.png)

**Computer-Zertifikate**

Verwendet man die Original-Vorlage für Computer-Zertifikate, dann muss folgende Richtlinie konfiguriert werden:

*Computerkonfiguration – Richtlinien – Windows-Einstellungen – Sicherheitseinstellungen – Richtlinien für öffentliche Schlüssel – Einstellungen der automatischen Zertifikatanforderung*

Dort mit der rechten Maustaste auf *„Neu – Automatische Zertifikatanforderung“* klicken und dem Assistenten folgen.

Dies entspricht dem „klassischen Weg“. Man kann mittels einer „Doppelten Vorlage“ die automatische Anforderung für Computer-Zertifikate ohne die oben genannte Gruppenrichtlinien-Einstellung konfigurieren.

* *„Server-Manager“* öffnen.
* Zu *„Rollen – Active Directory-Zertifikatsdienste – Unternehmens-PKI – Zertifikatvorlagen“* wechseln.
* Die Zertifikatvorlage *„Computer“* mit der rechten Maustaste anklicken und *„Doppelte Vorlage“* auswählen.
* Einen Namen für die „neue“ Vorlage vergeben und zur Registerkarte *„Sicherheit“* wechseln.
* Der Benutzergruppe *„Domänencomputer“* die Berechtigung *„Automatisch registrieren“* erteilen.

Nun muss die „alte“ Vorlage zurückgezogen und die neue Vorlage zugeteilt werden.

* *„Server-Manager“* öffnen.
* Zu *„Rollen – Active Directory-Zertifikatsdienste -NAME DER CA – Zertifiaktvorlagen“*wechseln.
* Die Zertifikatvorlage *„Computer“* löschen.
* Mit der rechten Maustaste auf *„Zertifikatvorlagen“* klicken und *„Neu – Auszustellende Zertifikatvorlage“* auswählen.
* Die neue Zertifikatvorlage hinzufügen.

**Benutzer-Zertifikate**

Damit die automatische Zertifikatverteilung für Benutzer funktioniert, muss das Benutzerkonto im Active Directory mit einer E-Mail-Adresse konfiguriert sein und eine *„Doppelte Vorlage“* in der Zertifizierungsstelle konfiguriert werden:

* *„Server-Manager“* öffnen.
* Zu *„Rollen – Active Directory-Zertifikatsdienste – Unternehmens-PKI – Zertifikatvorlagen“* wechseln.
* Die Zertifikatvorlage *„Benutzer“* mit der rechten Maustaste anklicken und *„Doppelte Vorlage“* auswählen.
* Einen Namen für die „neue“ Vorlage vergeben und zur Registerkarte *„Sicherheit“*wechseln.
* Der Benutzergruppe *„Domänen-Benutzer“* die Berechtigung *„Automatisch registrieren“* erteilen.

**Tipp:** Auf der Registerkarte *„Allgemein“* die Option *„Nicht automatisch neu registrieren wenn ein identisches Zertifikat bereits in Active Directory gespeichert ist“* aktivieren. Dadurch wird verhindert, das ein neues Zertifikat ausgestellt wird, wenn sich ein Benutzer an mehreren Computern anmeldet.

Nun muss die „alte“ Vorlage zurückgezogen und die neue Vorlage zugeteilt werden.

* *„Server-Manager“* öffnen.
* Zu *„Rollen – Active Directory-Zertifikatsdienste -NAME DER CA – Zertifiaktvorlagen“*wechseln.
* Die Zertifikatvorlage *„Benutzer“* löschen.
* Mit der rechten Maustaste auf *„Zertifikatvorlagen“* klicken und *„Neu – Auszustellende Zertifikatvorlage“* auswählen.
* Die neue Zertifikatvorlage hinzufügen.

Sobald die Gruppenrichtlinie greift, werden Zertifikate automatisch verteilt, erneuert und ggf. entfernt.

Je nach Zertifikatvorlage müssen weitere Konfigurationsschritte vorgenommen werden.

**Vorsicht Falle:** Nutzt man die automatische Zertifikatverteilung, dann werden manuell erstellte Zertifikate aus dem Zertifikatspeicher entfernt, sofern die GPO-Einstellung

*„Computerkonfiguration – Richtlinien – Windows-Einstellungen – Richtlinien für öffentliche Schlüssel – Zertifikatdienstclient – Automatische Registrierung“ – „Zertifikate, die Zertifikatvorlagen verwenden, aktualisieren“*

aktiviert ist. Dies geschieht immer dann, wenn keine passende Vorlage vorhanden ist.