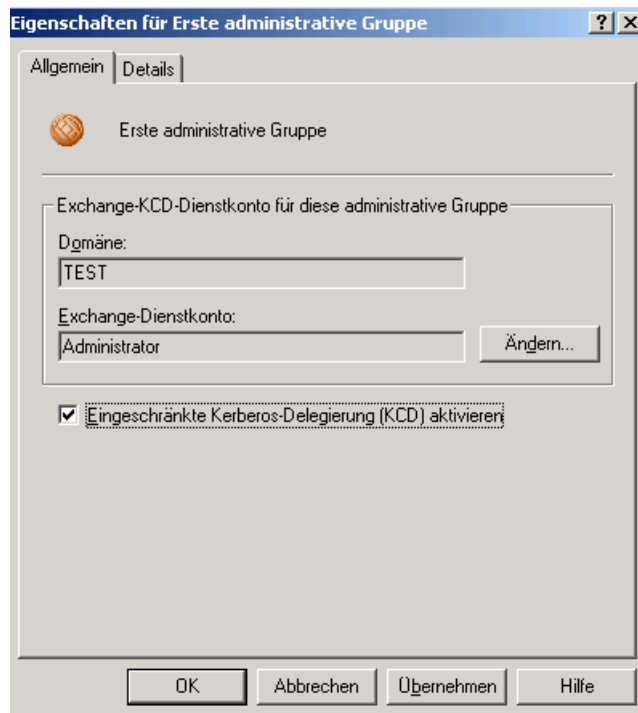


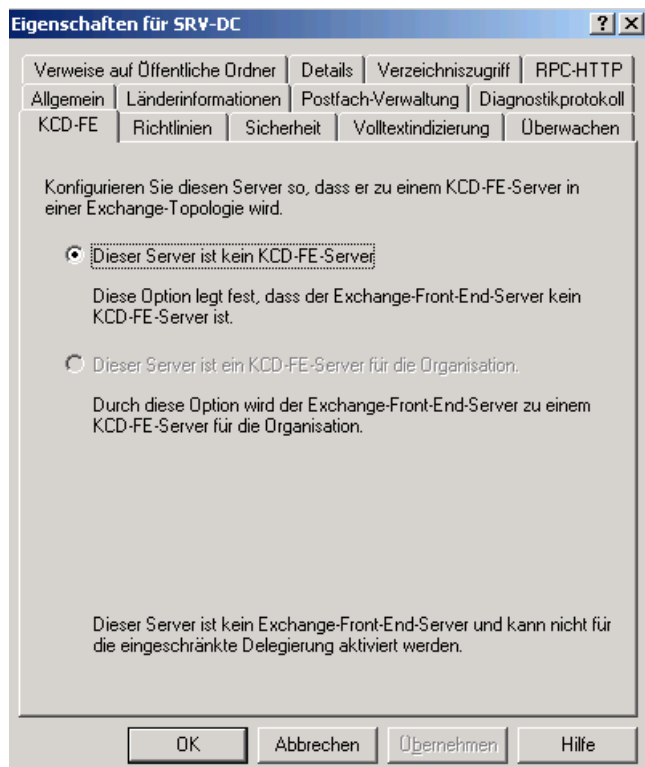
Exchange Server 2003 OWA mit Smartcard Authentifizierung ueber ISA Server 2006

Damit eine Smartcard Authentifizierung moeglich ist, muss als erstes folgendes Update geladen werden: <http://support.microsoft.com/kb/920209>
Dieses Update muss auf dem Exchange Front End Server installiert werden.

Dann muss der Account angegeben werden, welcher fuer die KCD (Kerberos Constrained Delegation) verwendet wird. Es muss sich hierbei nicht um einen Administrator Account handeln.



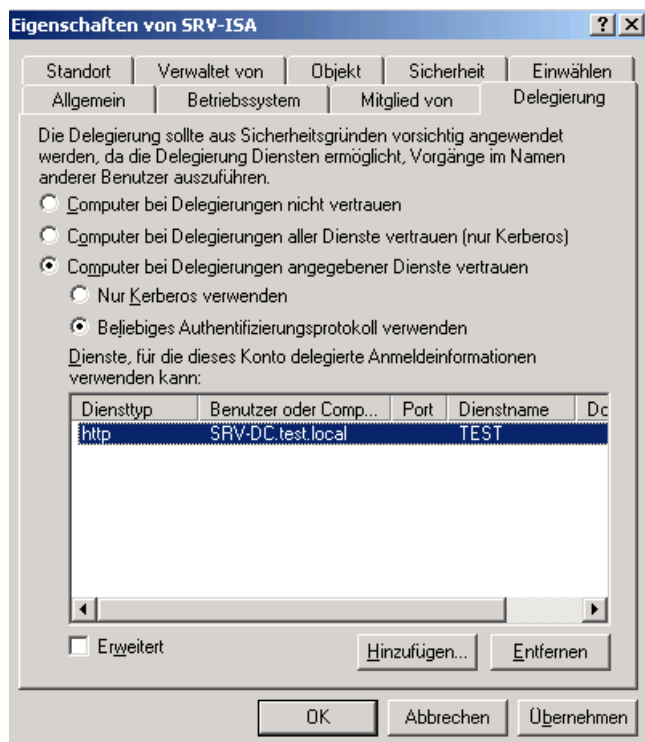
In den Eigenschaften des Front End Servers ist festzulegen ob es sich um einen KCD Frontend Server handelt. Das Feld ist nur auswaehlbar, wenn in der Exchange Organisation ein Exchange Frontend- und Backend-Server existiert.



Auf dem DC

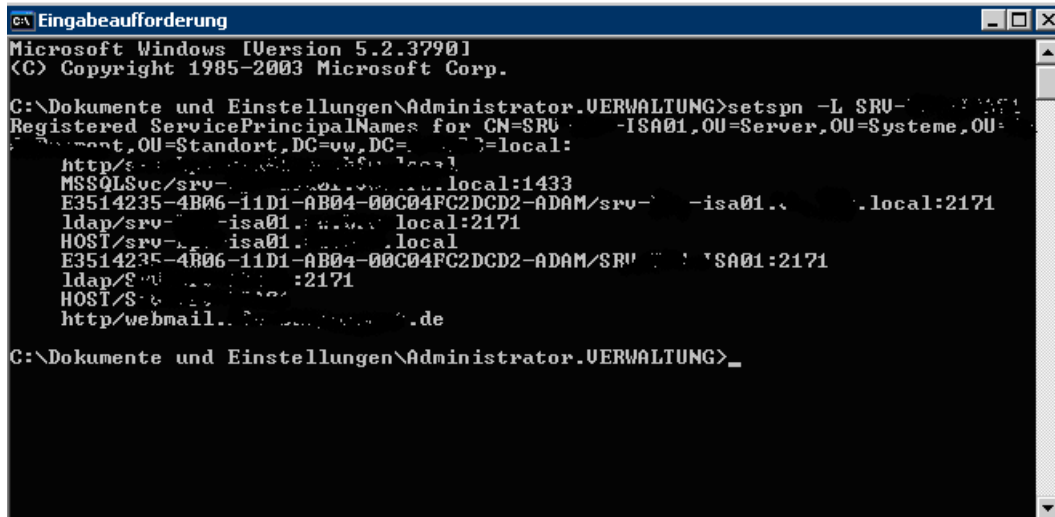
Damit ISA Server stellvertretend fuer den Smartcard Benutzer eine Authentifizierung durchfuehren kann, muss der ISA Server fuer die Kerberos Delegation vertraut sein.

Das geht mit dem Tool Active Directory Benutzer und Computer. Als Authentifizierungsprotokoll HTTP auswahlen.



Auf dem ISA Server

Auf dem ISA Server (bei einem Enterprise Array auf jedem Knoten), muss der SPN registriert werden, welcher fuer den Aufruf von OWA verwendet wird. Der Eintrag wird mit SETSPN -A hinzugefuegt. Anzeige mit SETSPN -L. Das SETSPN Tool findet sich in den Windows Server 2003 Support Tool.



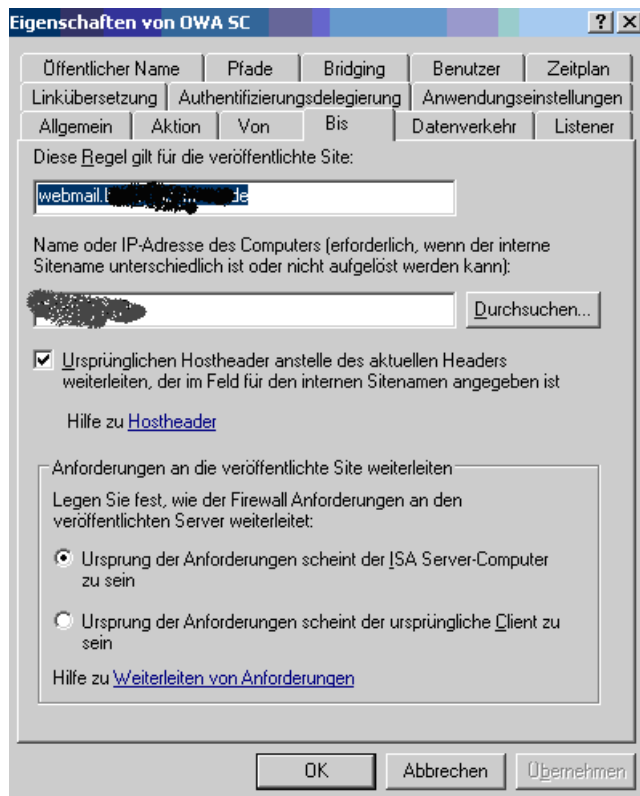
```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Dokumente und Einstellungen\Administrator\UERWALTUNG>setspn -L SRU-...
Registered ServicePrincipalNames for CN=SRU-... -ISA01,OU=Server,OU=Systeme,OU=...
http/srv-... local
MSSQLSvc/srv-... local:1433
E3514235-4B06-11D1-AB04-00C04FC2DCD2-ADAM/srv-... -isa01... local:2171
ldap/srv-... -isa01... local:2171
HOST/srv-... isa01... local
E3514235-4B06-11D1-AB04-00C04FC2DCD2-ADAM/SRU-... ISA01:2171
ldap/srv-... :2171
HOST/S... :2171
http/webmail... de

C:\Dokumente und Einstellungen\Administrator\UERWALTUNG>_
```

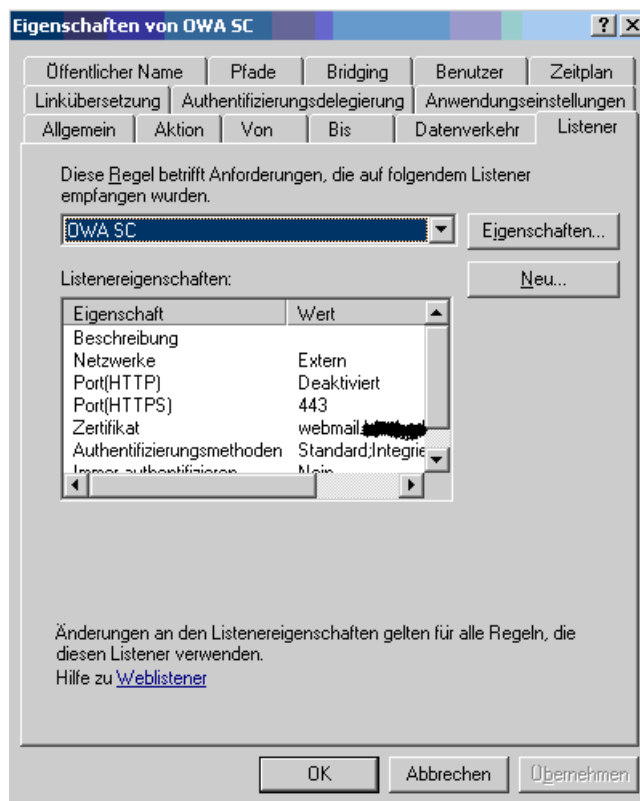
Erstellung der ISA Regel

In der Registerkarte „Bis“ muss der Name des internen Exchange Frontend Servers eingetragen sein. Der Name muss identisch sein mit dem Common Name des Zertifikats auf dem Front End Server (bei mehreren Front End Servern muss jeder Server das Zertifikat besitzen).

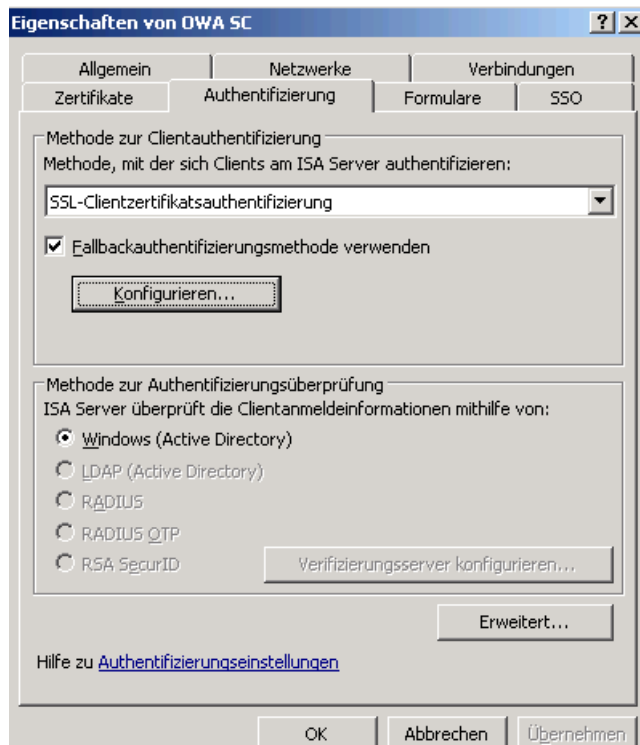


Erstellung des ISA Listeners

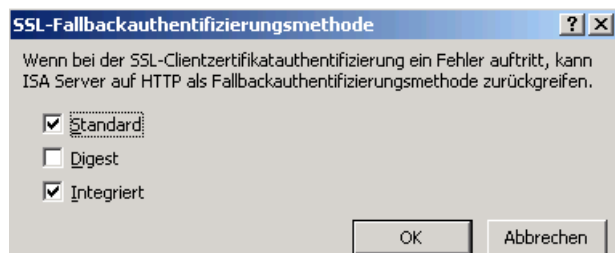
Der ISA Listener verwendet Client SSL Authentifizierung und wenn gewünscht, als Fallback, Integriert, Standard oder Digest (falls nicht alle User sich mit Smartcard authentifizieren muessen).



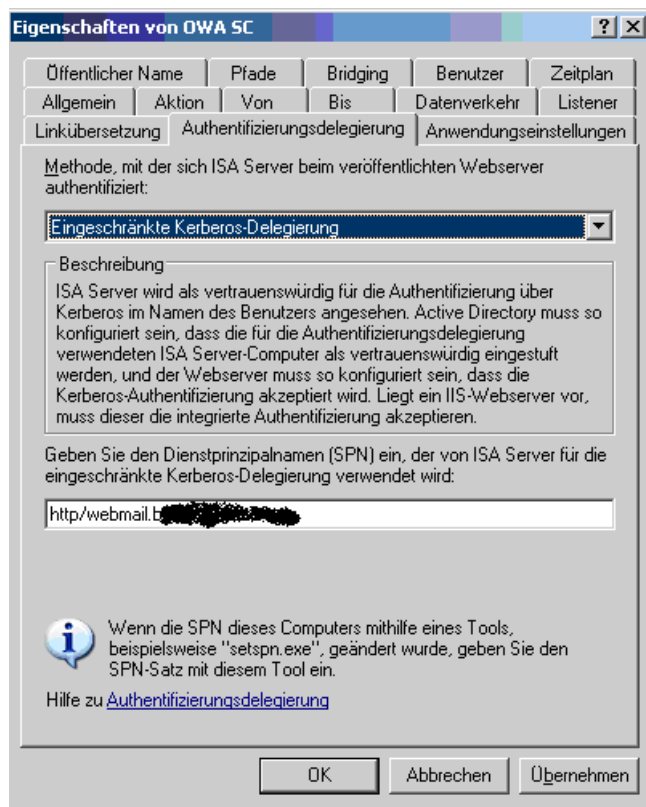
Auswahl der SSL Client Authentifizierung und einer Fallback Methode.



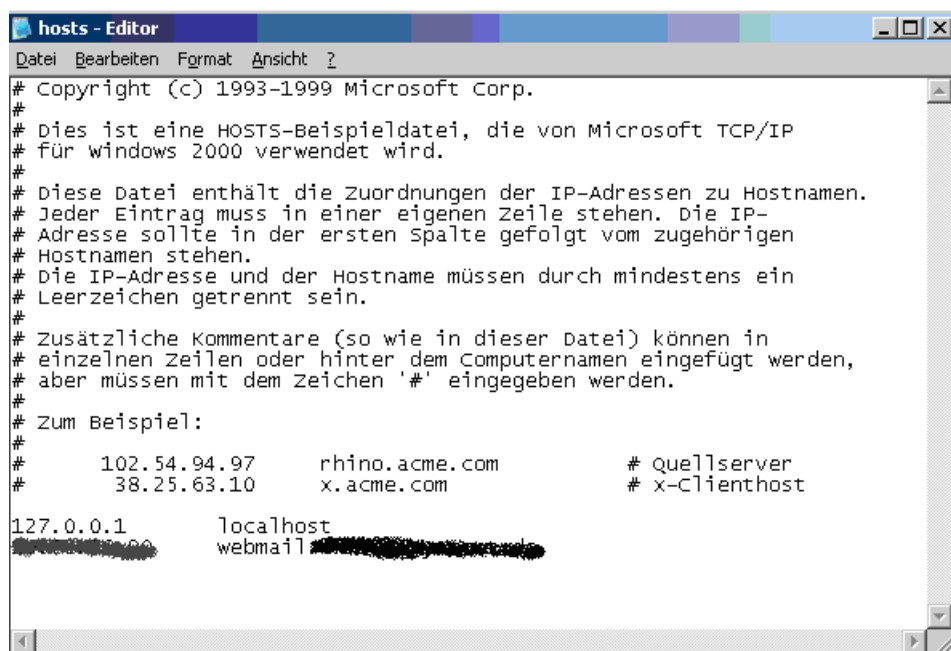
Auswahl der Fallback Methode



Bei der Authentifizierungsdelegation muss mit eingeschränkter Kerberos-Delegation gearbeitet werden. Der SPN lautet HTTP/>>>Name wie er in der OWA Regel in der Registerkarte „Bis“ eingetragen ist <<<

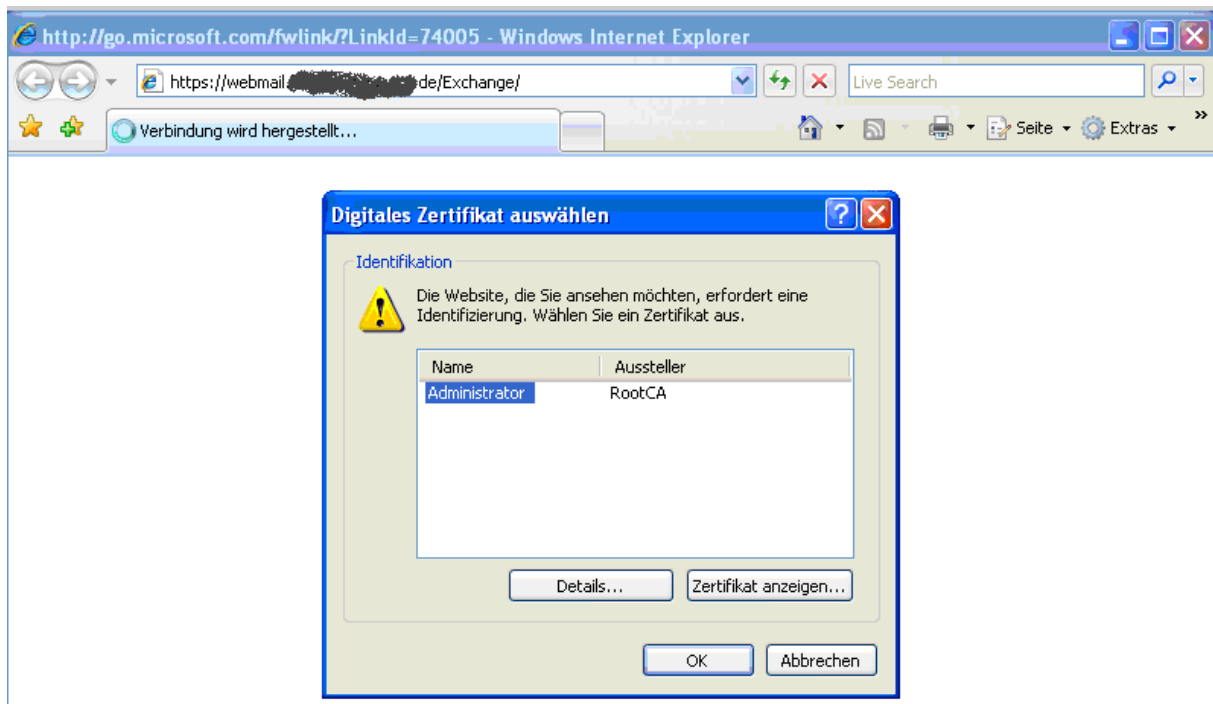


Wenn der interne Name und der öffentliche Name identisch sein soll, muss die HOSTS Datei am ISA gepached werden und der öffentliche Name auf den Exchange 2003 Front End Server zeigen.



Auf der Client Seite

Der Client benötigt ein Benutzerzertifikat oder ein Smartcard Zertifikat damit er sich anmelden kann. Bei dem Aufruf von OWA erscheint dann folgendes Fenster.



Hat der Benutzer kein Zertifikat oder verwendet keine Smartcard kann er einfach ESC druecken und die Fallbackauthentifizierung wird aktiv und fordert dann zur herkoemmlichen Eingabe der Credentials.

