

## Smartcard Enrollment mit Windows Server 2008 und Windows 7

Seit Windows Server 2008 hat sich das Verhalten des Webenrollment fuer Windows Server 2008 geaendert, dass keine Smartcard Registrierung fuer Benutzer ueber das Webinterface ausgefuehrt werden kann.

### Quelle:

[http://technet.microsoft.com/de-de/library/cc732517\(W.S.10\).aspx](http://technet.microsoft.com/de-de/library/cc732517(W.S.10).aspx)

Mit einer Windows Server 2003 PKI und Windows Vista / Windows 7 Clients kann das Verhalten wie folgt geaendert werden:

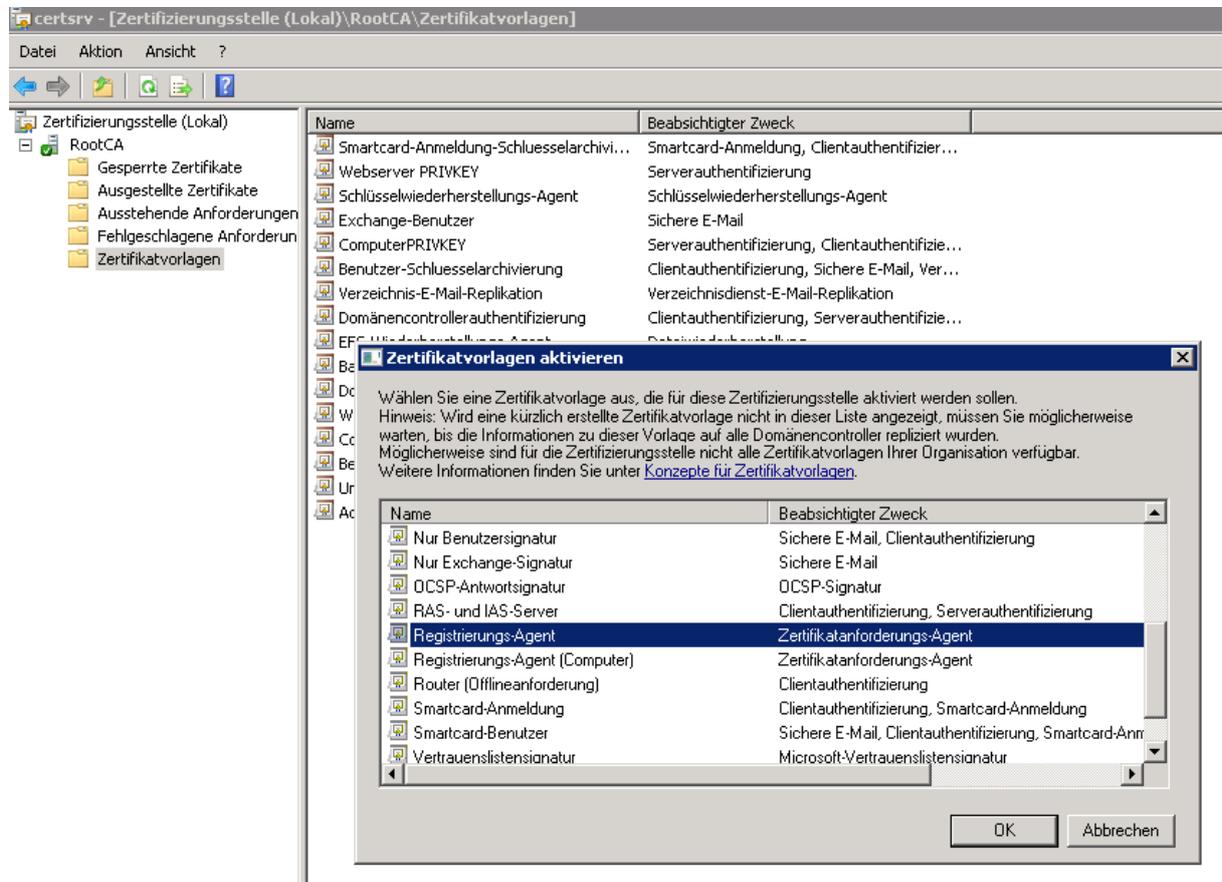
<http://www.it-training-grote.de/blog/?p=95>

Dank Windows Vista und Windows 7 koennen jetzt Smartcard Zertifikate auch fuer andere Benutzer ueber das Zertifikat-MMC SnapIn ausgerollt werden.

Auf der Smartcard Enrollment Workstation muss die Smartcard Middleware Software installiert werden. Hinweis: Fuer die Smartcard Enrollment Workstation sollten zusaetzliche Sicherheitsmassnahmen getroffen werden.

Als erstes ein Registrierungs Agenten Zertifikat fuer die Smartcard Enrollment Workstation ausrollen

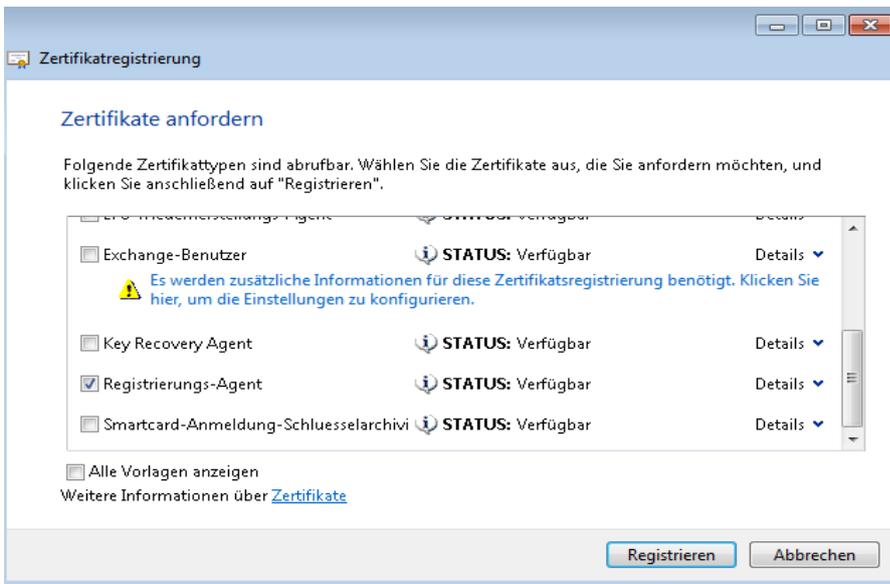
Auf der Windows Server 2008 Enterprise CA eine neue Vorlage aktivieren.



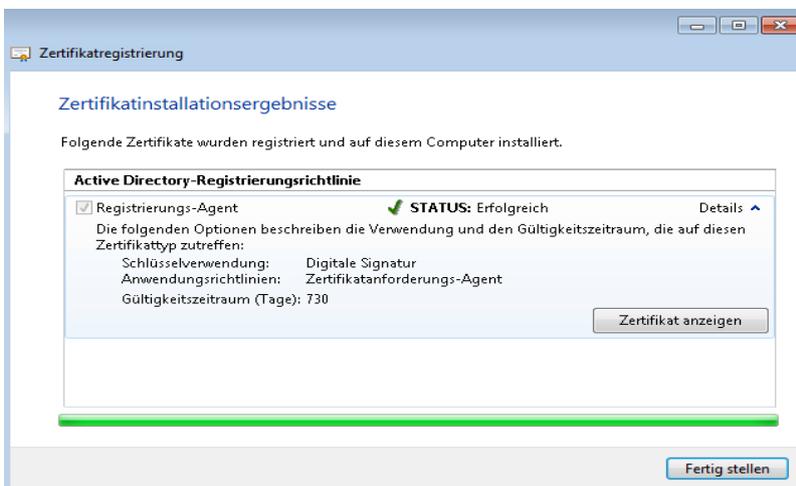
Auf der Smartcard Enrollement Workstation eine MMC öffnen und den Zertifikatspeicher des Benutzers öffnen.



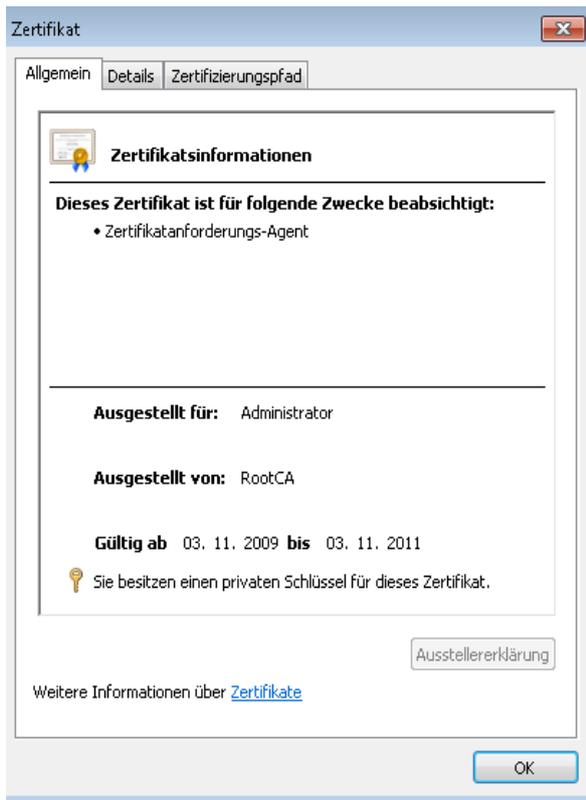
Dort unter Eigene Zertifikate ein Registrierungs-Agenten Zertifikat anfordern



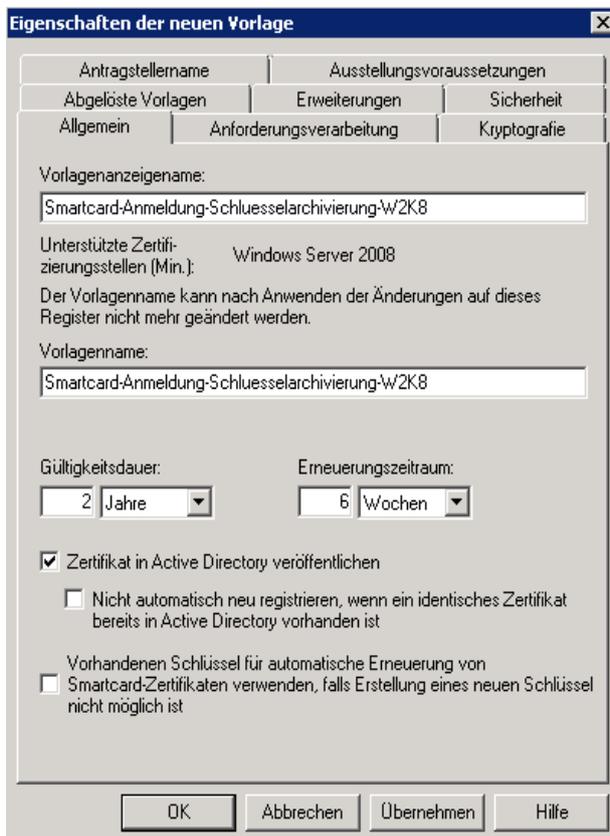
Hat gefunzt



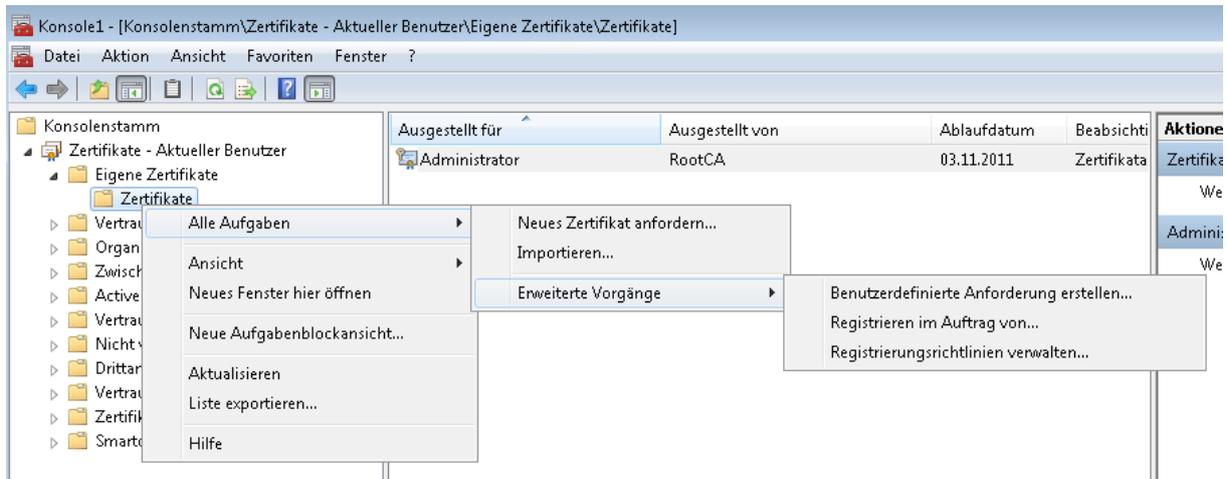
Alles sieht gut aus.



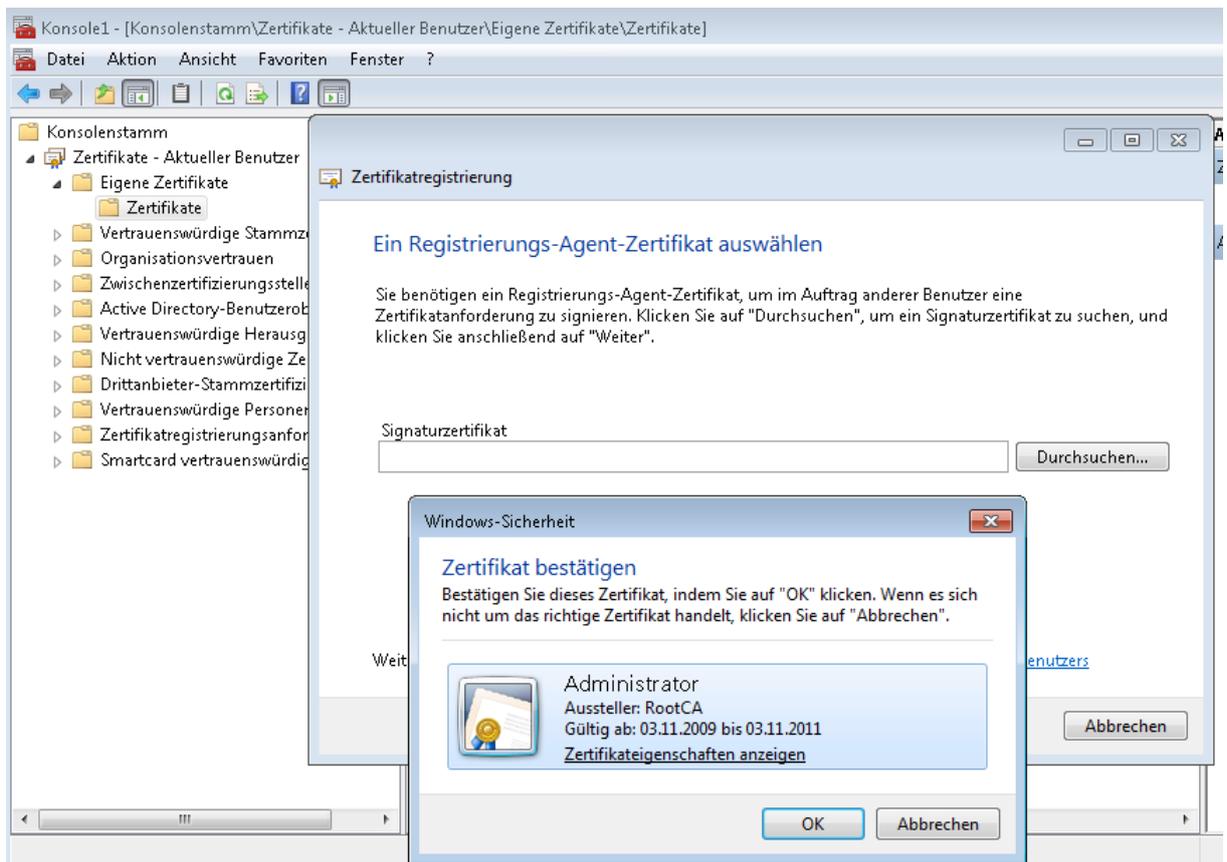
Benutzerdefinierte V3 Zertifikatvorlage fuer die Smartcard Anmeldung erstellen mit Schluesselarchivierung und ein paar anderen Besonderheiten



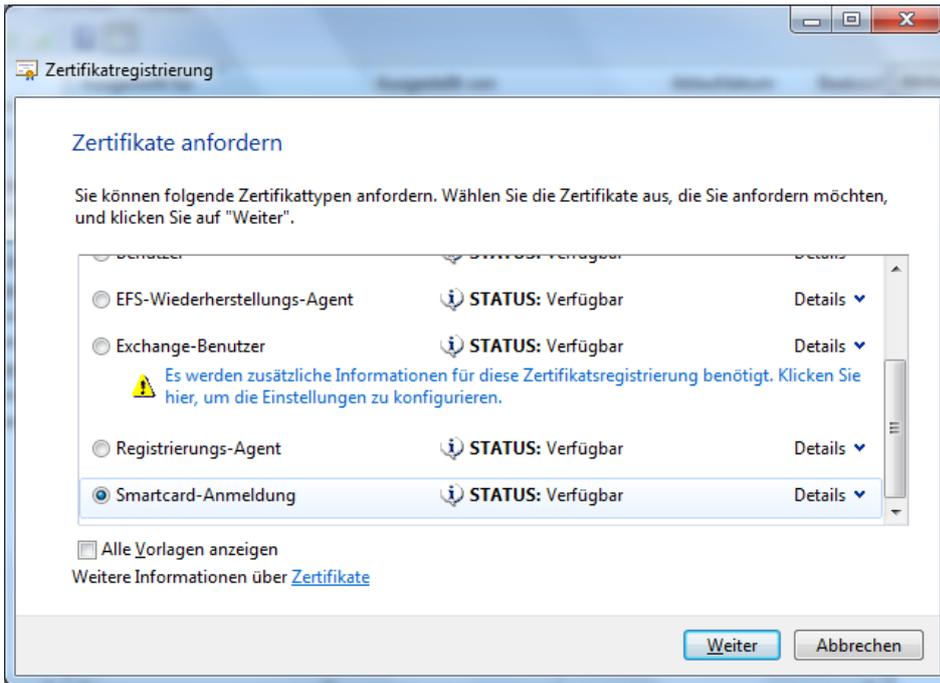
Auf der Smartcard Enrollment Workstation eine erweiterte Zertifikatanforderung auswaehlen und dort „Registrieren im Auftrag von“ auswaehlen



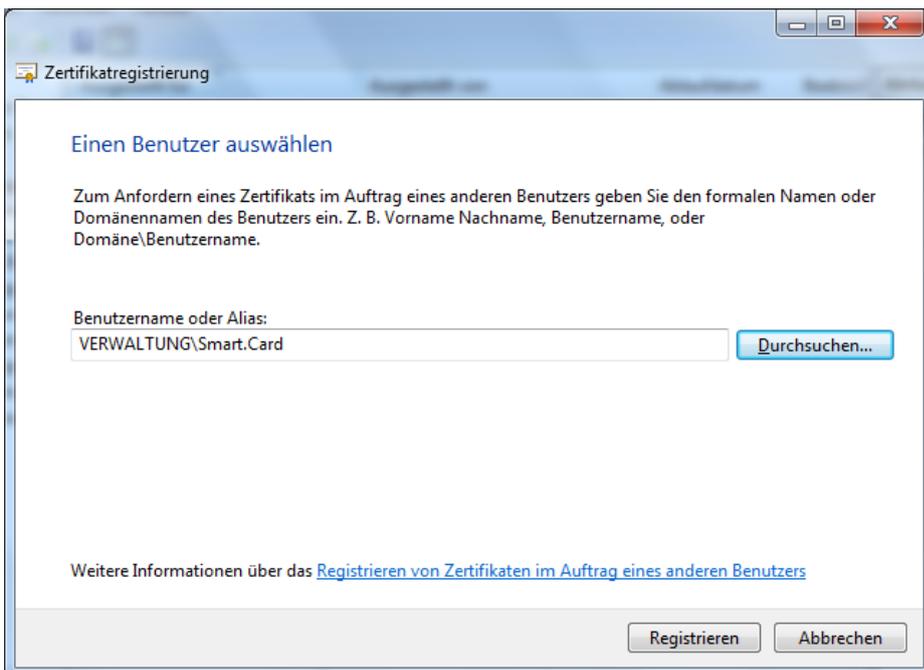
Das Registrierungs-Agenten Zertifikat auswaehlen



Danach die Smartcard-Anmeldungs-vorlage auswaehlen.

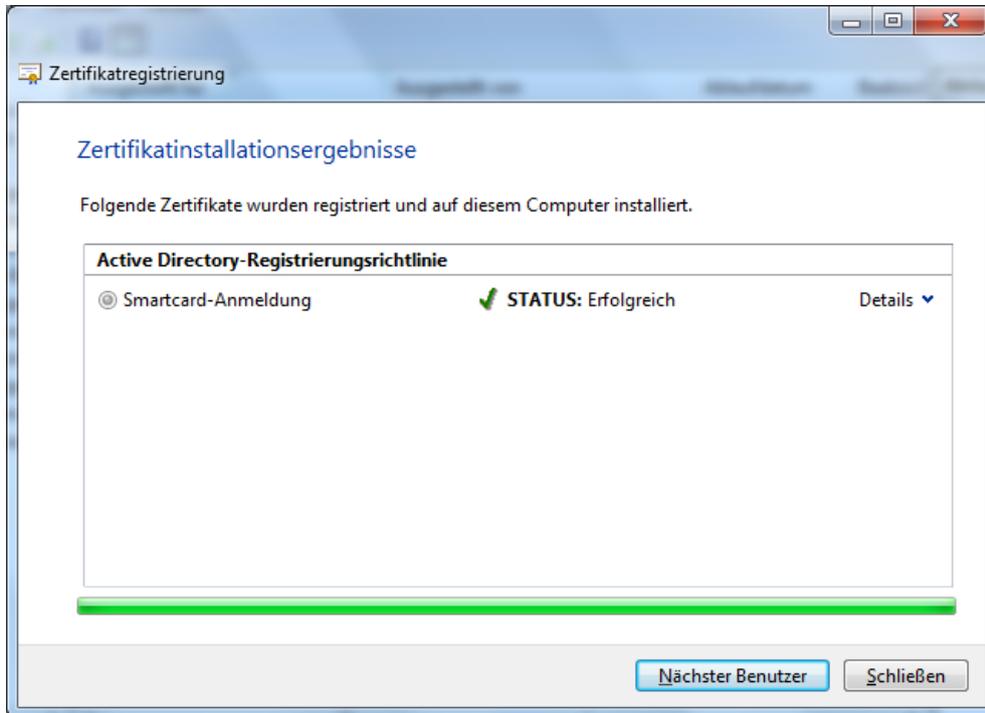


Einzuschreibenden Benutzer auswählen.

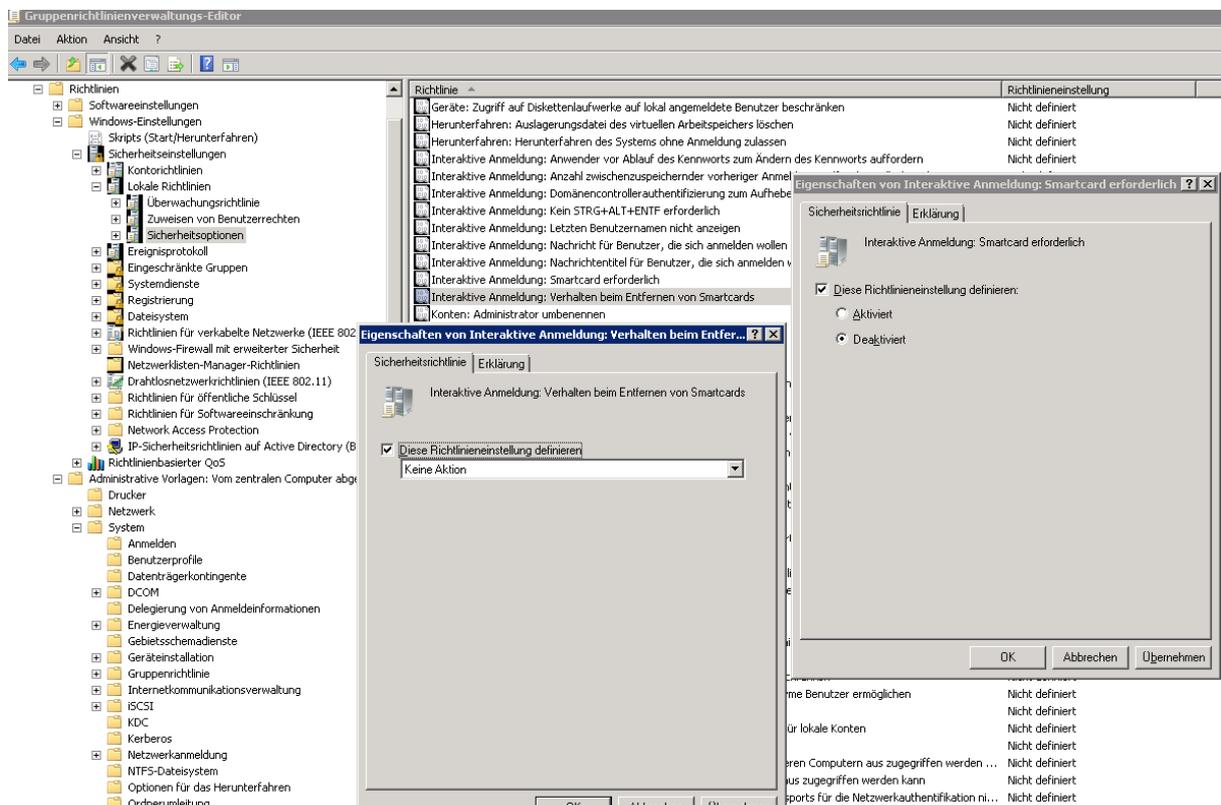


## Benutzer einschreiben

Bei der Einschreibung wird der private Schlüssel auf die Smartcard geschrieben und der Benutzer zur Eingabe der Smartcard Pin aufgefordert.

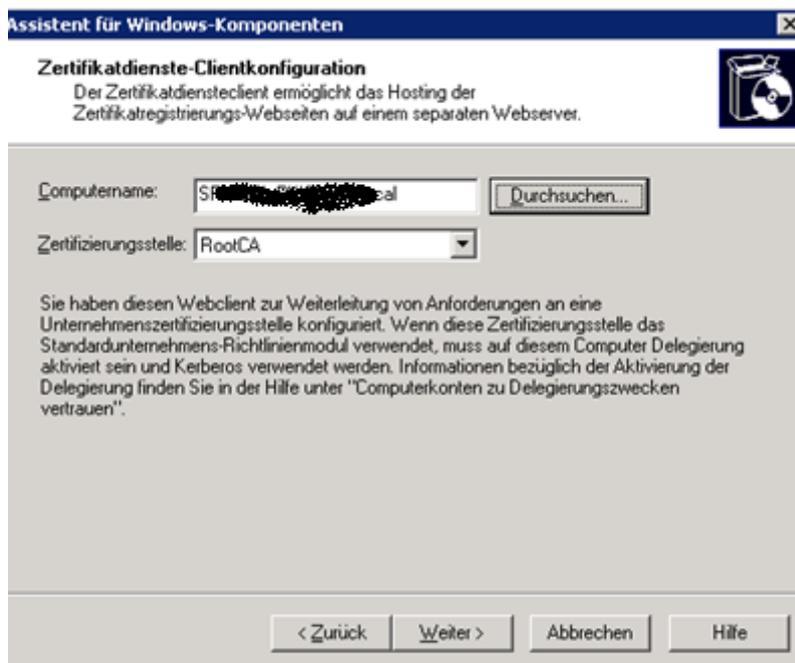
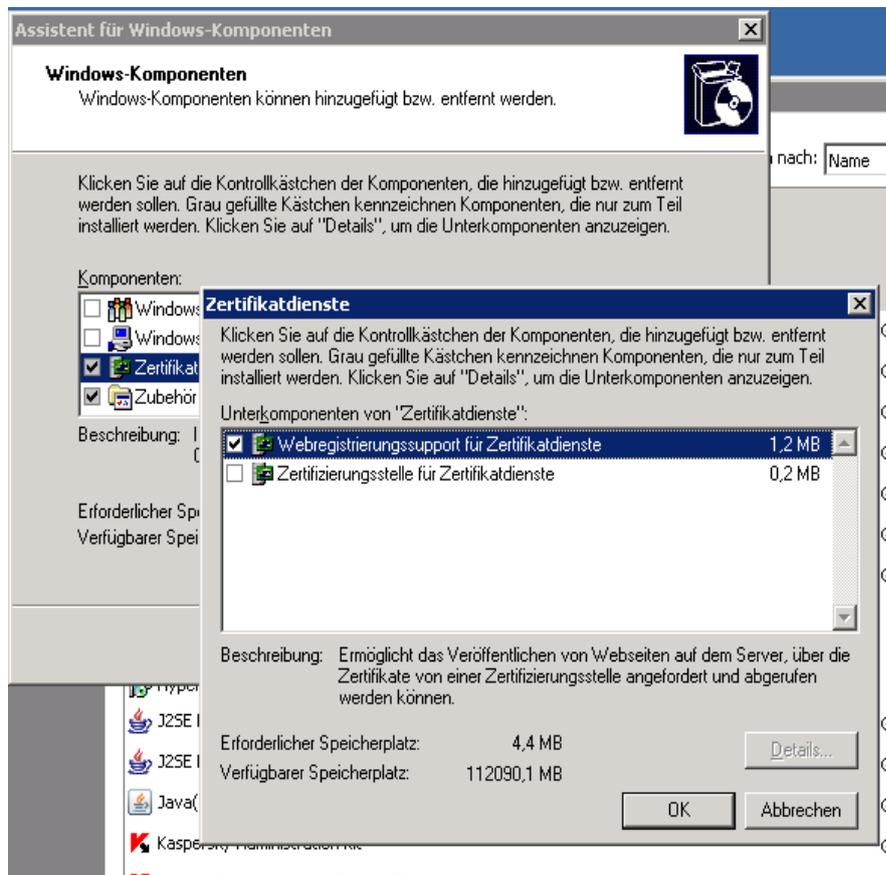


Jetzt kann man das ganze noch mit Hilfe von Gruppenrichtlinien verhuebschen

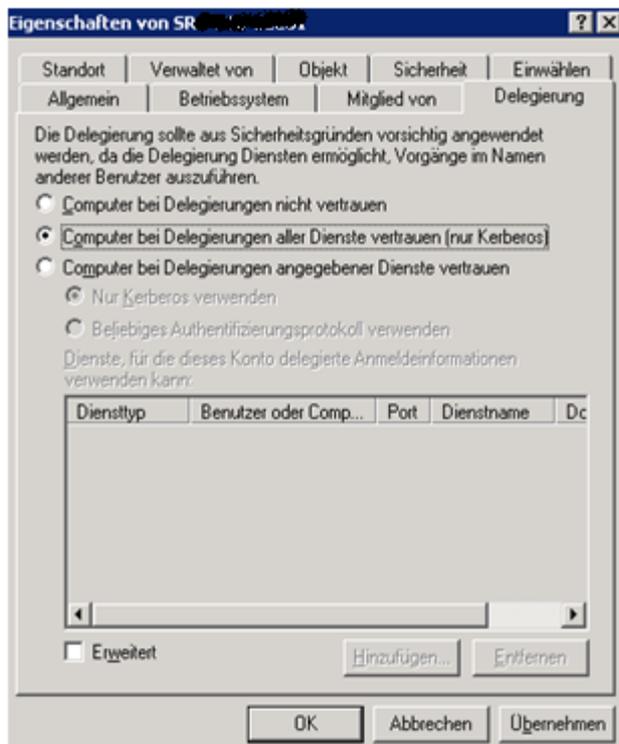


## Alternativ

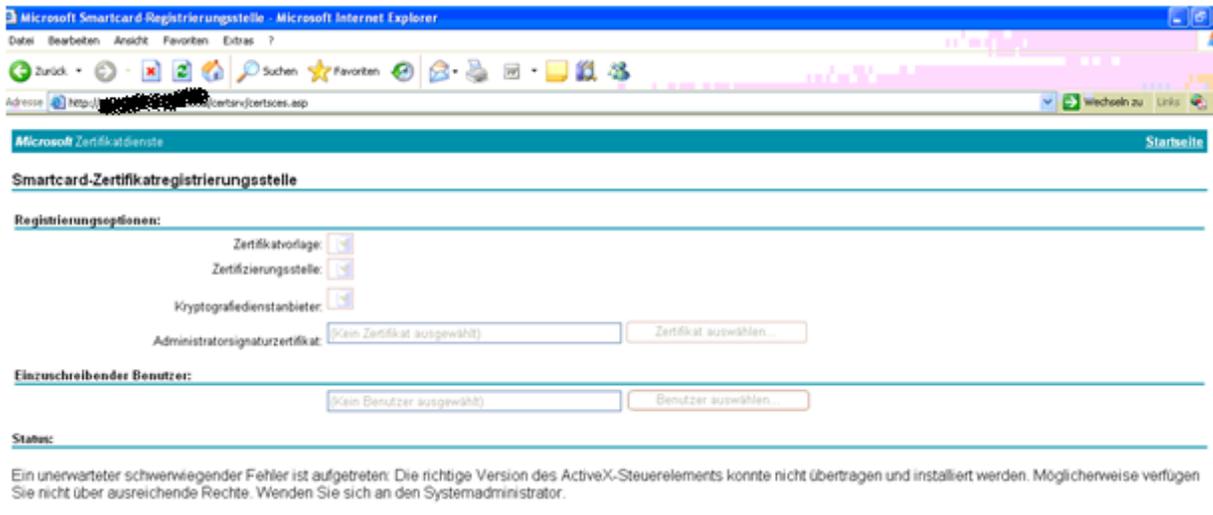
### Installation des Webregistrierungssupports auf einem Windows Server 2003



Der Computer mit der Webregistrierung muss „Trusted for Delegation“ sein



Standard Meldung seit Jahren ☺



Webseite in die vertrauenswürdigen Sites im IE uebernehmen

Microsoft Smartcard-Registrierungsstelle - Microsoft Internet Explorer

Datei Bearbeiten Ansicht Favoriten Extras ?

Zurück Zurück Suchen Favoriten

Adresse http://[redacted]local/certsrv/certsces.asp

---

**Microsoft** Zertifikatdienste

---

**Smartcard-Zertifikatregistrierungsstelle**

---

**Registrierungsoptionen:**

Zertifikatvorlage:

Zertifizierungsstelle:

Kryptografiedienstanbieter:

Administratorsignaturzertifikat:

---

**Einzuschreibender Benutzer:**

---

**Status:**

Einen Moment bitte. ActiveX-Control wird geladen.

Webseite zu den sicheren Sites hinzufuegen

Zurück Zurück Suchen Favoriten

Adresse http://[redacted]local/certsrv/certsces.asp

---

**Microsoft** Zertifikatdienste Startseite

---

**Smartcard-Zertifikatregistrierungsstelle**

---

**Registrierungsoptionen:**

Zertifikatvorlage:

Zertifizierungsstelle:

Kryptografiedienstanbieter:

Administratorsignaturzertifikat:

---

**Einzuschreibender Benutzer:**

---

**Status:**

Geben Sie die Smartcard des Benutzers in einen Leser ein, und klicken Sie auf "Registrieren".

Pin eingeben

Microsoft Zertifikatsdienste

### Smartcard-Zertifikatsregistrierungsstelle

**Registrierungsoptionen:**

Zertifikatsvorlage: Smartcard-Anmeldung  
 Zertifizierungsstelle: RootCA  
 Kryptografiedienstanbieter: eToken Base Cryptographic Provider  
 Administratorsignaturzertifikat: Administrator

**Einzuschreibender Benutzer:**  
 Smart Card

**Status:**  
 Warten Sie während der Benutzer eingeschrieben wird...

**Anmeldung: Test**

Beim eToken anmelden eToken

eToken-Kennwort eingeben

eToken-Name: Test  
 Kennwort: .....

Aktuelle Sprache: DE

OK Abbrechen

Fertig

Microsoft Zertifikatsdienste

### Smartcard-Zertifikatsregistrierungsstelle

**Registrierungsoptionen:**

Zertifikatsvorlage: Smartcard-Anmeldung  
 Zertifizierungsstelle: RootCA  
 Kryptografiedienstanbieter: eToken Base Cryptographic Provider  
 Administratorsignaturzertifikat: Administrator

**Einzuschreibender Benutzer:**  
 Smart Card@w.bfw.local

**Status:**  
 Die Smartcard ist fertig. Klicken Sie auf "Zertifikat anzeigen", um sicher zu stellen, dass das Zertifikat d...

**Zertifikat**

Algemein Details Zertifizierungspfad

**Zertifikatsinformationen**

Dieses Zertifikat ist für folgende Zwecke beabsichtigt:

- Garantiert dem Remotecomputer Ihre Identität
- Smartcard-Anmeldung

**Ausgestellt:** Smart Card

**Ausgestellt:** RootCA

**Gültig ab:** 04.11.2009 **bis:** 04.11.2010

☞ Sie besitzen einen privaten Schlüssel für dieses Zertifikat.

Ausstellereklärung

OK

Anmeldung an Windows 7



## Smart.Card

Sperrung mit Smartcard aufheben

Smart.Card [REDACTED]

FDV



Andere Anmeldeinformationen

 Windows 7 Enterprise