Exchange Active-Sync mit Zertifikatsbasierender Authentifizierung

Autor: Marc Jochems

bei www.faq-o-matic.de

Alternativ zur Verwendung von Benutzername und Passwort Kombination, können auf einigen mobilen Endgeräten auch die zertifikatsbasierende Authentifizierung verwendet werden. Dazu fordert das mobile Endgerät aus einer internen Zertifizierungsstelle (nachfolgend CA genannt) ein Clientzertifikat an, welches zur Authentifizierung verwendet wird. Dieser Artikel ist eine Übersicht, welche Konfigurationen und Einstellungen getroffen werden müssen, damit diese Art der Authentifizierung funktioniert.

Im ersten Schritt erläutere ich kurz die vorhandene Umgebung und führe die Anforderung zur Client-Zertifikats-Authentifizierung an.

Die Umgebung

Ich habe in meiner Testumgebung vier Server und zwei Client Computer installiert. In der folgenden Abbildung 0.1 werden die Funktionen der Server und die Positionen der Clients dargestellt.

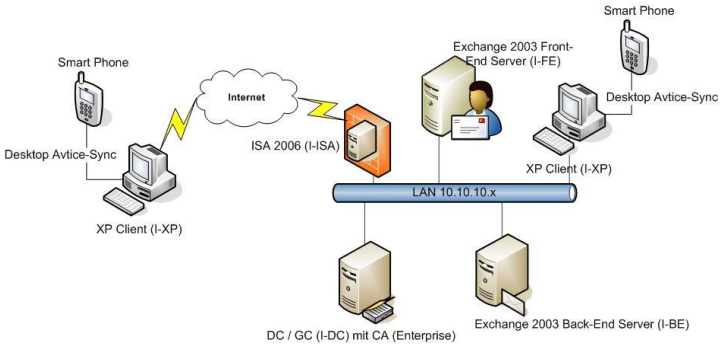

Abbildung 0.1: Testumgebung für EAS Authentifizierung

Als mobile Endgeräte habe ich den Windows Device Emulator mit MSFP (MSFP = Messaging Security und Feature Pack) verwendet.

Die Anforderungen

- Windows Server 2003 Enterprise CA
- mind. Desktop Active-Sync 4.1
- mobiles Endgerät, welches die Client Zertifikatsauthentifizierung unterstützt.
- ISA Server 2006 (Domänenmitglied für die Kerberos Delegierung)
- Exchange Server 2003 SP2
- Zertifikat-Verteilungstools (CertAuthTool.exe)
- Windows 2003 native Mode der Domäne

Hinweis:

Weitere Informationen zu den Anforderungen und eine Anleitung von Microsoft gibt es unter dieser URL: http://www.microsoft.com/technet/solutionaccelerators/mobile/deploy/msfp_a.mspx und auf der Seite MSXFAQ: http://www.msxfaq.net/mobil/eascert.htm .

Vorbereiten der CA

Im ersten Schritt überprüfe ich, ob die interne CA für die Ausstellung von Clientzertifikaten vorbereitet ist und ob das Clientzertifikat den Anforderungen (Verschlüsselungsstärke usw.) entspricht. In den meisten Fällen sollte die Standard Vorlage ausreichend sein und Sie müssen keine Veränderungen vornehmen.

Hinweis:

Bei einer deutschen Installation der CA wird die Standard Vorlage der Benutzer Zertifikate mit dem Namen „**Benutzer**“ geführt. Bei der Konfiguration der XML Datei (weiter unten in diesem Artikel) muss aber für diese Vorlage weiterhin der Name „**user**“ verwendet werden, da dies der Vorlagenname ist. „**Benutzer**“ ist nur ein Anzeigename.

Ein weiterer wichtiger Punkt bei der Vorbereitung der CA ist die Erreichbarkeit der Zertifikatssperrliste. Diese Liste ist dafür verantwortlich,

dass die Information über gesperrte Zertifikate veröffentlicht wird und der Client dieses Zertifikat nicht mehr verwenden darf.

Überprüfen Sie in der CA den Pfad zur Sperrliste und stellen Sie sicher, dass dieser auch von extern (über das Internet) zu erreichen ist. Um heraus zu finden, welchen Pfad ein Zertifikat verwendet, können Sie z.B. das Stammzertifikat öffnen und sich den Pfad anzeigen lassen.

1. Um das Stammzertifikat zu öffnen, gehen Sie auf einem Domänen Computer oder Server in die Zertifikats MMC des lokalen Computers und wechseln in den Ordner der vertrauenswürdigen Stammzertifikate.
2. Öffnen Sie das „**Stammzertifikat**“ mit einem Doppelklick und wechseln Sie auf die Registerkarte „**Details**“.
3. Unter dem Punkt „**Sperrliste-Verteilungspunkt**“ finden Sie die URL, unter der Ihrer CA Sperrliste zu erreichen ist.

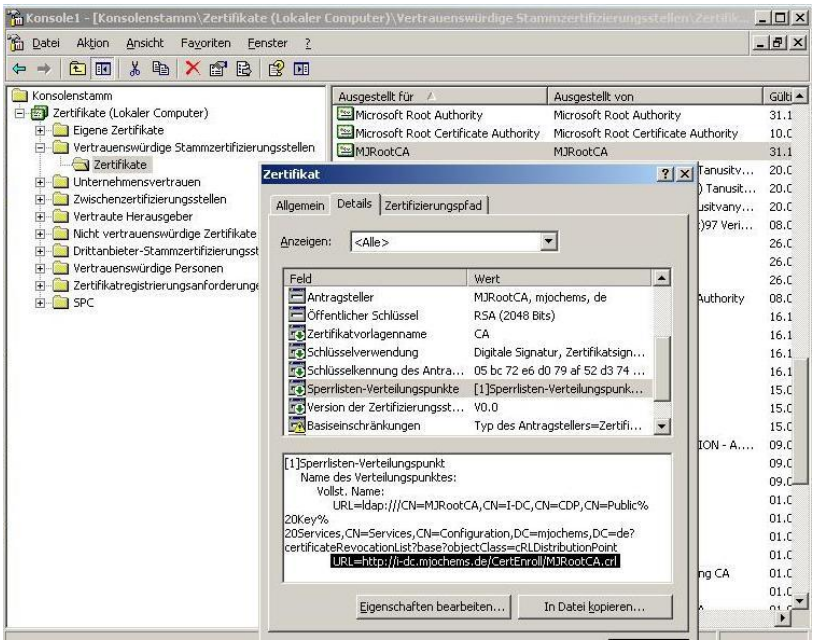

Abbildung 0.2: Sperrlisten Pfad der CA

4. Um zu überprüfen, ob dieser Pfad auch in Ihrer CA eingetragen ist, öffnen Sie die Zertifikats-MMC und wechseln in die Eigenschaften der CA.

5. Wechseln Sie auf die Registerkarte „**Erweiterungen**“ und überprüfen Sie den „**http**“ Pfad. Sollte dieser von der Einstellung im Stammzertifikat abweichen, passen Sie diesen an.

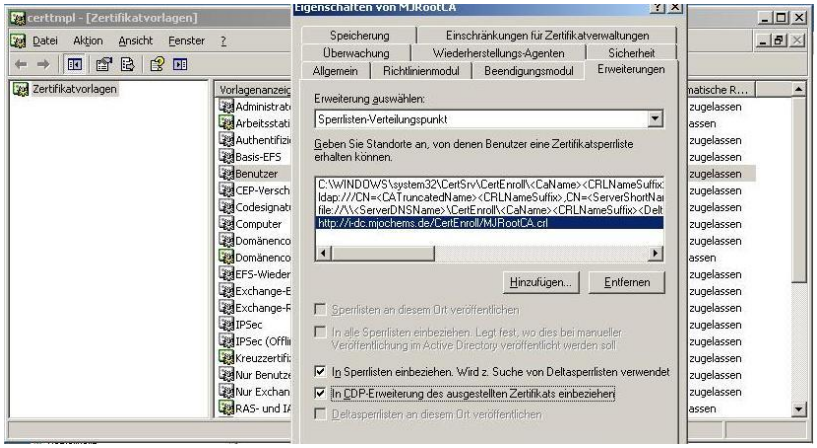

Abbildung 0.3: Angepasster Sperrlisten Pfad

> Hinweis:
>
> Stellen Sie sicher, dass diese URL auch von extern zu erreichen ist, bzw. fügen Sie weitere Pfade hinzu, die ein abrufen der Sperrliste ermöglichen.

Zertifikat Verteilungs Tools (CertAuthTool.exe)

Dieses Tool kann von der Microsoft Website heruntergeladen werden (URL: http://www.microsoft.com/downloads/details.aspx?FamilyID=82510E18-7965-4883-A8C3-F73F1F4733AC&displaylang=en) und ist nur in englischer Sprache verfügbar. Die EXE Datei kann über einen Doppelklick entpackt werden und enthält die folgenden Dateien:

- **Cert_based_Auth.doc** ist eine Anleitung zur Verwendung der Tools und sollte unbedingt gelesen werden.

- **EASAuthUploadXMLtoAD.vbs** ist ein VB-Script zur Verteilung der XML Datei im AD, die für die Zertifikatsverteilung vom Desktop Active-Sync ausgelesen wird.

Hinweis:

Da das Script nur in englisch verfügbar ist, muss noch eine Anpassung vorgenommen werden, damit die richtigen Berechtigungen gesetzt werden. Dazu muss die Datei *EASAuthUploadXMLtoAD.vbs* mit einem Texteditor geöffnet werden und der Wert im Feld „**Const strDomainUser**“ von Englisch auf Deutsch angepasst werden. In meinem Fall von „**Autheticated Users**“ nach „**Authentifizierte Benutzer**“.

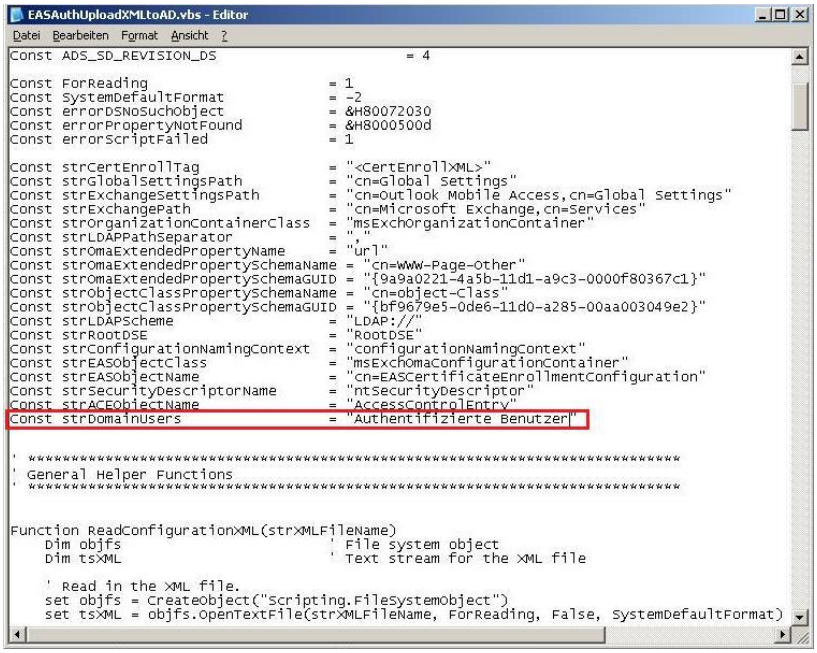

Abbildung 0.4: Authentifizierte Benutzer

Weitere Infos dazu gibt es im MS Artikel KB927471 (URL: http://support.microsoft.com/?kbid=927471)

- **EASCertAuthSampleXML.xml** ist eine Vorlage der XML Datei, die mit dem Script EASAuthUploadXMLtoAD.vbs in das

AD geschrieben wird. Diese Vorlage muss auf Ihre Umgebung abgepasst werden.

- **RapiConfig.exe** ist ein Tool um am Client zu überprüfen, ob die XML Datei aus dem AD gelesen werden kann.
- **QryCertReg.xml** ist die Konfigurationsdatei für das Tool RapiConfig.exe und wird beim aufrufen von RapiConfig.exe mit angegeben. Über die Eingabeaufforderung wird am Client folgender Aufruf durchgeführt: „***RapConfig.exe /P /M QryCerReg.xml***“. Es wird eine Ausgabe XML Datei geschrieben. Weitere Informationen später in diesem Artikel.

Nachdem die CertAuthTools auf dem DC entpackt wurden, passe ich die XML Vorlage „**EASCertAuthSampleXML.xml**“ an. Auf der Abbildung 1.5 ist die XML Datei nach der Anpassung zu sehen.

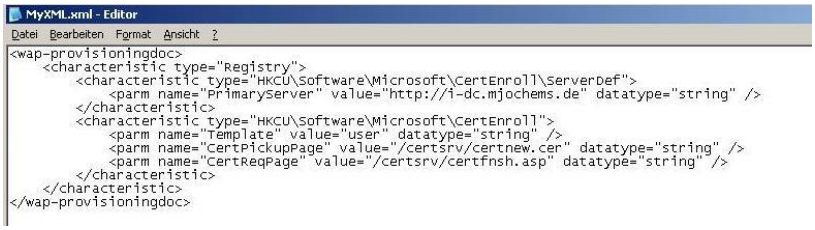

Abbildung 0.5: Angepasste XML Datei

Die Anpassungen ergeben sich aus meiner Umgebung. Da ich nur einen CA Server habe, füge ich auch nur den Namen dieser Server in das Feld „**PrimeryServer**“ ein. Weiterhin habe ich den kompletten Bereich für eine zweite PKI entfernt, da ich diese auch nicht betreibe. Im Feld „**Template**“ behalte ich die Standard Einstellungen bei.

Hinweis:

Weitere Informationen zum Aufbau der XML Datei gibt es im Word Dokument „**Cert_based_Auth.doc**“ aus den CertAuthTools.

1. Nach der Anpassung speichern Sie die Datei als „**MyXML.xml**“ ab. Folgende Schritte werden zum Upload ins AD durchgeführt.
2. Öffnen Sie die Eingabeaufforderung auf dem Server, auf dem die CertAuthTools entpackt wurden.

3. Wechseln Sie in das Verzeichnis in dem die Dateien „**EASAuthUploadXMLtoAD.vbs**“ und „**MyXML.xml**“ abgelegt sind.

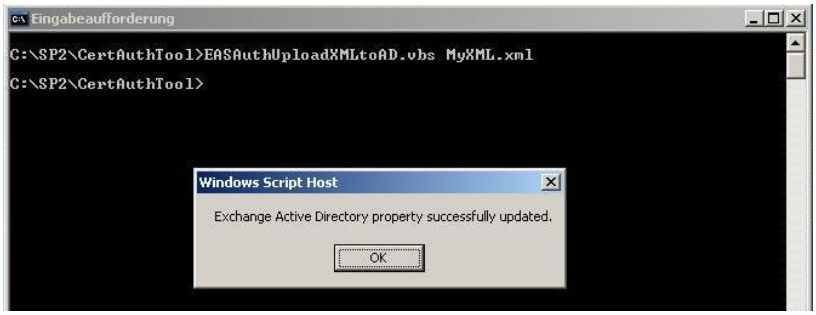

Abbildung 0.6: Upload des XML Files

4. Nach erfolgreichem Upload kann die Meldung „**Exchange Active Directory property successfully updated**“ mit „**OK**“ bestätigt werden.
5. Um zu überprüfen, ob die Informationen auch im Active Directory gelandet sind, kann man mit ADSIEDIT den Pfad zu diesem Wert öffnen.
6. Öffnen Sie dazu **ADSIEDT** (in den Support Tools, auf der Windows Server CD zu finden).
7. Verbinden Sie sich mit dem „**Configuration**“ Ordner.

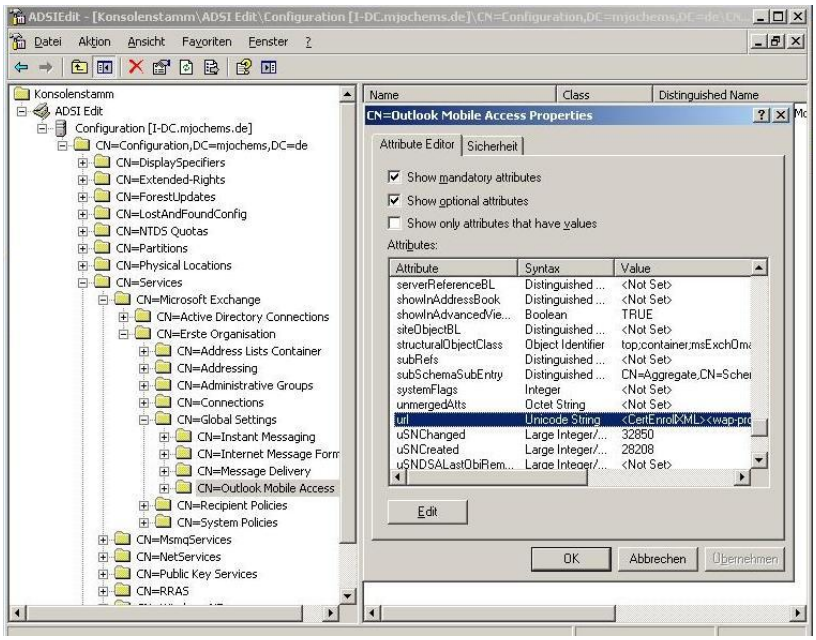

Abbildung 0.7: Überprüfen der XML Datei im AD

8. Öffnen Sie die Eigenschaften von „**Oulook Mobile Access**“ im folgenden Pfad. „**CN=Outlook Mobile Access,CN=Global Settings,CN=<Name der Exchange Organisation>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<DomainName>, DC=de**“

In dem String stehen die Informationen, die Sie vorher in der XML Datei definiert haben. Dieser String wird vom Desktop Active-Sync des Client ausgelesen, um die CA und die Client Zertifikatsvorlage zu finden.

Hinweis:

Diesen Vorgang führt nicht das mobile Endgerät aus, sondern nur Desktop Active-Sync. Daher können Sie das Zertifikat nur mit einer aktiven Verbindung mit Desktop Active-Sync anfordern.

Konfigurieren des Exchange Front-End Servers

Damit der Front-End Server auch die entsprechenden Anforderungen erfüllen kann, müssen die virtuellen Verzeichnisse angepasst werden. Im ersten Schritt sichern wir den Zugriff auf die Standardwebsite via SSL ab. Damit wird verhindert, dass ein Zugriff über die Standard Authentifizierung ohne SSL Verschlüsselung durchgeführt werden kann, da bei der Standard Authentifizierung der Benutzername und das Passwort im Klartext übertragen werden. Dies stellt eine unsichere Übertragung dar.

Schritt 1 Anfordern eines Zertifikates für die Standardwebsite des Front-End Servers (im folgenden FE genannt).

1. Im IIS Manager des FE wechseln wir in die Eigenschaften der Defaultwebsite.
2. Dort auf die Registerkarte „**Verzeichnissicherheit**“ und klicken auf den Button „**Serverzertifikat**“.
3. Folgen Sie dem Assistenten, indem Sie auf „**weiter**“, „**Neues Zertifikat erstellen**“ und „**weiter**“ klicken.
4. Wählen Sie den Punkt „**Anforderung jetzt vorbereiten, aber später senden**“.

Vergeben Sie einen Namen für das Zertifikat. Es empfiehlt sich, einen Namen zu wählen, der mit dem FE in Verbindung gebracht werden kann. In meinem Fall habe ich den FQDN des Servers verwendet.

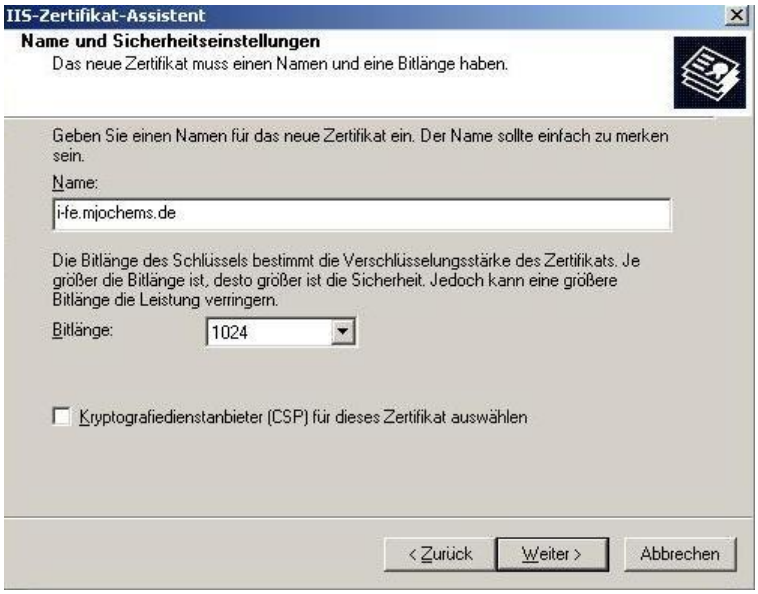

Abbildung 0.8: Zertifikatsname

5. Klicken Sie auf „**weiter**“ und vergeben Sie in den folgenden Fenstern die erforderlichen Informationen.
6. Im Fenster „**Gemeinsamer Name (CN) der Site**“ geben Sie den FQDN des FE Servers an und klicken auf „**weiter**“.
7. Geben Sie die weiteren Informationen ein und klicken auf „**weiter**“.
8. Wählen Sie den Pfad und den Namen aus, unter dem die Anforderung gespeichert werden soll und klicken Sie auf „**weiter**“.
9. Klicken Sie auf „**weiter**“ und auf „**Fertig stellen**“.
10. Es wurde eine Text Datei erstellt, die die Anforderungsinformationen enthält. Öffnen Sie diese Datei und kopieren Sie sich den Inhalt in die Zwischenablage.

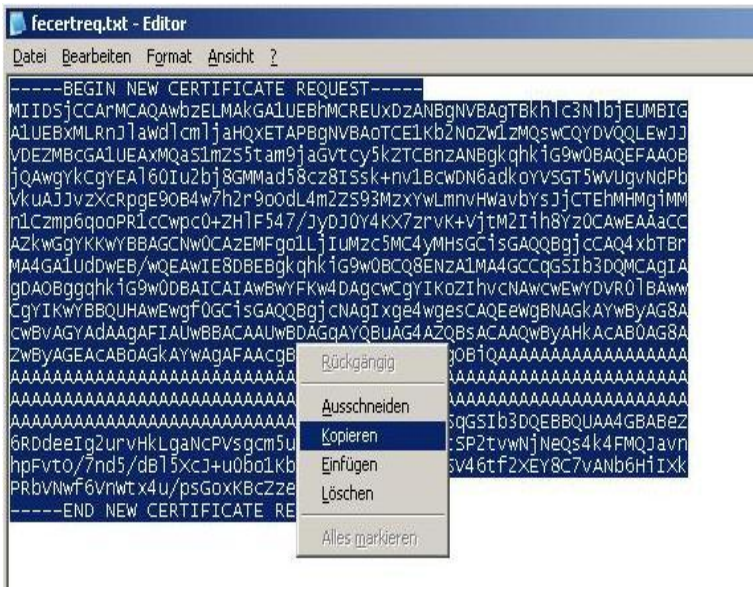

Abbildung 0.9: Kopieren der Anforderung

11. Schließen Sie die Datei wieder und öffnen den „**Internet Explorer**“.
12. Rufen Sie die Seite der CA auf, in meinem Fall ist das der DC (***Bsp.: i-dc.mjochems.de/certsrv***)
13. Sie werden aufgefordert die Anmeldedaten eines Benutzers anzugeben, der berechtigt ist, ein Zertifikat anzufordern. Melden Sie sich mit dem Administrator Account an.
14. Auf der Seite der CA, klicken Sie auf „**Ein Zertifikat anfordern**“ und auf „**erweiterte Zertifikatsanforderung**“.
15. Wählen Sie die zweite Option „**Reichen Sie eine Zertifikats…**“.

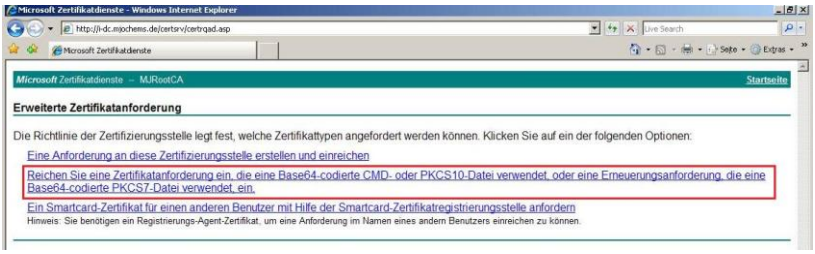

Abbildung 0.10: Anforderung des Zertifikates Einreichen

16. Im Feld „**Gespeicherte Anforderung**“ kopieren Sie den Inhalt aus der Anforderungsdatei von Punkt 10. Die Informationen befinden sich noch in der Zwischenablage.
17. Wählen Sie „**Webserver**“ als Zertifikatsvorlage aus und klicken Sie auf „**Einsenden**“.
18. Das Zertifikat wird ausgestellt und Sie können es über den Punkt „**Download des Zertifikates**“ speichern.
19. Schließen Sie den Internet Explorer und wechseln Sie wieder in den IIS Manager des FE auf die Registerkarte „**Verzeichnissicherheit“ der Standardwebsite**“.
20. Klicken Sie dort erneut auf „**Serverzertifikat**“ und „**weiter**“.
21. Wählen Sie den Punkt „**Ausstehende Anforderung verarbeiten und Zertifikat installieren**“.
22. Klicken Sie auf „**weiter**“ und wählen Sie die Datei aus, die Sie soeben von der Website heruntergeladen haben.
23. Klicken Sie zweimal auf „**weiter**“ und auf „**Fertig stellen**“.

Sie haben jetzt ein Zertifikat auf die Standardwebsite hinzugefügt und eine Verbindung über HTTPS (Port 443) ist nun auf die Exchange Verzeichnisse möglich.

Hinweis:

Sollten Sie ein SAN (SAN=Subject Alternative Name) Zertifikat verwenden wollen, mit dem Sie mehr als nur einen CN Namen angeben können (z.B. i-fe.mjochems.de, mail.mjochems.de und autodiscover.mjochems.de), dann müssen Sie die CA vorher dafür konfigurieren. Wie dies konfiguriert wird und wie Sie dann einen SAN Namen hinzufügen, finden Sie im MS Artikel KB931351 unter der URL: http://support.microsoft.com/kb/931351/en-us

Schritt 2 Authentifizierungseinstellungen auf den virtuellen Verzeichnissen.

Damit auf das virtuelle Verzeichnis „**Microsoft-Server-ActiveSync**“ nur noch via Clientzertifikat zugegriffen werden kann, müssen weitere Einstellungen auf diesem Verzeichnis vorgenommen werden.

1. Öffnen Sie den IIS Manager und erweitern Sie die Standardwebsite. Öffnen Sie die Eigenschaften des virtuellen Verzeichnisses „**Microsoft-Server-ActiveSync**“ und wechseln Sie auf die Registerkarte „**Verzeichnissicherheit**“.
2. Klicken Sie unter „**Sicher Kommunikation**“ auf „**Bearbeiten**“ und aktivieren Sie die Haken bei „**Sicheren Kanal voraussetzten (SSL)**“ und „**128-Bit Verschlüsselung erforderlich**“.
3. Erst dann können Sie den Punkt „**Clientzertifikat voraussetzten**“ anwählen.
4. Setzten Sie den Haken bei „**Zuordnung von Clientzertifikaten aktivieren**“ und klicken Sie auf „**Bearbeiten**“.

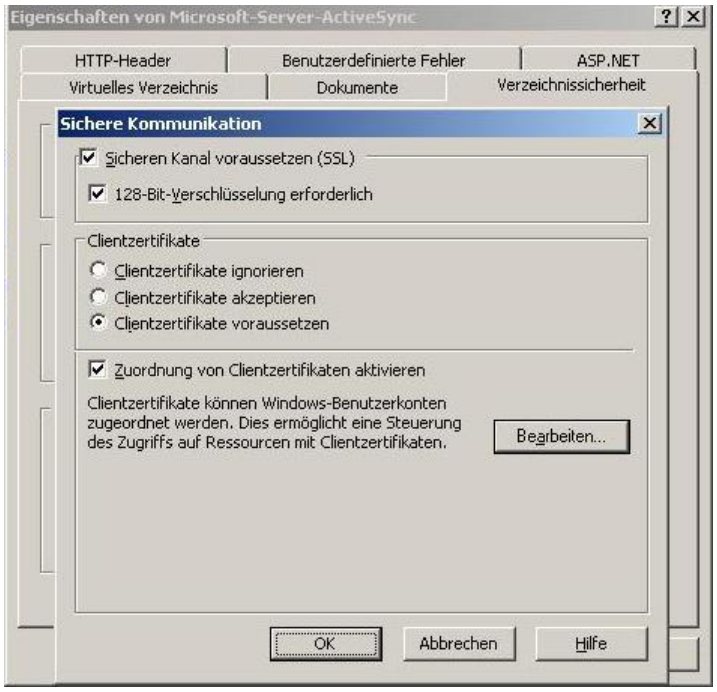

Abbildung 0.11: EAS virtuelles Verzeichnis

5. Im Fenster „**Kontozuordnung**“ müssen Sie keine Einstellungen treffen. Das öffnen dieser Fenster setzt nur die richtigen Konfigurationseinstellungen für das virtuelle Verzeichnis. Klicken Sie auf „**OK**“ und nochmal auf „**OK**“.

6. Klicken Sie auf „**OK**“ um die Eigenschaften des virtuellen Verzeichnisses zu schließen.

7. Öffnen Sie nun im IIS Manager die Eigenschaften des Ordners „**Websites**“ und wechseln auf die Registerkarte „**Verzeichnissicherheit**“.

8. Dort setzen Sie den Haken bei „**Windows-Verzeichnisdienstzuordnung aktivieren**“ unter „**Sichere Kommunikation**“.

9. Klicken Sie auf „**OK**“ und im Fenster „**Vererbungsüberschreibung**“ auch auf „**OK**“.

10. Um weitere virtuelle Verzeichnisse von Exchange vor dem Zugriff ohne SSL zu schützen, können Sie den Punkt „**Sicheren Kanal**

voraussetzten (SSL)“ und „**128-Bit-Verschlüsselung erforderlich**“ für die weiteren Exchange Verzeichnisse aktivieren.

- ExAdmin
- Exchange
- ExchWeb
- OMA
- Public

Hinweis:

Das setzen der oben genannten Haken „**Sicheren Kanal voraussetzten (SSL)**“ und „**128-Bit-Verschlüsselung erforderlich**“, erzwingt eine SSL Verbindung zu diesen Verzeichnissen. Ein Zugriff auf die Verzeichnisse via *HTTP* ist nicht mehr möglich und Sie bekommen bei dem Versuch, eine Fehlermeldung, dass diese Seiten nur noch via *HTTPS* zu erreichen sind.

Schritt 3 Setzen des SPN Namens

Damit die Keberos Delegierung auch auf den entsprechenden Server zugreifen kann, muss für den http Dienst noch der entsprechende SPN gesetzt werden.

1. Öffnen Sie dazu wieder „**ADSIEDIT**“ und verbinden sich diesmal mit der Domain Partition.
2. Suchen Sie das „**Front-End**“ Serverobjekt und öffnen Sie die Eigenschaften des Objektes.
3. Suchen Sie das Attribut „**servicePrincipalName**“ und klicken Sie auf „**Edit**“.
4. Fügen Sie folgende SPNs hinzu:

- *http/<Servernem> (Bsp.: http/i-fe)*
- *http/<FQDN> (Bsp.: http/i-fe.mjochems.de)*

Sollten Sie noch weitere Namen für den FE Server vergeben haben, dann geben Sie auch diese hier an. Weitere Informationen dazu finden Sie im Word Dokument „**Cert_based_Auth.doc**“.

Schritt 4 Setzen der Kerberos Delegierung

Damit die Authentifizierung auch durchgeführt werden kann, besteht ab ISA Server 2006 die Möglichkeit, einer Kerberos Authentifizierung am ISA Server. Dabei muss dann nicht mehr die Anforderung des Clients bis zum Front-End Server durchgereicht werden, sondern der ISA Server übernimmt diese Aufgabe. Damit der ISA Server aber prüfen kann, ob die Anfrage des Clients auch authentifiziert werden kann, muss eine sogenannte Delegierung stattfinden. Dazu befragt der ISA Server den FE und der FE befragt den BE (Back-End) Server. Um diese Delegierung einzurichten, müssen Sie die MMS „**Active Directory-Benutzer und –Computer**“ auf einem Exchange Server oder einem Computer der die Exchange Verwaltungstools sowie das Adminpack installiert haben, verwenden.

Hinweis:

Der ISA Server muss Mitglied der Domäne sein, da Sie sonst keine Delegierung auf das Computerobjekt des ISA Servers im AD vornehmen können.

1. Öffnen Sie ADBuC und gehen Sie in die Eigenschaften des ISA Server Objektes.
2. Wechseln Sie auf die Registerkarte „**Delegierung**“ und wählen Sie „**Computer bei Delegierung angegebener Dienst vertrauen**“. Sowie „**Beliebiges Authentifizierungsprotokoll verwenden**“.
3. Klicken Sie auf „**Hinzufügen**“ und auf „**Benutzer und Computer**“.
4. Geben Sie den Hostnamen des FE Servers an und klicken Sie auf „**OK**“. Wählen Sie die Dienste „**http**“ und „**w3svc**“ aus und klicken auf „**OK**“.
5. Klicken Sie auf „**OK**“ um die Einstellungen zu übernehmen.
6. Wiederholen Sie diese Schritte mit dem Computerobjekt des FE Servers, aber geben Sie den Hostnamen des BE Servers an.

Verbindung mit Desktop Active-Sync herstellen

Nun sind alle Vorkehrungen getroffen, um an den Client zu gehen und ein Clientzertifikat über das Desktop Active-Sync anzufordern. Verbinden Sie dazu Ihr mobiles Endgerät via Desktop Active-Sync mit dem Client Computer.

Hinweis:

Es darf vorher keine Serververbindung auf mobilem Endgerät und dem Desktop Active-Sync bestanden haben. Sollte dies der Fall sein, löschen Sie diese Verbindung vorher. Ansonsten fordert Active-Sync kein Clientzertifikat an.

Hinweis:

Stellen Sie sicher, dass das mobile Endgerät über das Stammzertifikat Ihrer CA verfügt, da ansonsten keine Verifizierung der Zertifikate stattfinden kann. Wie Sie das Stammzertifikat auf das mobile Endgerät kopieren, finden Sie hier: URL: http://www.microsoft.com/technet/solutionaccelerators/mobile/deploy/msfp_d.mspx. Sie können diesen Vorgang auch manuell ausführen, indem Sie das Stammzertifikat von Ihrem PC exportieren und über eine Speicherkarte oder eine Kabelverbindung auf das mobile Endgerät kopieren. Über einen Doppelklick importieren Sie das Stammzertifikat dann auf dem mobilen Endgerät.

Nach dem verbinden des mobilen Endgerätes, wird Active-Sync eine Verbindung aufbauen und automatisch die Konfigurationsoberfläche starten. Geben Sie dort die erforderlichen Informationen ein und klicken sie auf „**OK**“.

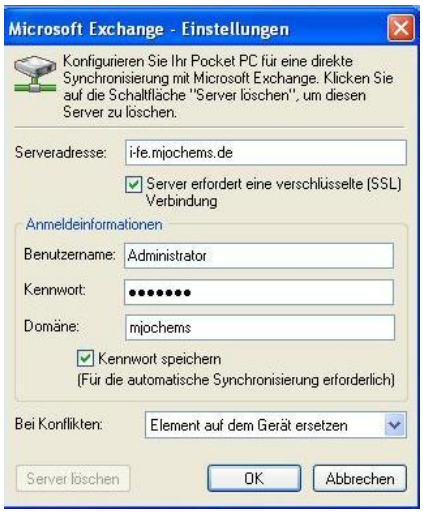

Abbildung 0.12: Serververbindung im Desktop Active-Sync

Der Desktop Active-Sync verbindet sich mit dem Exchange Server und wird angewiesen ein Clientzertifikat zu verwenden. Daraufhin liest Active-Sync die AD Informationen zur CA aus und fordert ein Client Zertifikat an.

Abbildung 0.13: Ausrollen des Clientzertifikates

Nachdem das Zertifikat auf das mobile Endgerät kopiert wurde, verbindet Desktop Active-Sync sich erneut mit dem Exchange Server und synchronisiert die Postfacheinstellungen.

Abbildung 0.14: Sync mit Clientzertifikat

Sie können sich auf dem mobilen Endgerät das Clientzertifikat anzeigen lassen und im Desktop Active-Sync die Einstellungen kontrollieren. Dort wird kein Benutzername und Passwort mehr benötigt, da die Authentifizierung über das Clientzertifikat durchgeführt wird.

Abbildung 0.15: Einstellungen am mobilen Endgerät

ISA Veröffentlichung mit Kerberos Delegierung

Damit der Zugriff auch von extern funktioniert, muss der Exchange FE Server über den ISA 2006 Server freigegeben werden. Dies erreichen Sie über eine Veröffentlichungsregel. Dabei wird die Authentifizierung auf Kerberos festgelegt und vom ISA Server delegiert.

Erstellen Sie auf dem ISA Server einen Listener mit folgenden Einstellungen:

1. Vergeben Sie einen aussagekräftigen Namen für den Listener.
2. Wählen Sie im Fenster „**Sicherheit der Clientverbindung**“ den Punkt „**Sichere SLL-Verbindung am Client erforderlich**“ und klicken Sie auf „**weiter**“.
3. Wählen Sie das „**Externe**“ Netzwerk aus und klicken Sie auf „**weiter**“.
4. Wählen Sie das erforderliche Zertifikat aus.

Hinweis:

Sie können entweder das Zertifikat des FE Servers mit dem privaten Schlüssel exportieren und hier verwenden oder ein eigenes Zertifikat verwenden, sollte der externe Name der Exchange URL nicht dem internen Namen entsprechen.

5. Wählen Sie im nächsten Fenster „**SSL-Clientzertifikatsauthentifizierung**“ um ausschließlich diese Authentifizierung zu verwenden. Klicken Sie auf „**weiter**“.
6. Klicken Sie auf „**weiter**“ und „**Fertig stellen**“.

Nun haben Sie einen Weblistener erstellt, der nur für die Clientzertifikatsauthentifizierung konfiguriert ist.

Erstellen Sie nun eine Veröffentlichungsregel um Exchange Active-Sync zu erlauben.

1. Wählen Sie dazu im ISA Server den Aufgabenpunkt „**Exchange-Webclientzugriff veröffentlichen**“ und vergeben einen aussagekräftigen Namen.
2. Wählen Sie „**Exchange ActiveSync**“ und klicken Sie auf „**weiter**“.
3. Wählen Sie „**Einzelne Website oder Lastenausgleich veröffentlichen**“ und klicken auf „**weiter**“.
4. Wählen Sie im Fenster „**Sicherheit der Clientverbindung**“ den Punkt „**Sichere SLL-Verbindung am Client erforderlich**“ und klicken Sie auf „**weiter**“.

5. Geben Sie den internen Hostnamen des FE Server an (FQDN) und klicken Sie auf „**weiter**“.
6. Geben Sie den öffentlichen Namen der Website an. Sollte dieser vom internen Namen abweichen, so geben Sie diesen an. (Bsp.: interner Name: *i-fe.mjochems.de* / öffentlicher Name: *mail.mjochems.de*) und klicken Sie auf „**weiter**“.
7. Wählen Sie den Weblistener aus, den Sie vorher erstellt haben und klicken Sie auf „**weiter**“.
8. Wählen Sie im Fenster „**Authentifizierungsdelegierung**“ den Wert „**Eingeschränkte Kerberos-Delegierung**“ und geben den SPN Namen des FE Server an.
9. Wählen Sie die Benutzergruppe aus, die über diese Regel zugreifen darf und klicken Sie auf „**weiter**“.
10. Klicken Sie auf „**weiter**“ und auf „**Fertig stellen**“. In der angezeigten Meldung klicken Sie auf „**OK**“. Den SPN haben Sie in einem vorherigen Schritt bereits konfiguriert (*siehe Schritt 3*).
11. Übernehmen Sie die ISA Regel und testen Sie den Zugriff des mobilen Endgerätes von extern.

Hinweis:

Diese Konfiguration des ISA ist nur eine sehr oberflächliche Einstellung. Sie sollten in Ihrer produktiven Umgebung weit aus stärkere Einschränkungen in der Veröffentlichungsregel festlegen.

Fehlersuche

Sollten Sie nicht in der Lage sein, das Zertifikat erfolgreich auf das mobile Endgerät zu transportieren, überprüfen Sie folgende Punkte.

- Kann das mobile Endgerät über den Browser auf das Verzeichnis *https:// FQDN des FE/Microsoft-Server-ActiveSync* zugreifen.
- Überprüfen Sie die Zertifikatsanforderung in Ihrer CA
- Überprüfen Sie die Einträge des Client Computers im IIS Log der CA
- Kann der Client Computer auf die URL *https:// FQDN des FE>/Microsoft-Server-ActiveSync* zugreifen.
- Kann der Client Computer die Einstellungen für die CA im AD abrufen. Verwenden Sie dazu das Tool „**RapiConfig.exe**“ und die „**QryCertReg.xml**“. Anweisungen zur Nutzung finden Sie im Word Dokument „**Cert_based_Auth.doc**“.