Zertifikatanforderung von einer internen CA am ISA Server 2004 / 2006

Standardmäßig kommuniziert eine Windows Server 2003 CA mit den Clients via RPC und DCOM.

RPC wird von Windows 2000 Pro und Server verwendet und von Windows XP und Server 2003 unterstützt.

Da eine Firewall wie ISA Server 2004/2006 aber RPC-Datenverkehr blockiert, sind einige Schritte erforderlich (auf CA und ISA-Seite) um Zertifikate anfordern können.

Die bisherigen Aussagen von waren bisher immer, eine „All Open“ Firewallregel zu erstellen, das strikte „RPC Enforcement“ zu deaktivieren und ggfs. temporär den RPC-Filter von ISA Server zu deaktivieren. Harter Tobak ☺, an dem ich mich auch immer gehalten habe, bis ich durch Zufall auf einen Artikel stieß, der das ganze etwas anders beschreibt.

Als erstes muss an der CA das RPC-Interface deaktiviert werden. Das hat nur Auswirkungen auf Windows 2000 Clients die dann kein Enrollment für Zertifikate mehr durchführen können. Alles andere ist unbetroffen.

Deaktivieren des RPC-Interface an der CA

Anmelden als lokaler Administrator an der CA (oder mit entsprechenden Berechtigungen eines Domänenkontos)

CERTUTIL –SETREG CA\interfaceflags +0x8
NET STOP CERTSVC & NET START CERTSVC

Um die Einstellungen wieder rückgängig zu machen führen Sie folgenden Befehl aus:

CERTUTIL –SETREG CA\interfaceflags -0x8

Konfigurieren der DCOM-Einstellungen

Die Windows Server 2003 CA ist primär als DCOM-Applikation implementiert worden. DCOM verwendet High Ports um Client-Anfragen zu beantworten. Nicht gut für Firewalls ☺

Mit Hilfe des COM-Konfigurationstools können Sie DCOM aber zur Verwendung eines festen Ports konfigurieren.

Führen Sie folgende Tätigkeiten durch:

- Start – Ausführen - DCOMCNFG.EXE
- Component Services
- Computers
- DCOM Config
- Certsrv Request
- Properties
- Endpoints Tab
- Add
- Auswählen von „Select Static Endpoint“
- Eingabe einer nicht verwendeten Port-Nummer, zum Beispiel 4711
- NET STOP CERTSVC & NET START CERTSVC

Konfigurieren der ISA-Firewall

Damit die Firewall jetzt Certificate anfordern kann, müssen folgende Ports geöffnet werden:

Protokoll	Portbereich	Protokolltyp	Richtung
HTTP	80	TCP	Ausgehend
DCOM-Port4711	4711	TCP	Ausgehend
Kerberos-Sec (UDP)	88	UDP	Senden/Empfangen
LDAP	389	TCP	Ausgehend
LDAP (UDP)	389	UDP	Senden/Empfangen
RPC (Alle Schnittstellen)	135	TCP	Ausgehend

In der Regel wird noch DNS benötigt, aber das sollte vermutlich sowieso schon erlaubt sein. Wenn nicht, entsprechende Regel für DNS erstellen.