#### 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(WS.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 Enrollement Workstation ausrollen

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



Auf der Smartcard Enrollement Workstation eine MMC oeffnen und den Zertifkatspeicher des Benutzers oeffnen.

🚡 Konsole1 - [Konsolenstamm\Zertifikate - Aktuell	er Benutzer]
🔚 Datei Aktion Ansicht Favoriten Fenster	?
🗢 🔿 🔽 🗔 🤄 🔀 🗊	
<ul> <li>Konsolenstamm</li> <li>Zertifikate - Aktueller Benutzer</li> <li>Eigene Zertifikate</li> <li>Vertrauenswürdige Stammzertifizierungs</li> <li>Organisationsvertrauen</li> <li>Zwischenzertifizierungsstellen</li> <li>Active Directory-Benutzerobjekt</li> <li>Vertrauenswürdige Herausgeber</li> <li>Nicht vertrauenswürdige Zertifikate</li> <li>Drittanbieter-Stammzertifizierungsstellen</li> <li>Vertrauenswürdige Personen</li> <li>Zertifikatregistrierungsanforderungen</li> <li>Smartcard vertrauenswürdige Stämme</li> </ul>	Name des logischen Speichers         Eigene Zertifikate         Vertrauenswürdige Stammzertifizierungsstellen         Organisationsvertrauen         Zwischenzertifizierungsstellen         Active Directory-Benutzerobjekt         Vertrauenswürdige Herausgeber         Nicht vertrauenswürdige Zertifikate         Drittanbieter-Stammzertifizierungsstellen         Vertrauenswürdige Personen         Zertifikatregistrierungsanforderungen         Smartcard vertrauenswürdige Stämme

Dort unter Eigene Zertifikate ein Registrierungs-Agenten Zertifikat anfordern

		- • •
Zertifikatregistrierung		
Zertifikate anfordern Folgende Zertifikattypen sind abrufb	ar. Wählen Sie die Zertifikate aus, die Sie anfo	rdern möchten, und
klicken sie anschließend auf Registri	eren .	
Exchange-Benutzer	😲 STATUS: Verfügbar	Details 💌
Es werden zusätzliche Info hier, um die Einstellunger	ormationen für diese Zertifikatsregistrierung k n zu konfigurieren.	enötigt. Klicken Sie
🔲 Key Recovery Agent	🐳 STATUS: Verfügbar	Details 👻 🗌
Registrierungs-Agent	🗘 STATUS: Verfügbar	Details 👻 🗏
Smartcard-Anmeldung-Schlues	selarchivi 🔱 STATUS: Verfügbar	Details 👻 🔔
Alle Vorlagen anzeigen Weitere Informationen über Zertifikat	<u>e</u>	
	Regist	rieren Abbrechen

### Hat gefunzt

ertifikatregistrierung		
Zertifikatinstallationserge	bnisse	
Folgende Zertifikate wurden regis Active Directory-Registrierun	triert und auf diesem Computer installiert. gsrichtlinie	
📝 Registrierungs-Agent	🖌 STATUS: Erfolgreich	Details 🔺
Die folgenden Optionen bes Zertifikattyp zutreffen: Schlüsselverwendung: Anwendungsrichtlinien: Gültigkeitszeitraum (Tag	chreiben die Verwendung und den Gültigke Digitale Signatur Zertifikatanforderungs-Agent (e): 730	itszeitraum, die auf diesen Zertifikat anzeigen
		Fertig steller

Alles sieht gut aus.



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

Eigenschaften der neuen Vorlage
Antragstellername Ausstellungsvoraussetzungen
Abgelöste Vorlagen Erweiterungen Sicherheit
Allgemein Anforderungenerscheitung Kupterstie
Vorlagenanzeigename:
Smartcard-Anmeldung-Schluesselarchivierung-W2K8
Unterstützte Zertifi- zierungsstellen (Min.):
Der Vorlagenname kann nach Anwenden der Änderungen auf dieses Register nicht mehr geändert werden.
Vorlagenname:
Smartcard-Anmeldung-Schluesselarchivierung-W2K8
Gültigkeitsdauer: Erneuerungszeitraum:
Zertifikat in Active Directory veröffentlichen
Nicht automatisch neu registrieren, wenn ein identisches Zertifikat bereits in Active Directory vorhanden ist
Vorhandenen Schlüssel für automatische Erneuerung von Smartcard-Zertifikaten verwenden, falls Erstellung eines neuen Schlüssel nicht möglich ist
OK Abbrechen Übernehmen Hilfe

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



#### Das Registrierungs-Agenten Zertifikat auswaehlen



Danach die Smartcard-Anmeldungsvorlage auswaehlen.

Zertifikate anfordern		
Sie können folgende Zertifikattypen anfo und klicken Sie auf "Weiter".	rdern. Wählen Sie die Zertifikate aus, die	Sie anfordern möchten
© EFS-Wiederherstellungs-Agent	STATUS: Verfügbar	Details 🗸
Exchange-Benutzer	③ STATUS: Verfügbar	Details 🗸
Es werden zusätzliche Informa hier, um die Einstellungen zu	ationen für diese Zertifikatsregistrierung konfigurieren.	benötigt. Klicken Sie
Registrierungs-Agent	🤹 STATUS: Verfügbar	Details 👻
Smartcard-Anmeldung	(i) STATUS: Verfügbar	Details 💌
Alle Vorlagen anzeigen		

Einzuschreibenden Benutzer auswaehlen.

Zertifikatregistrierung
Einen Benutzer auswählen Zum Anfordern eines Zertifikats im Auftrag eines anderen Benutzers geben Sie den formalen Namen oder
Domanennamen des Benutzers ein. 2. B. vorname Nachname, Benutzername, oder Domäne\Benutzername. Benutzername oder Alias:
VERWALTUNG\Smart.Card
Weitere Informationen über das <u>Registrieren von Zertifikaten im Auftrag eines anderen Benutzers</u>
Registrieren Abbrechen

Benutzer einschreiben

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

📮 Ze	ertifikatregistrierung	August an annua	
	Zertifikatinstallationsergebnis	sse	
	Folgende Zertifikate wurden registriert	t und auf diesem Computer installiert.	
	Active Directory-Registrierungsrid	chtlinie	
	Smartcard-Anmeldung	STATUS: Erfolgreich	Details 🕶
8			
		<u>N</u> ächster Benutz	zer <u>S</u> chließen

Jetzt kann man das ganze noch mit Hilfe von Gruppenrichtlinien verhuebschen



## Alternativ

Installation des Webregistrierungssupports auf einem Windows Server 2003

Assistent für Windows-Komponenten 🛛 🗙
Zertifikatdienste-Clientkonfiguration Der Zertifikatdiensteclient ermöglicht das Hosting der Zertifikatregistrierungs-Webseiten auf einem separaten Webserver.
Computername: SHAMEN Computername: Durchsuchen
Sie haben diesen Webclient zur Weiterleitung von Anforderungen an eine Unternehmenszertifizierungsstelle konfiguriert. Wenn diese Zertifizierungsstelle das Standardunternehmens-Richtlinienmodul verwendet, muss auf diesem Computer Delegierung aktiviert sein und Kerberos verwendet werden. Informationen bezüglich der Aktivierung der Delegierung finden Sie in der Hilfe unter "Computerkonten zu Delegierungszwecken vertrauen".
< <u>Z</u> urück <u>W</u> eiter> Abbrechen Hilfe

Der Computer mit der Webregistrierung muss "Trusted for Delegation" sein

ansenarcen rom	SR CHARLEN			?
Standort Ver Allgemein	waltet von   Obj Betriebssystem	jekt   Sich Mitglied vo	enheit Einv n Delegi	wählen ierung
Die Delegierung so werden, da die Del anderer Benutzer a	lte aus Sicherheitsgr egierung Diensten er uszuführen.	ründen vorsich möglicht, Vorg	tig angewendel jänge im Namer	t n
Computer bei D	elegierungen nicht v elegierungen aller Di	ertrauen	n (nur Kerberor	3
C Beliebiges / Dienste, für die	kuthentifizierungspro dieses Konto delegi	tokoll verwend erte Anmeldeir	len formationen	
Diensttyp	Benutzer oder Co	omp Port	Dienstname	Dc
				P
✓ [ □ Erweitert		Hinzufüge	n Entier	▶ nen

Standard Meldung seit Jahren ©

Alicrosoft Smartcard Registrierungsstelle - Microso	ft Internet Explorer				
Datei Bearbeiten Ansicht Favoriten Extras ?				1.00	4
🕜 Zurick • 🐑 · 💌 🖻 🏠 🔎 Suchen 🚽	(Favoritan 🕢 🔗 🍓	🖻 • 🧾 🏭 🦓		alati-t	V 🗗 Wachasin nu 🛛 Linia 🖗 🛛
and a set and a set of a set o					
Microsoft Zertrikatdienste					Startseite
Smartcard-Zertifikatregistrierungsstelle					
Registrierungsoptionen:					
Zertifikatvorlage:					
Zertifizierungsstelle:					
Kryptografiedienstanbieter.					
Administratorsignaturzertifikat:	(Kein Zertifikat ausgewählt)		Zertifikat auswählen		
Einzuschreibender Benutzer:					
	(Kein Benutzer ausgewählt)		Benutzer auswählen	0	
Status:					
Ein unerwarteter schwerwiegender Fehler ist a Sie nicht über ausreichende Rechte. Wenden S	ufgetreten: Die richtige Vers Sie sich an den Systemadmi	sion des ActiveX-S inistrator.	teuerelements konnte nich	t übertragen und installiert wer	den. Möglicherweise verfügen

Webseite in die vertrauenswuerdigen Sites im IE uebernehmen

Microsoft Smartcard-Registrierungsstelle - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
🌀 Zurück 🔹 💿 🔹 😰 🏠 🔎 Suchen 🤺 Favoriten 🏼 🊱 😒 - 🌺 🔟 🕶 🧫 🏭 🍇
Adresse 🛃 http://gtownanew.gtownanew.cal/certsrv/certsces.asp
Microsoft Zertifikatdienste
Smartcard-Zertifikatregistrierungsstelle
Registrierungsoptionen:
Zertifikatvorlage:
Zertifizierungsstelle:
Kryptografiedienstanbieter:
Administratorsignaturzertifikat: (Kein Zertifikat ausgewählt) Zertifikat auswählen
Einzuschreibender Benutzer:
(Kein Benutzer ausgewählt) Benutzer auswählen
Status:
Einen Moment bitte. ActiveX-Control wird geladen.

## Webseite zu den sicheren Sites hinzufuegen

🔇 ðarúði 🔹 🐑 - 💌 🖻 🏠 🔎 Suchen 🥠	Pavoten 🕢 🔗 - 🌺 🖂 - 🛄 🇱 🦓
Adresse 🕘 http://www.ada.cla.it/ada.cajicertary/certaces.asp	👻 🛃 Wechseln zu Unis 🔍
Microsoft Zentifikatdienste	Startseit
Smartcard-Zertifikatregistrierungsstelle	
Registrierungsoptionen;	
Zertifikatvorlage:	Smartcard-Anneldung 🛩
Zentifizierungsstelle:	RootCA 💌
Kryptografiedienstanbieter:	eToken Base Cryptographic Provider
Administratorsignaturzertilikat:	Administrator Zertifikat auswählen
Einzuschreibender Benutzer:	
	Smart, Card@vw.bfw.local Benutzer auswählen
Status:	
Geben Sie die Smartcard des Benutzers in ein	en Leser ein, und klicken Sie auf "Registrieren".
	Registrieren

Pin eingeben

🌀 Zurick • 💿 - 💌 🖻 🏠 🔎 Suchen 👷	- Favorten 🔗 🍰 🕅 - 🛄 🏭 🥸					
Adresse 1 http://second.cal/certsrv/certsces.asp						
Microsoft Zertifikatdienste						
Smartcard-Zertifikatregistrierungsstelle						
Registrierungsoptionen:						
Zertifikatvorlage: Smartcard-Anmeldung 🕑						
Zertifizierungsstelle: RootCA 📝						
Kryptografiedienstanbieter.	Kryptografiedienstanbieter: eToken Base Cryptographic Provider					
Administratorsignaturzertifikat:	Administrator					
Einzuschreibender Benutzer:	т.¢					
8	Smart.Cardi Beim eToken anmelden eToKen					
Status:	eToken-Kenneurst einneben					
Warten Sie während der Benutzer eingeschriebe	ben wird					
	Criver Preside					
	Kennwort:					
	Aktuelle Sprache: DE					
	OK Abbrechen					

# Fertig

Microsoft Smartcard Registrierungsstelle - Microsof	t Internet Explorer			
label Dearbeiten Ansicht Pavoriten Eidnas 7				
🌀 Zurick • 🔘 · 💌 🗟 🚮 🔎 Suchen 対	(Favorken 🚱 🝰 🍓 📧 • 🛄 🛍 3	8		
dresse a) http://www.www.alcertary/certaces.asp			Vechseh zu Uni	
Microsoft Zertifikatőienste				Sta
Smartcard-Zertifikatregistrierungsstelle				
Registrierungsoptionen:	A		200000	
Zertifikatvorlage:			Zerinikai	
Zertifizierungsstelle:	RectCA		Aligemein Details Zertifizierungspfad	-
Kryptografiedienstanbieter:	eToken Base Cryptographic Provider 🤘		823	* II.
A desirate test sectors at sector at the st	Administrator	Zertifik	Zertifikatsinformationen	
Administratorsignacurzentikat:			Dieses Zertifikat ist für folgende Zwecke beabsichtigt:	
Einzuschreibender Benutzer:			Smartcard-Anneidung	
	Smart, Card@vw.bfw.local	Benuta		
Status:				
Die Smartcard ist fertig. Klicken Sie auf "Zertifi	kat anzeigen", um sicher zu stellen, dass das	s Zertifikat d	Ausgestellt Smart.Card	
				Des des
			Ausgestellt RootCA	per Denutzer
			Gilltig ab 04.11.2009 bis 04.11.2010	
			P Sie besitzen einen privaten Schlüssel für dieses Zert/Fkat.	
			1	
			Ausstellererlöbrung	
				_

Anmeldung an Windows 7

