Owner of the content within this article is www.isaserver.org
Written by Marc Grote – www.it-training-grote.de

How to publish Microsoft Exchange Active Sync (EAS) with ISA Server 2006 – Part two

Abstract

In this article series, I will show you how to publish Microsoft Exchange Server Active Sync (EAS) with ISA Server 2006 to provide secure e-mail access for you Windows Mobile 5 and 6.x clients.

Let's begin

This is part two of the article series how to publish Microsoft Exchange Active Sync with ISA Server 2006. I will show you how to create the ISA Server Web publishing rule and the Windows mobile device configuration.

The ISA publishing rule

After everything is configured on the internal network, we can now start by creating a new Exchange publishing rule. You should give the rule a name like *EAS publishing* or something else which is easy to remember.

The Exchange version is Exchange Server 2003 and we would only publish Exchange Active Sync.

Please note:

If you want to publish Exchange Active Sync with Exchange Server 2007, the publishing process on ISA Server is quite similar, but the configuration steps on Exchange Server site are more different. You can read here more about these steps.

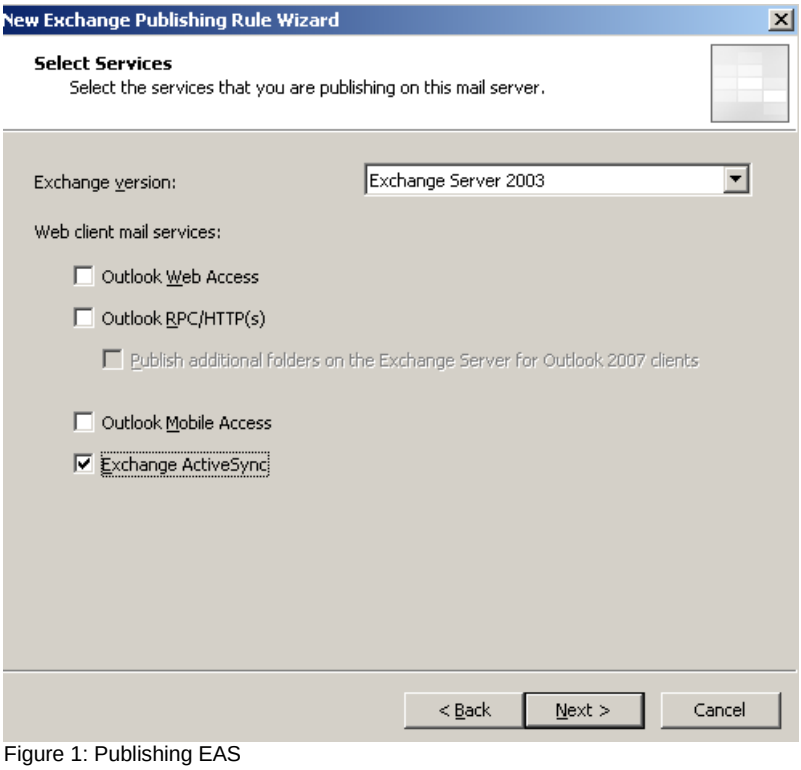

Figure 1: Publishing EAS

Click *Publish a single Website or Load Balancer*

We will use SSL to connect to the published Web server or server farm, because we also enabled the use of SSL on the Microsoft-Server-ActiveSync directory.

Enter the internal site name. Please remember that the internal site name must match the Common Name of the certificate issued to the Exchange Server and the name must be resolvable from ISA Server. Before you click next, try to ping the Exchange Server by the name you enter in the following picture.

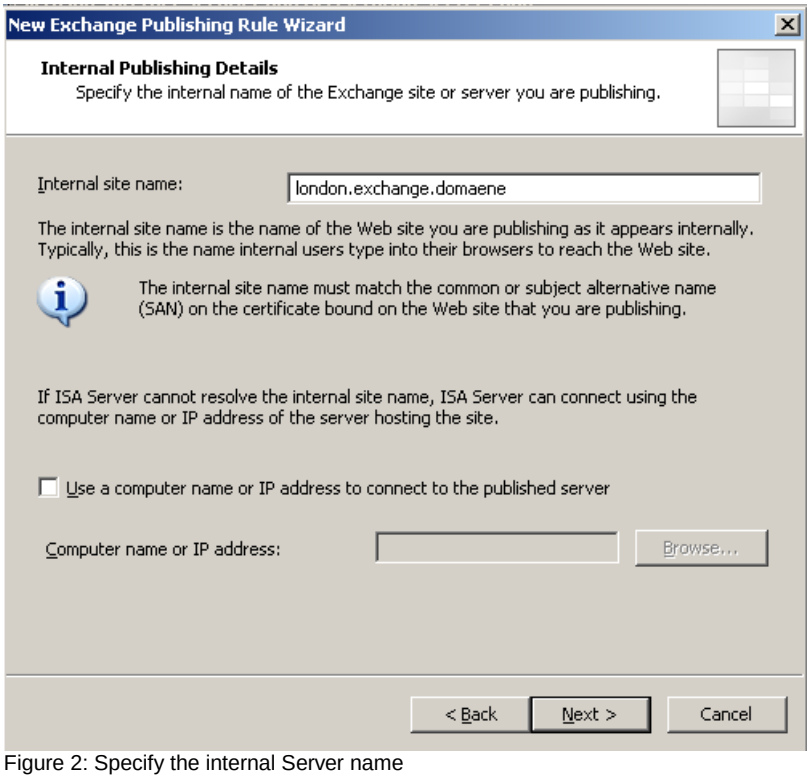

Figure 2: Specify the internal Server name

Enter the public name which you will use in the mobile device configuration (remember that you have issued a certificate on ISA which Common Name (CN) must match with the public name).

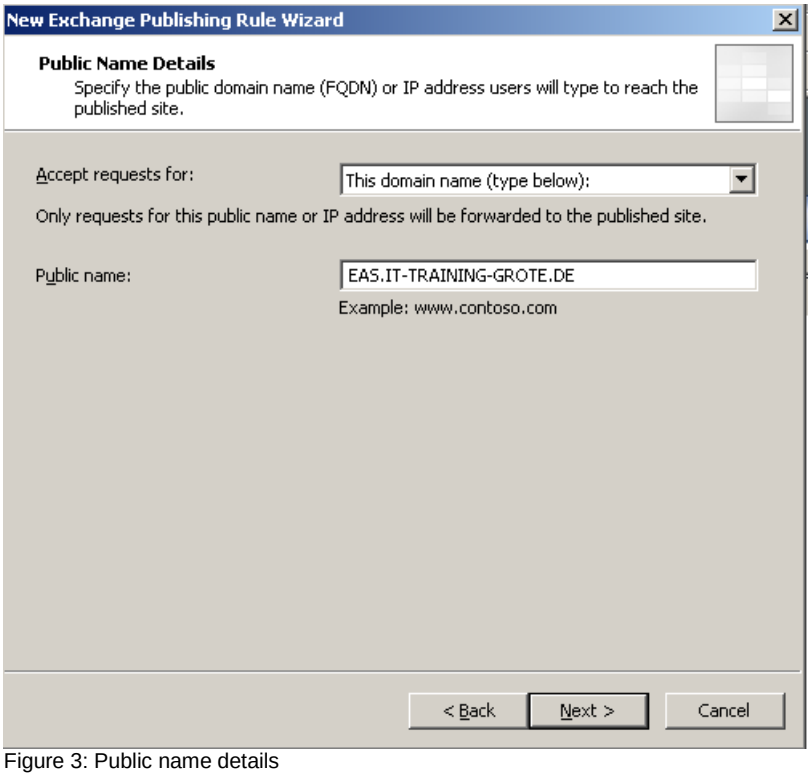

Figure 3: Public name details

Create a new Weblistener and name it *EAS* or something like that.

Require SSL secured connections with clients

In the Weblistener properties specify the external network as the source for the listener. If you plan to use more than on listener, specify the IP address which will be used to publish EAS.

Select the certificate for the EAS publishing rule. If the certificate doesn't show in the console, check that the certificate is in the local computer certificate store, that the certificate has a corresponding private key, that the certificate is valid and can be verified to the certificate chain path.

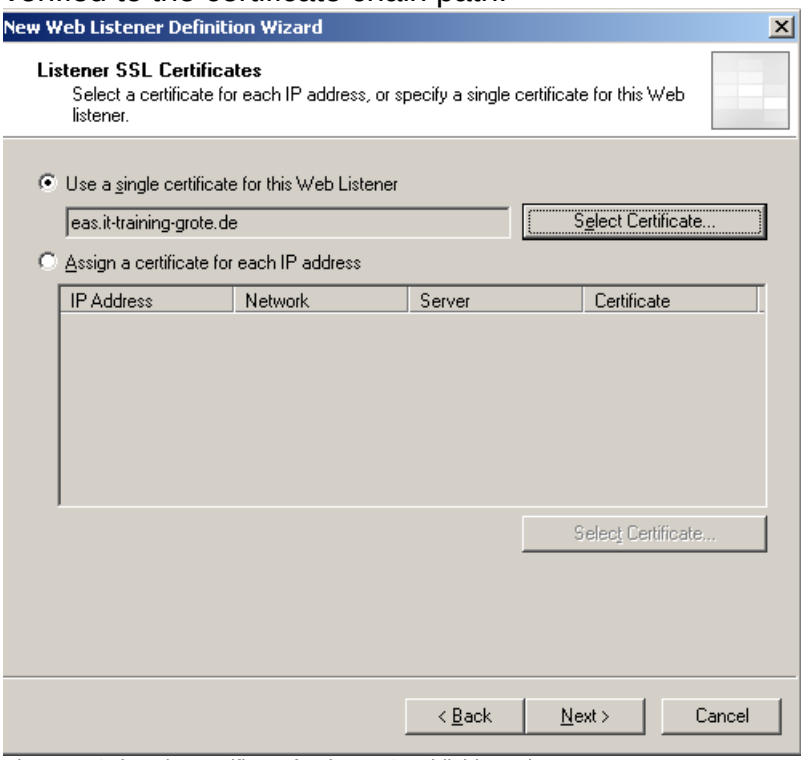

Figure 4: Select the certificate for the EAS publishing rule

As the authentication method you must select *SSL Client Certificate Authentication*.

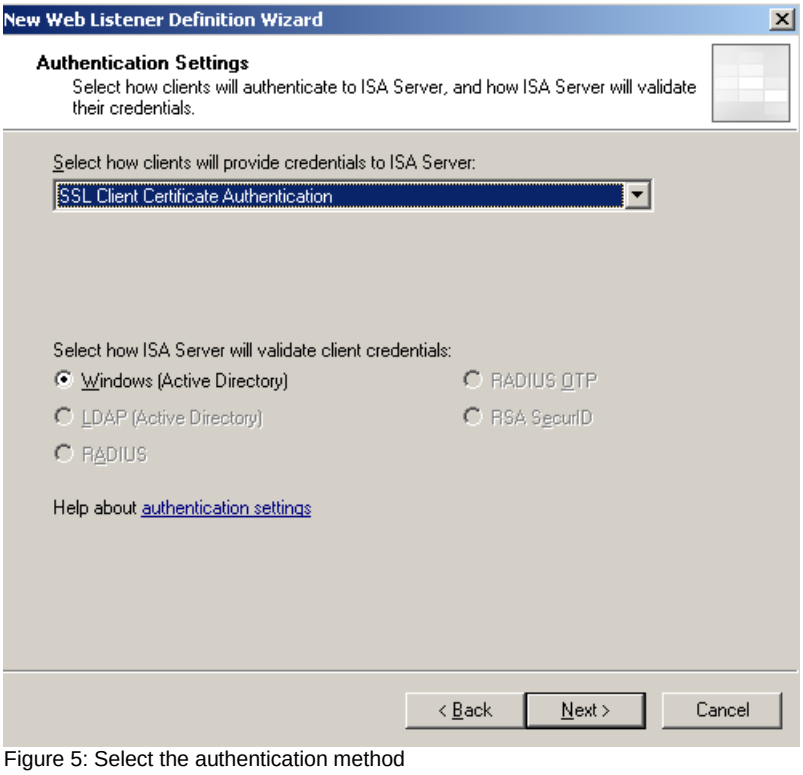

Figure 5: Select the authentication method

If you use client certificate authentication, ISA Server must be able to access the internal CA Server to access the CRL (Certificate Revocation List). If you click Yes, ISA Server will enable a system policy rule to get access to the internal network for CRL download.

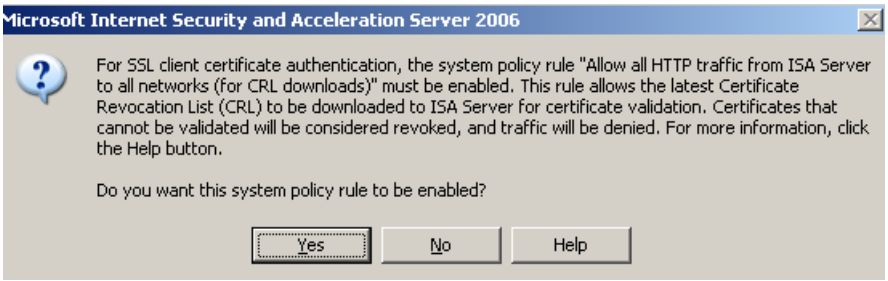

Figure 6: Enable a system policy rule for HTTP access

In a client certificate scenario with ISA Server we must use Kerberos Constrained Delegation (KCD), so ISA Server can impersonate the user to authenticate them against the authentication provider which is Active Directory.

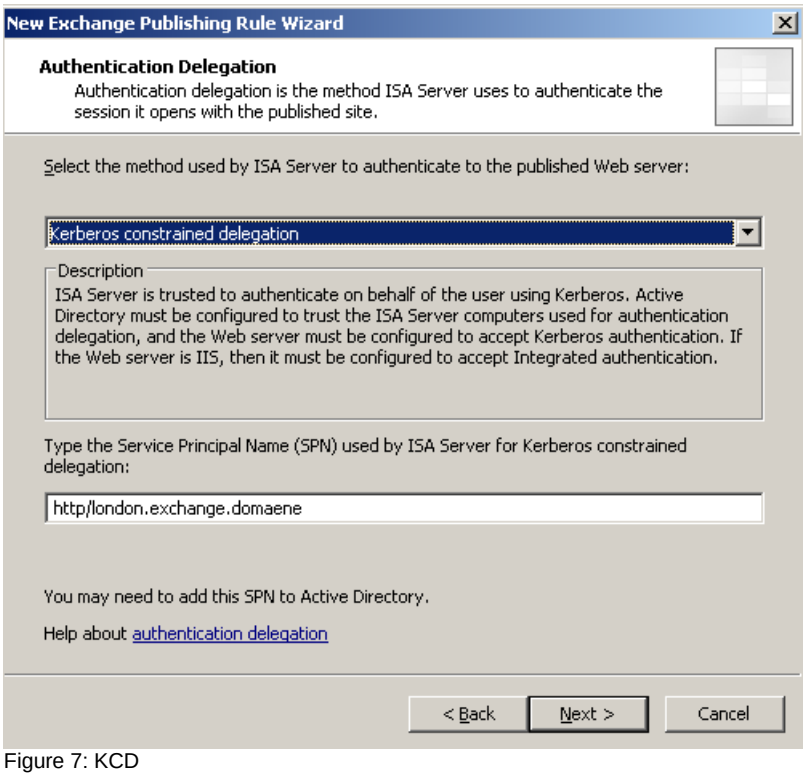

Figure 7: KCD

The SPN (Service Principal Name) is based on the internal site name. Under some circumstances you have to manually add the SPN to ISA Server with the help of the command line tool SETSPN. You will find the SETSPN tool in the Windows Server 2003 support tools which can be found on the Windows Server 2003 CD or better as an updated version on the Microsoft website.

Specify the user group which is allowed to get access through the ISA publishing rule to the published Exchange Server.

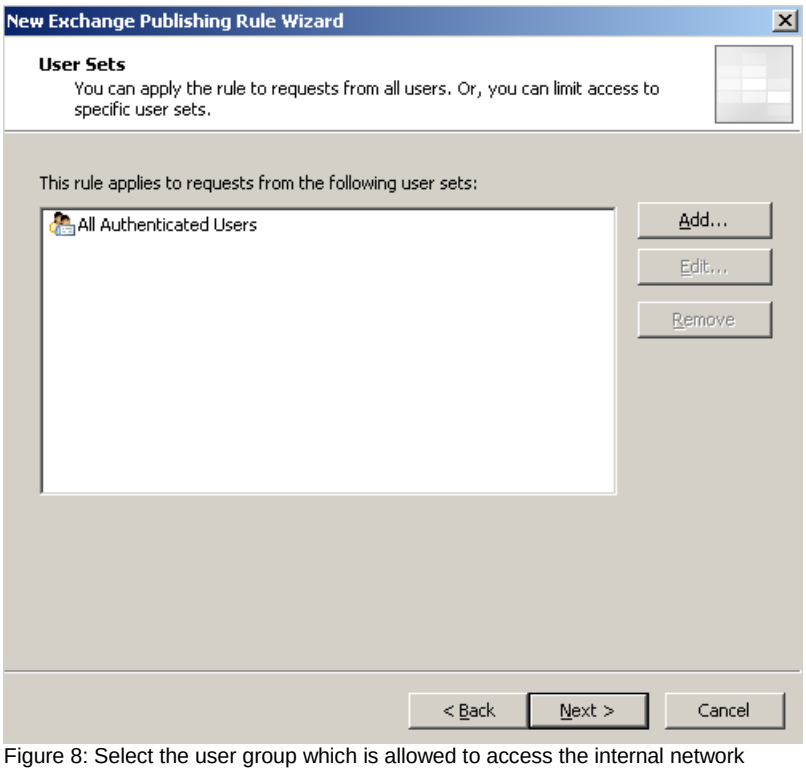

Figure 8: Select the user group which is allowed to access the internal network

The user also needs a certificate published to Active Directory. You must logon with the user credentials and request a user certificate. You can do this with the local MMC SnapIn.

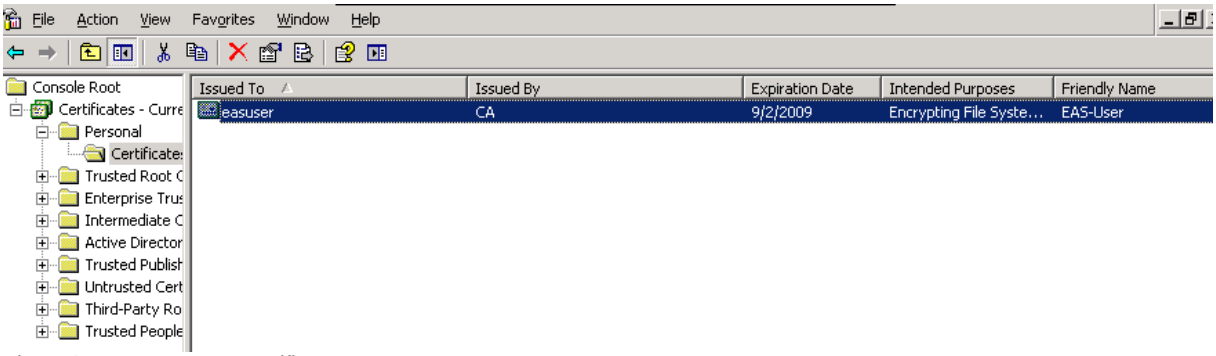

Figure 9: Request a user certificate

Please note:

In this example we use this not user friendly and a little bit complicated process. If you must enable EAS with client certificates for a bunch of users you can use tools like CertAuthTool to automate this process, but this is out of the scope of this article.

In the next picture you can see the public key certificate mapped to the user account which would like to use Exchange Active Sync from his mobile device.

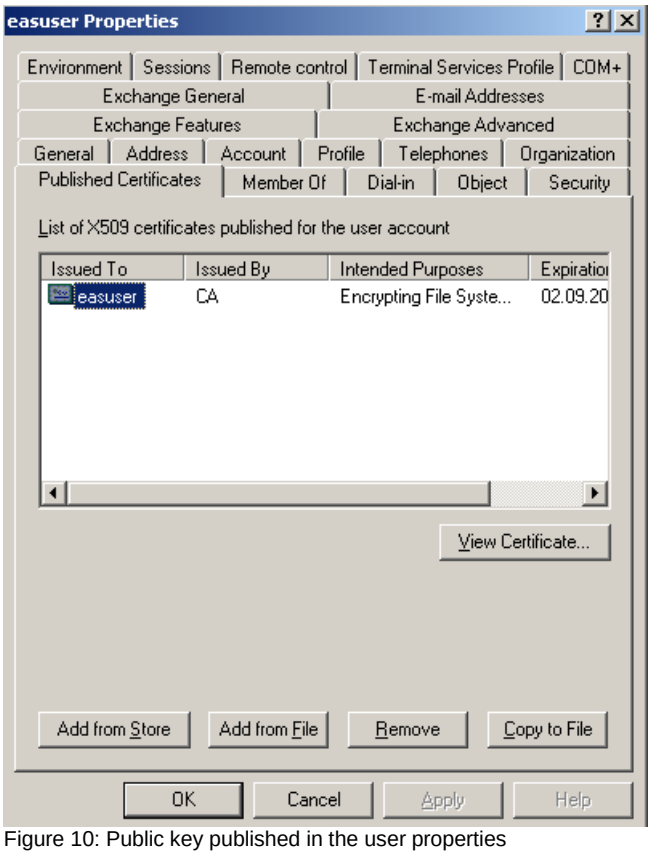

Figure 10: Public key published in the user properties

Mobile device configuration

If you don’t want to use a physical mobile device to test EAS with client certificates, you can use a Windows Mobile Device emulator like the Microsoft Device Emulator 3.0. You can find the link for the Emulator at the end of this article.

After downloading the Emulator, follow the installation instructions.

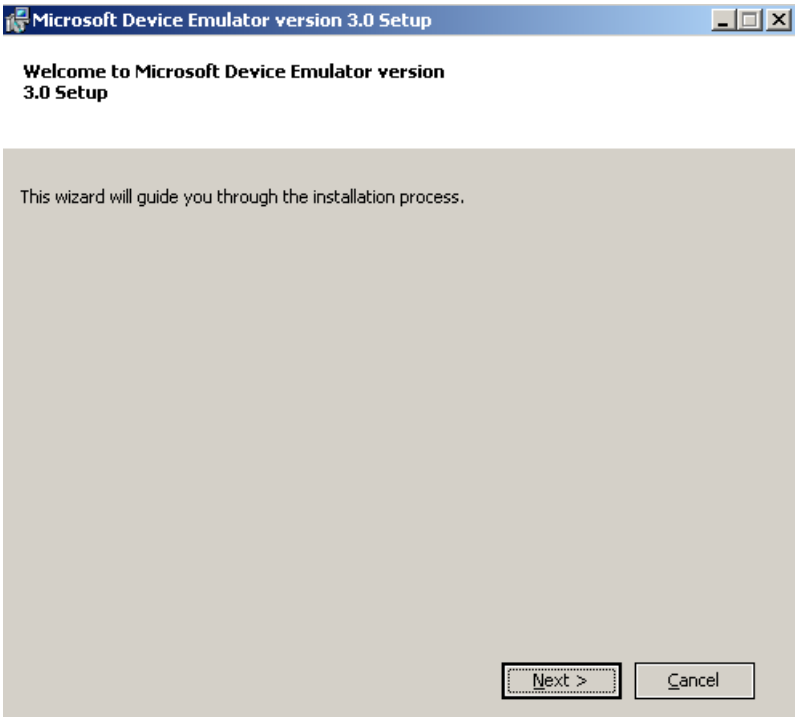

Figure 11: Installing the device Emulator

After the mobile device is correctly installed and configured you must import the user certificate for the mobile user into the certificate store of the mobile device. To do that, the first part is to export the issued user certificate from the local user certificate store to a memory card and insert this memory card into the mobile device. You can also use the Windows Mobile Device Center in Windows Vista or Active Sync if you use Windows XP.

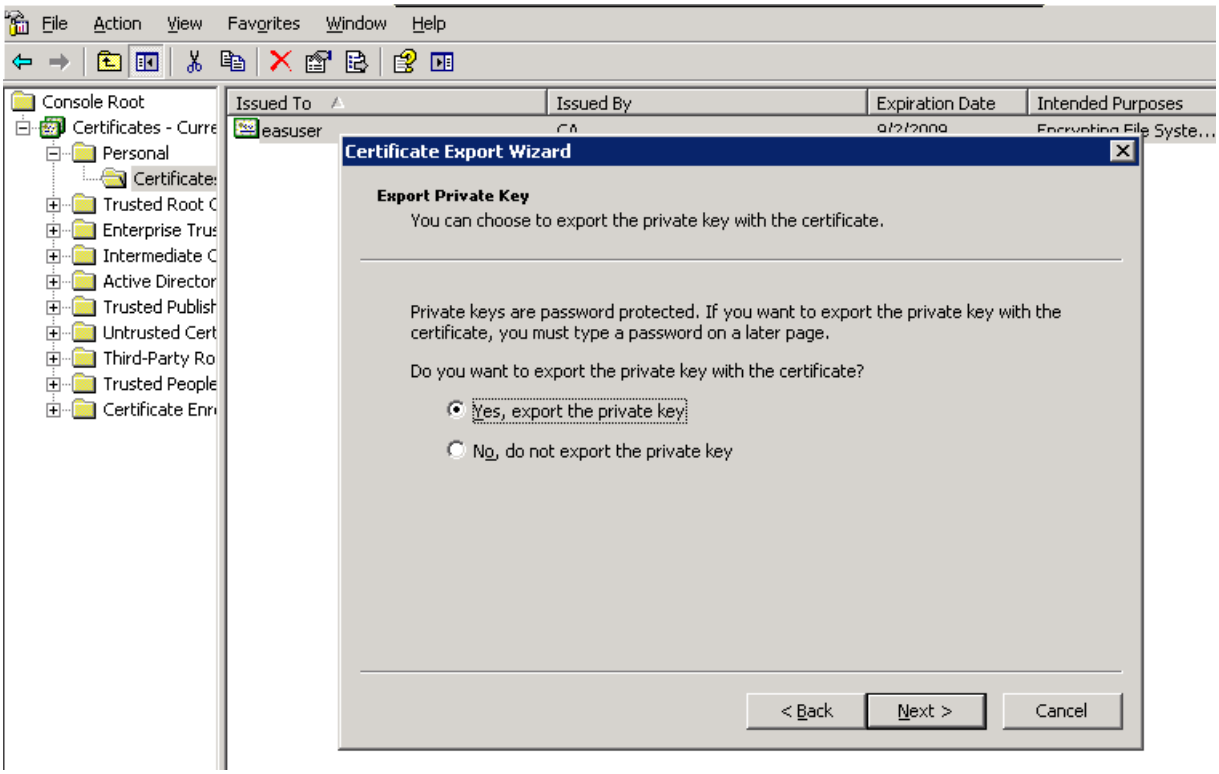

Figure 12:Export the certificate with the private key

On the Mobile device

After importing the certificate, start Microsoft Active Sync on the mobile device and follow the instructions to establish a connection to the Exchange Server.

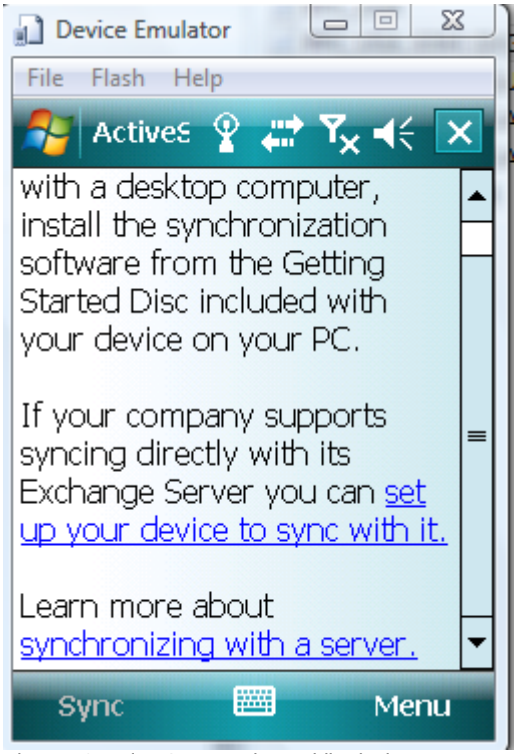

Figure 13:Active Sync on the mobile device

If you are using a mobile device emulator, you must first cradle the device. To cradle the device you must use the Device Emulator Manager. This function allows the

mobile device to connect the Exchange Server over the TCP/IP connection of the client computer where the mobile device is connected to.
The client device must also have Exchange Active Sync (Windows XP) or the Windows Mobile Device Center (Windows Vista) installed.

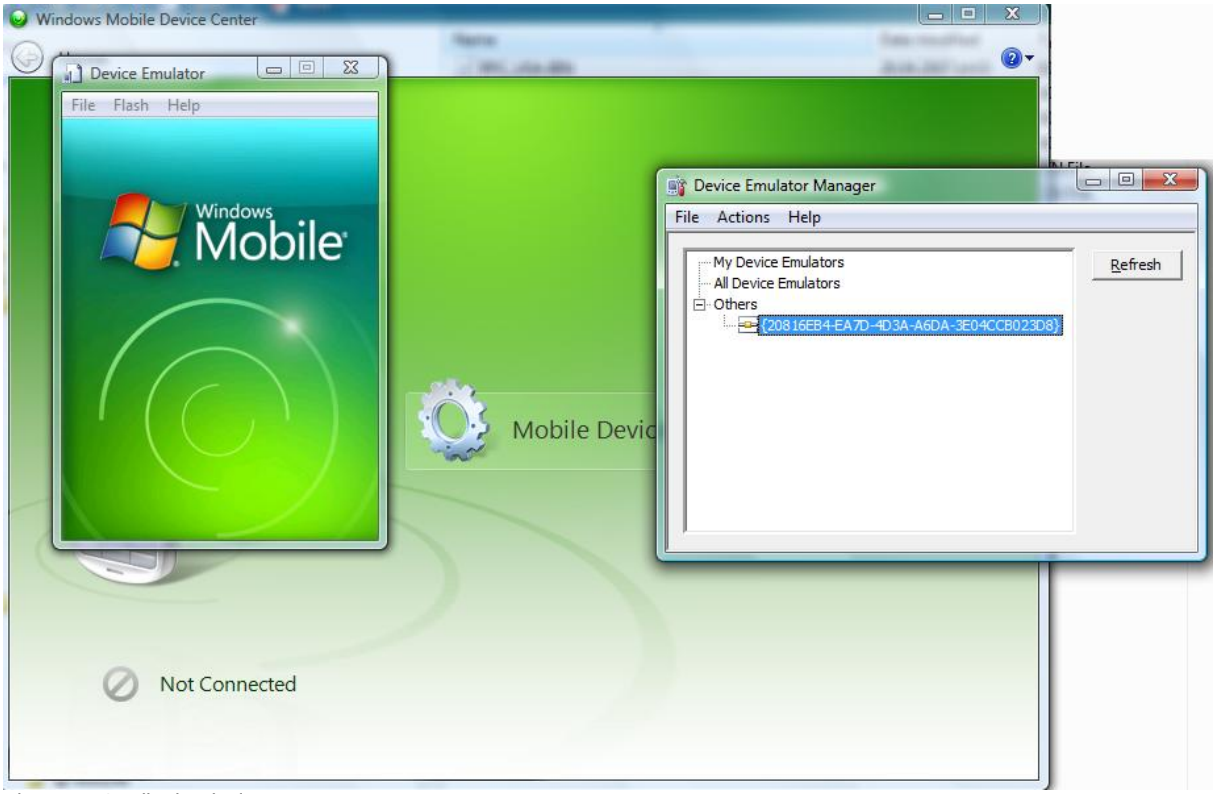

Figure 14:Cradle the device

If you cradled the device to the client PC, you can use DMA to connect the mobile device to the Client PC:

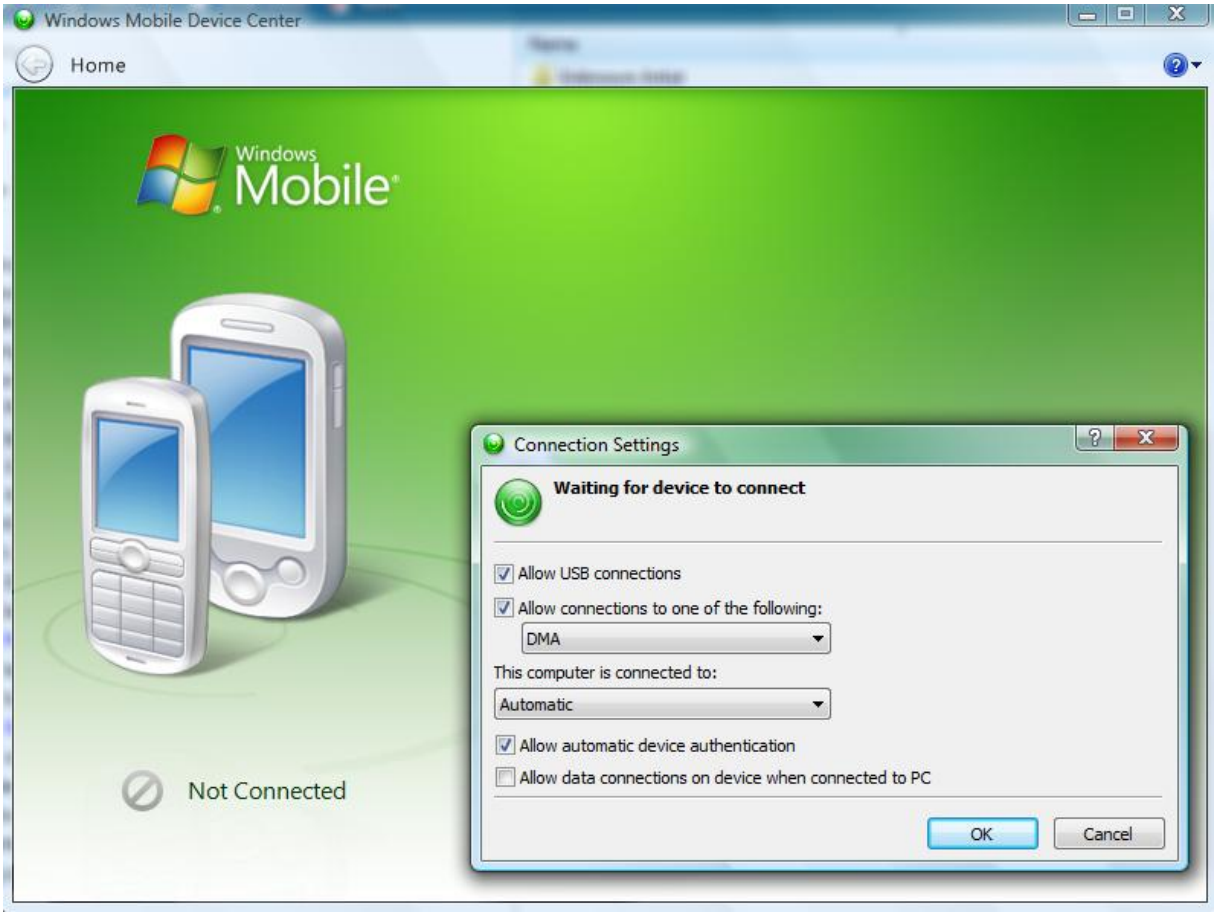

Figure 15:Use DMA to connect to the Mobile device

Synchronize the mobile device

To synchronize the mobile device click *Menu* on your mobile device. In the context menu click *Add Server Source*.
Add the Server name. The server name is the name which clients will use from the Internet. Do not enter the name of the internal Exchange Server! – Activate The Server name requires an encrypted connection.
Enter the username, password and Windows domain name of the user. After that you must select the items to sync. For some items it is possible to specify the sync time range (calendar) and the size of synced messages (e-mail).

If everything is correctly configured, click *Sync* and the mobile device should sync with your Exchange Server.

Conclusion

In this article, I tried to show you how to use Exchange Active Sync with ISA Server 2006 and Exchange Server 2003 SP2 and client certificates. The combination of ISA Server 2006 and client certificates gives you a maximum of Security for Exchange Active Sync. As you have seen, multiple steps are required to enable Exchange Active Sync in this configuration and there are some pitfalls like wrong certificates and not correctly configured Kerberos Constrained Delegation, but I hope that this article will give you a good understanding how to implement a scenario like this in your environment.

Related links

Step-by-Step Guide to Deploying Windows Mobile-based Devices with Microsoft Exchange Server 2003 SP2
http://www.microsoft.com/technet/solutionaccelerators/mobile/deploy/msfpdepguide.mspx
How to use Microsoft Exchange Active Sync with SSL
http://support.microsoft.com/kb/817379/en-us
Microsoft Device Emulator 3.0 -- Standalone Release
http://www.microsoft.com/downloads/details.aspx?familyid=a6f6adaf-12e3-4b2f-a394-356e2c2fb114&displaylang=en
Securing Exchange Data from Unapproved Mobile Devices (or how to block a phone or service from taking data out of your Exchange Server)
http://msexchangeteam.com/archive/2008/09/05/449757.aspx
Microsoft System Center Mobile Device Manager 2008
http://www.microsoft.com/windowsmobile/en-us/business/solutions/enterprise/mobile-device-manager.mspx
Overview of Exchange ActiveSync in Exchange Server 2007
http://technet.microsoft.com/en-us/library/aa998357(EXCHG.80).aspx
Microsoft Exchange Server ActiveSync Certificate-Based Authentication Tool
http://www.microsoft.com/downloads/details.aspx?FamilyId=82510E18-7965-4883-A8C3-F73F1F4733AC&displaylang=en