Windows Server 2008 und R2 Terminal Server Publishing mit Zertifikataushandlung

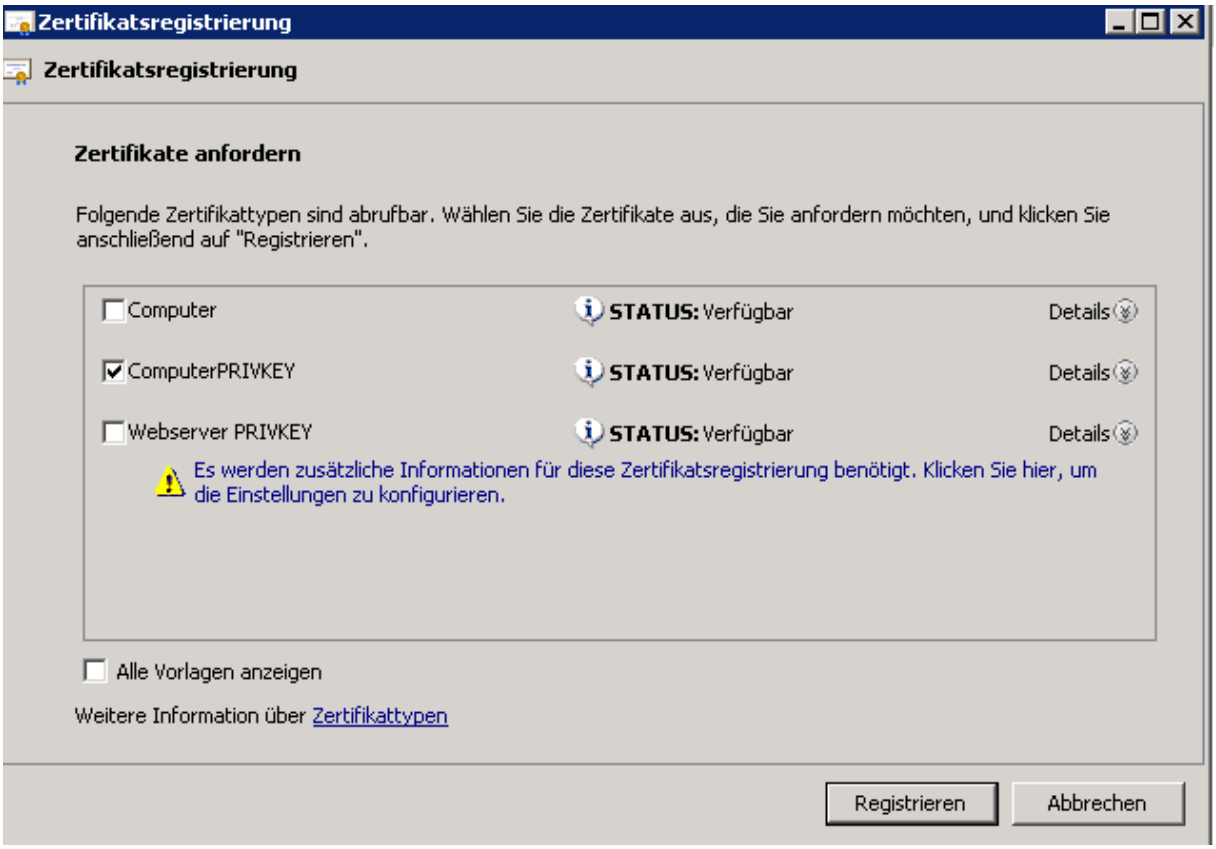
Umgebung:

1 Forest – 3 Domaenen
1 Windows Server 2008 Enterprise PKI in der Root Domain
1 TS 2008 Licensing Server in der Root Domain
1 TS Session Broker 2008 in der Subdomain
2 TS Server 2008 in der Subdomain
2 ISA Server EE mit Publishing fuer TS Gateway

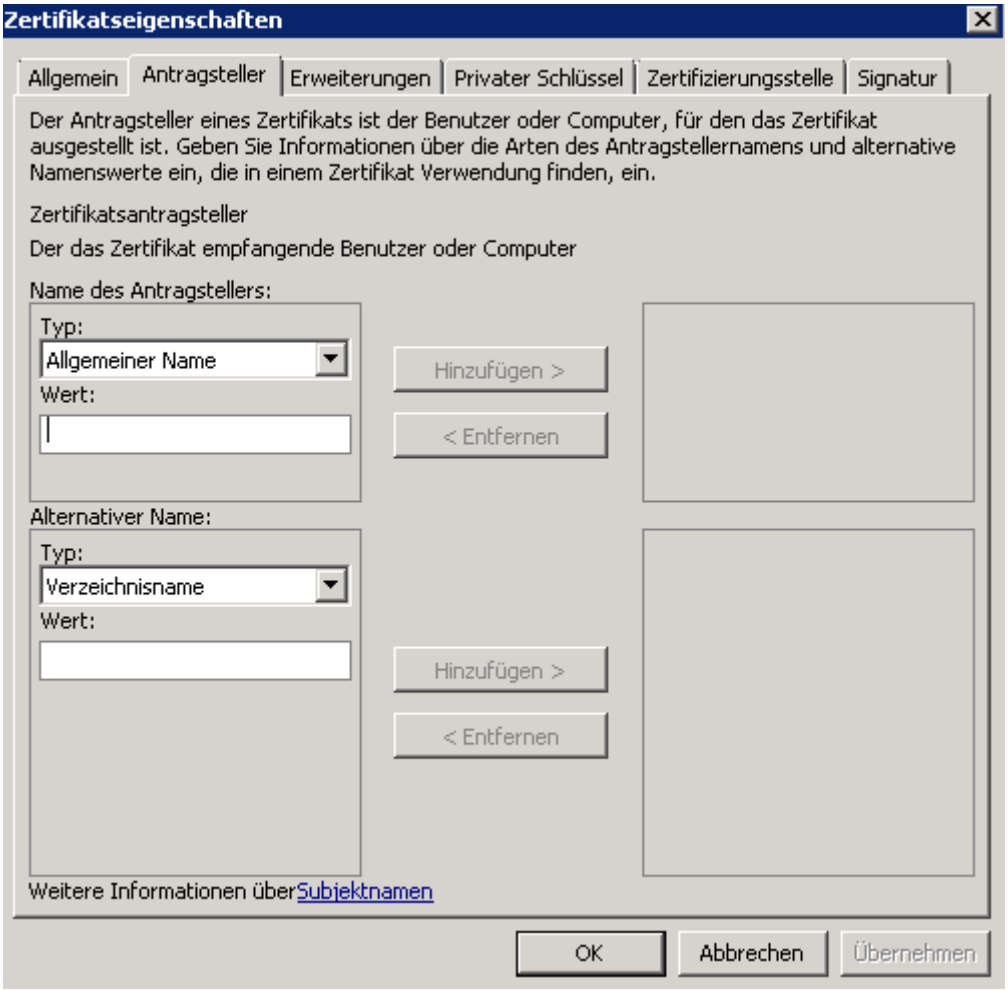
Domaenen- und Nicht Domaenen PC.

Terminal Server-Sicherheit auf Netzwerkebene

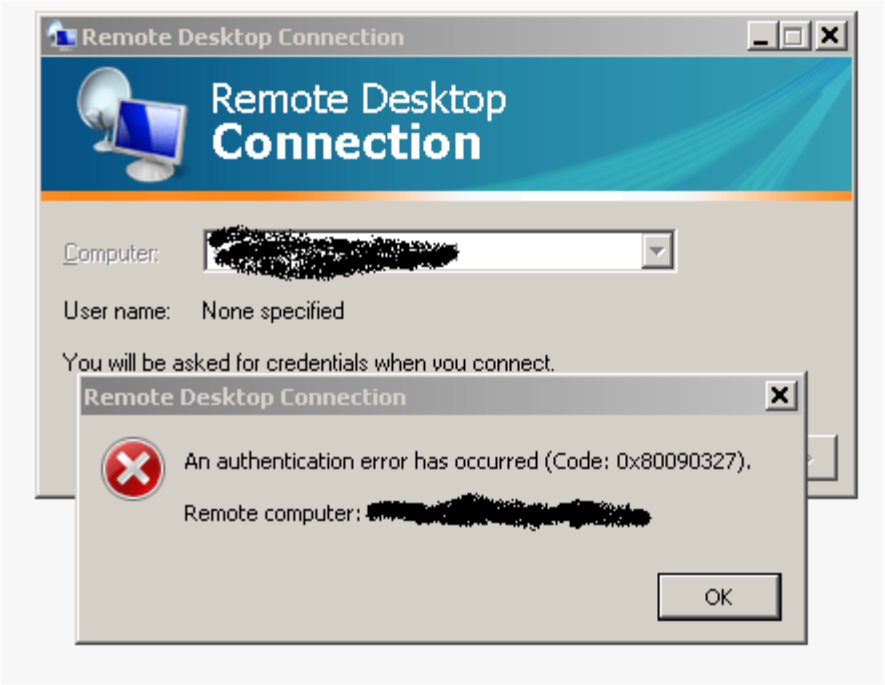
Nachdem ich die zwei Terminal Server mit Session Broker und NLB installiert hatte, habe ich fuer die beiden TS Server ein Zertifikat mit einem Custom V3 Template mit Schluesselarchivierung von der Enterprise eingespielt, um die Authentifizierung auf Netzwerkebene zu ermoeglichen.



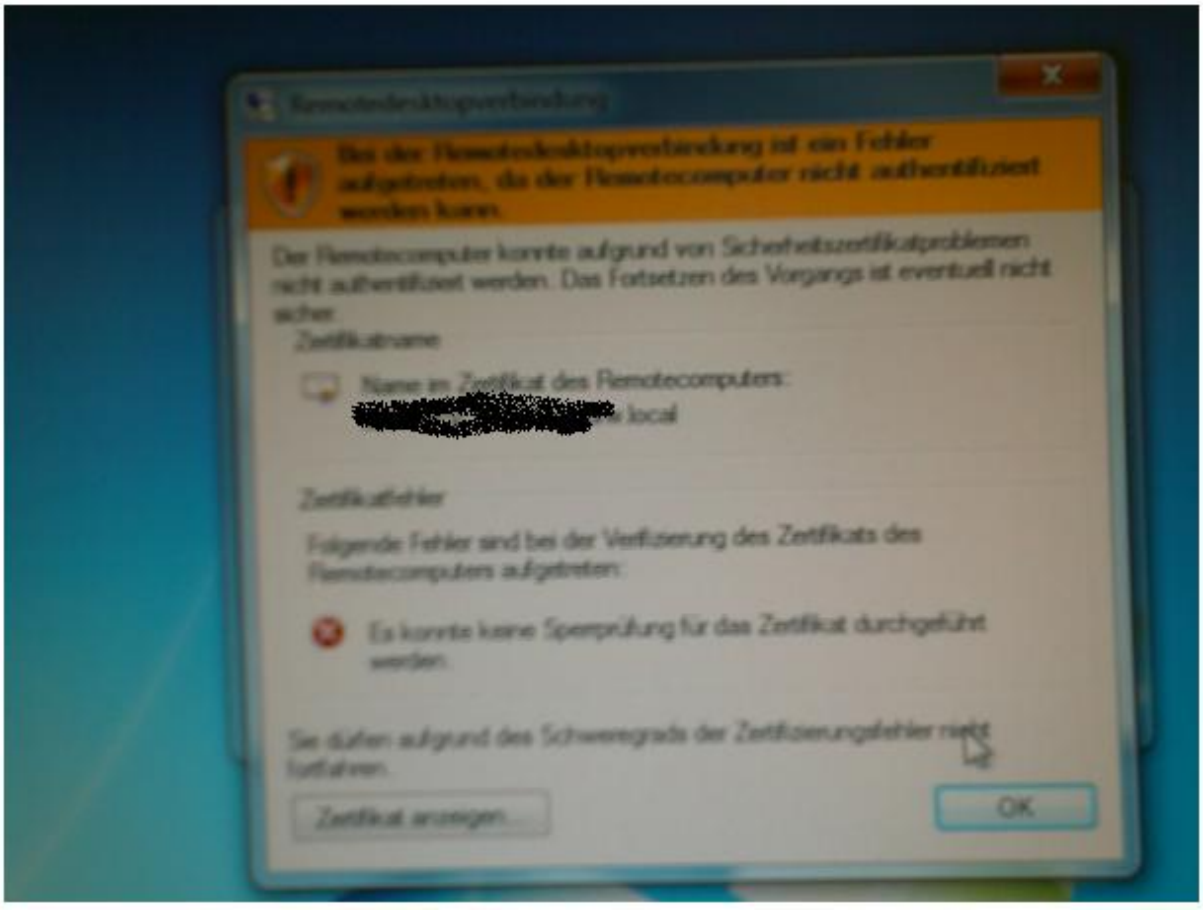
Der Anzeigename und Common Name habe ich auf den FQDN der Server und die VIP sowie den VIP FQDN ausgestellt. Exemplarisch, wo dies einzustellen ist, zeigt der folgende Screenshot:



So, auf Domaenen PCs alles prima. Super Authentifizierung, keine Zertifikat Fehlermeldungen, wenn man den FQDN angibt, welcher auch im CN des Zertifikats ist.
Dann aber habe ich das ganze von meinem Notebook (nicht Domaenen PC des Kunden) probiert und nix ging, eigentlich logisch, aber im ersten Moment Verwirrung meinerseits, welche sich dann nach ein paar Minuten lichtete ☺



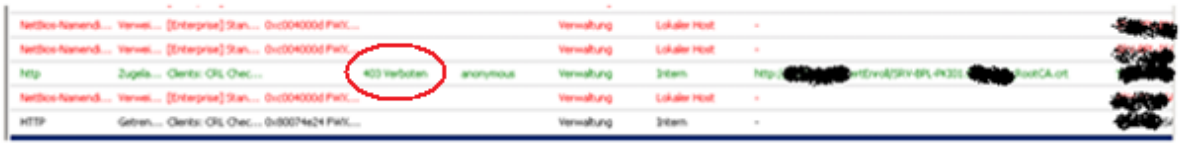
Diese Meldung kam von einem Windows Server 2008; nicht sehr aussagekraeftig, ein Windows 7 Rechner war da schon gespraechiger und sagte, das er die CRL Informationen nicht ermitteln kann!



Recht hat er, sagte mir auch der ISA Server im Logging.

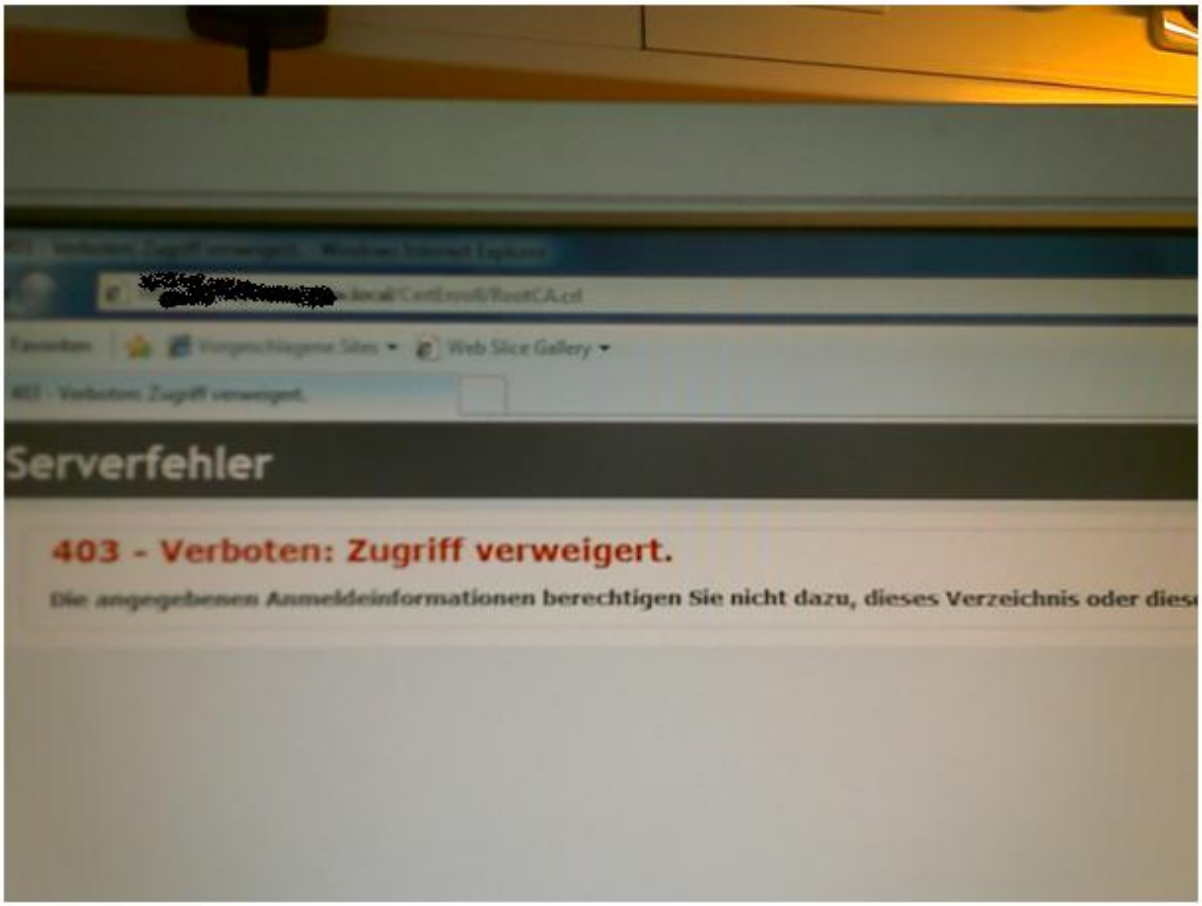
Nachdem ich eine neue Firewallregel erstellt hatte, welche HTTP zum PKI Rechner erlaubte, sah das ISA Log schon sauberer aus.

… siehe folgenden Screenshot

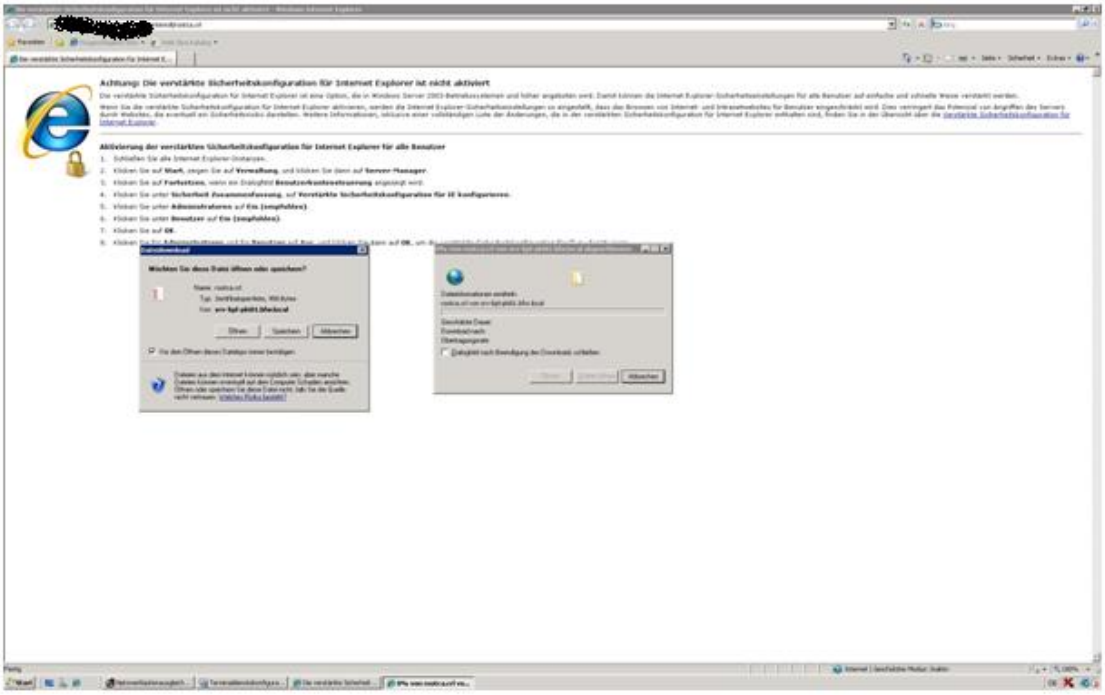


Aber, ein HTTP 403 verboten, also noch eine Sicherheitseinstellung auf dem IIS der PKI.

Kurz noch einen Check, ob der betroffene Client die CRL ueber den IE abfragen kann, fehlgeschlagen:

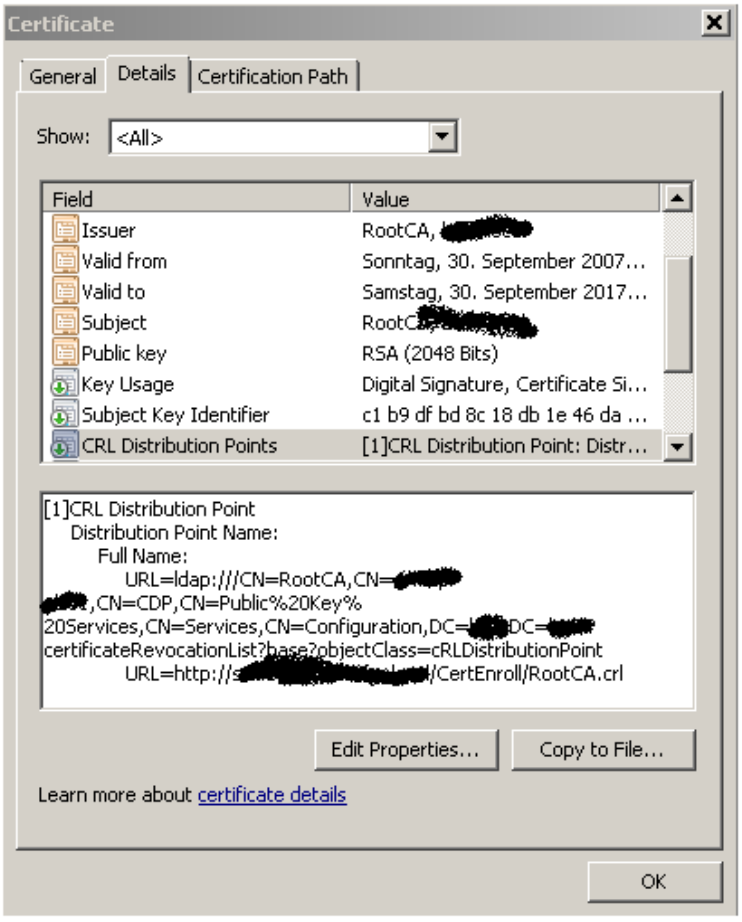


Von einem Domaenen PC laesst sich die CRL abfragen, siehe folgenden Screenshot:

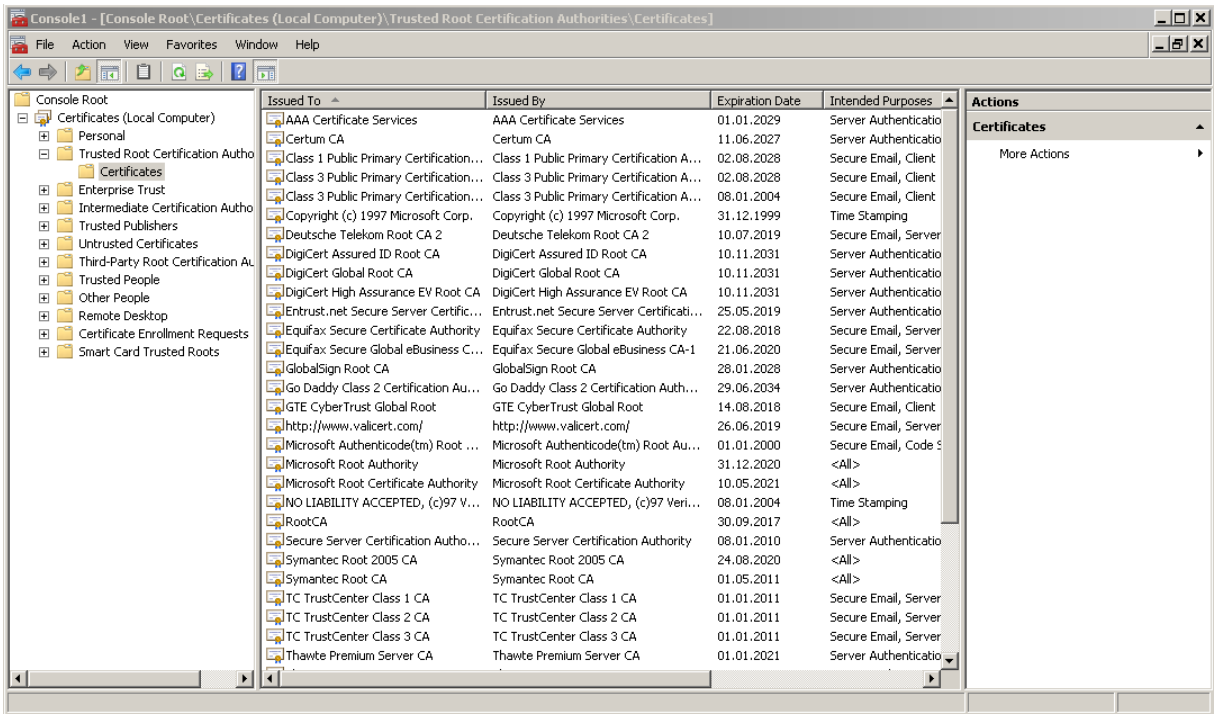


Etwas Hintergrundwissen:

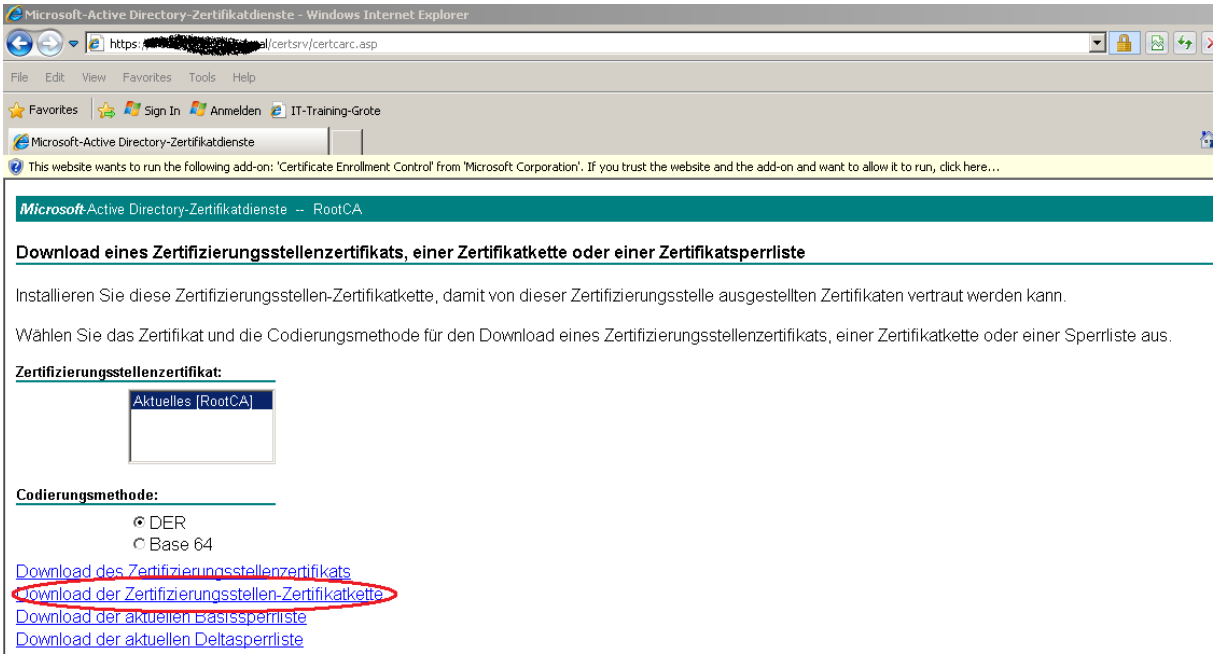
In jedem Zertifikat steht der CRL (Certificate Revocation Point) Veroeffentlichungspunkt, siehe Screenshot:



Der CRL Punkt muss zugelassen sein, damit die Applikation das Zertifikat gegen die ausstellende CA auf Revocation pruefen kann.
Zusaetzlich muss der Client noch das RootCA Zertifikat der ausstellenden CA im Computerspeicher der vertrauenswuerdigen Stammzertifizierungsstellen haben, was bei Domaenen PC und einer Windows Server Unternehmens CA automtisch der Fall ist, siehe folgenden Screenshot:

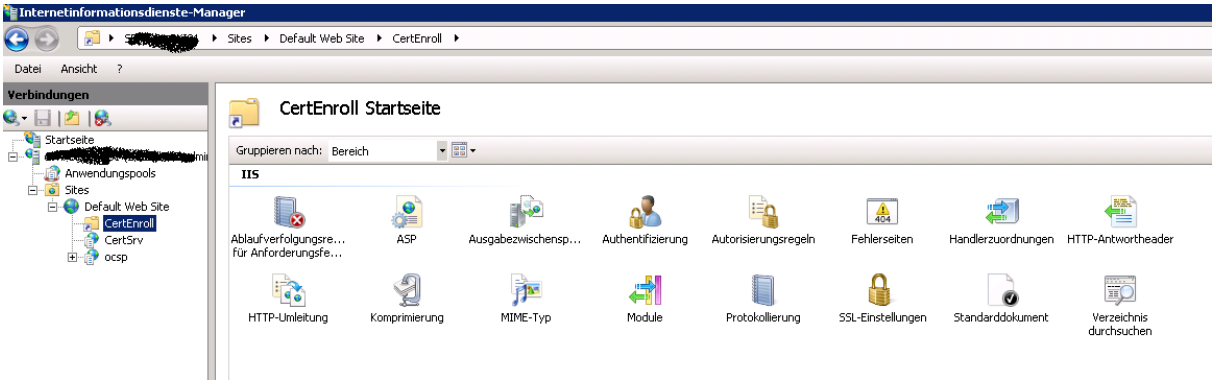


Bei nicht Domaenen PC muss das Root CA Zertifikat manuell importiert werden.



Am IIS

Also am IIS fuer das betroffene Verzeichnis den anonymen Zugriff zulassen (Certenroll).

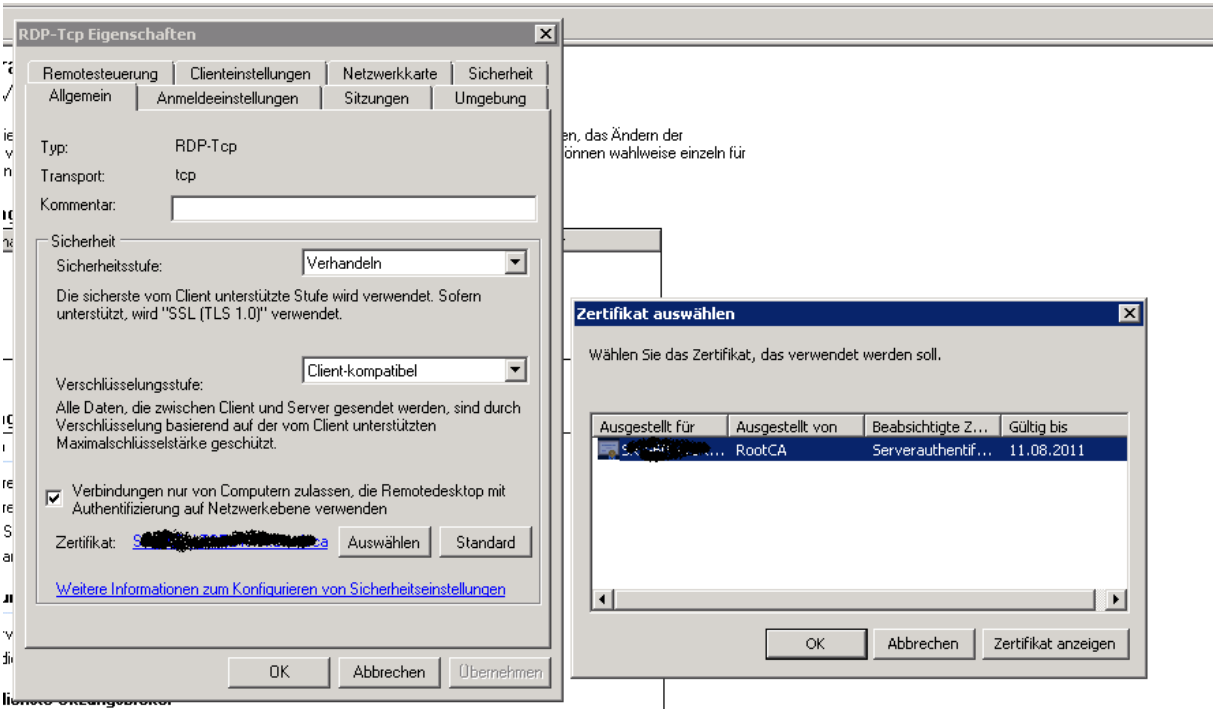


Der Schuldige

„Schuld“ an allem hat die Sicherheitseinstellung …

- Sicherheitsstufe – Verhandeln und
- Authentifizierung auf Netzwerkebene

Dort wird ein Computerzertifikat fuer die Serverauthentifizierung (Mutual Authentication) eingespielt, welches fuer den verbindungsaufbau zwischen Client und Server verwendet wird.



Danach klappte es auch mit dem Nachbarn