Securing E-Mails with S/MIME and Smartcards in Exchange 2003

Written by Marc Grote - mailto:grotem@it-training-grote.de

Abstract

In this article I will give you a high level overview about the necessary steps how to secure E-Mails with Outlook 2003 and Smartcards.

Let's begin

I think we should start with some basic information about S/MIME and why to use Smartcards with S/MIME.

What is S/MIME?

S/MIME is short for Secure / Multipurpose Internet Mail Extension and provides two security services:

- Message encryption
- Digital signatures

S/MIME is one of two industry wide accepted standards for encrypting and signing e-mails. The other Standard is PGP (Pretty Good Privacy) but of the scope in this article.

The first version of S/MIME (S/MIME 1) was developed in 1995 and was not widely accepted. S/MIME 2 was introduced in 1998. S/MIME 2 was submitted to the IETF (Internet Engineering Task Force). The IETF created RFC2311 and RFC2312. Since S/MIME was an IETF standard it establishes as a standard for message security. The actual Standard is S/MIME 3 which was proposed by the IETF to enhance the S/MIME capabilities (RFC2632, RFC2633 and RFC2634). S/MIME version 3 is beside PGP the most used Standard.

S/MIME version 3 is supported by the following Microsoft products:

- Microsoft Outlook Express 5.01 and later
- Microsoft Outlook 2000 SR1 and later
- Microsoft Exchange 5.5 and later

Why S/MIME?

Before S/MIME, administrators used unencrypted E-Mails which were transmitted via SMTP in clear text. As you know, the Single Mail Transfer Protocol (SMTP), transports data unencrypted over the wire. As a solution for this problem, you can use S/MIME which encrypts and/or signs e-mails carried over SMTP.

Why use S/MIME with Smartcards

S/MIME deployment with Smartcards and S/MIME Deployment via Soft Token (Key and certificate stored on hard disk) are very similar. For both deployments certificates and Keys will be used for e-mail encryption and e-mail signing. The main difference is where private keys are stored. If you are using Smartcards the Private Key is stored on the Smartcard and can only be accessed through the Smartcard PIN. The Two Factor Authentication is more secure than the stored Private Key on the hard disk (which can be protected by a password and saved in the Protected Storage).

Let's start with the demo

For this demonstration you will need a Windows Server 2004 machine with installed IIS 6 and certificate services and at a minimum a Windows XP Client with Outlook 2003.

First of all we will need a Certificate Authority which will issue the required certificates. Installing and maintaining a CA is out of the scope of this article. For this article we need a smartcard enrollment agent. The Smartcard enrollment Agent can issue Smartcard certificates to users which uses these Smartcards. The following picture shows the Certificate templates of a Windows Server 2004 Enterprise CA.

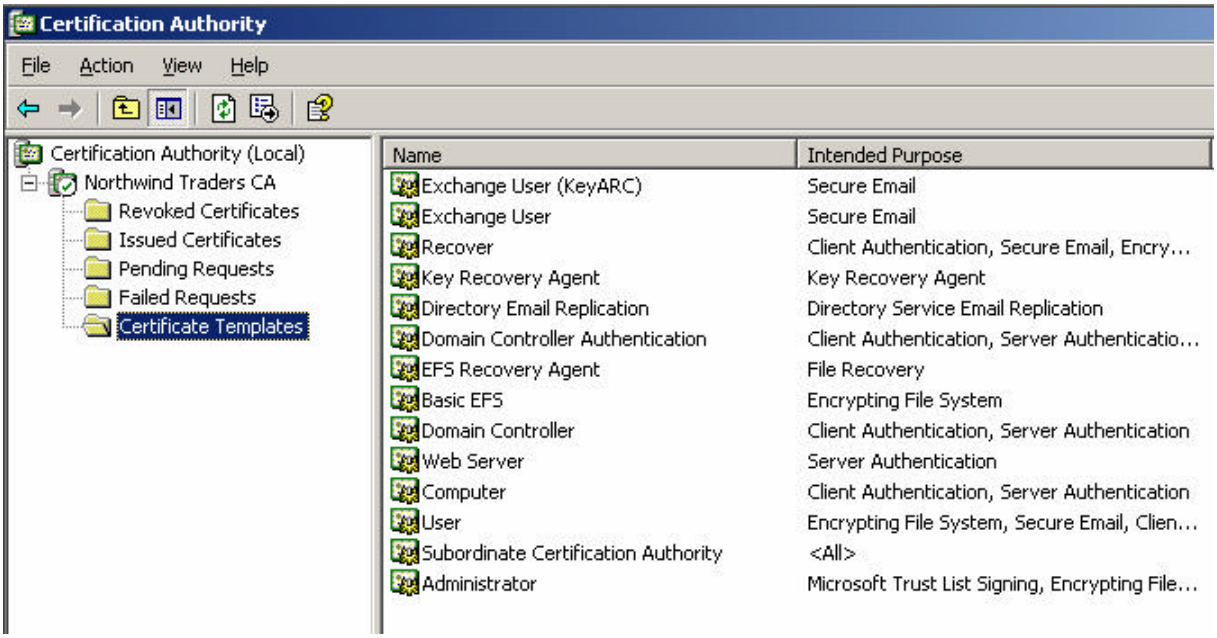

Figure 1: Certificate Template of a Windows 2003 Enterprise CA

If you issue a Smartcard User certificate you will automatically issue an S/MIME certificate for the user.

To issue certificates you must give one or more users in your Enterprise the right to deploy certificates on Smartcards for ordinary users. This is accomplished by the Enrollment Agent certificate shown in the following picture. After the certificate is issued to the user, you can start requesting certificates for your users.

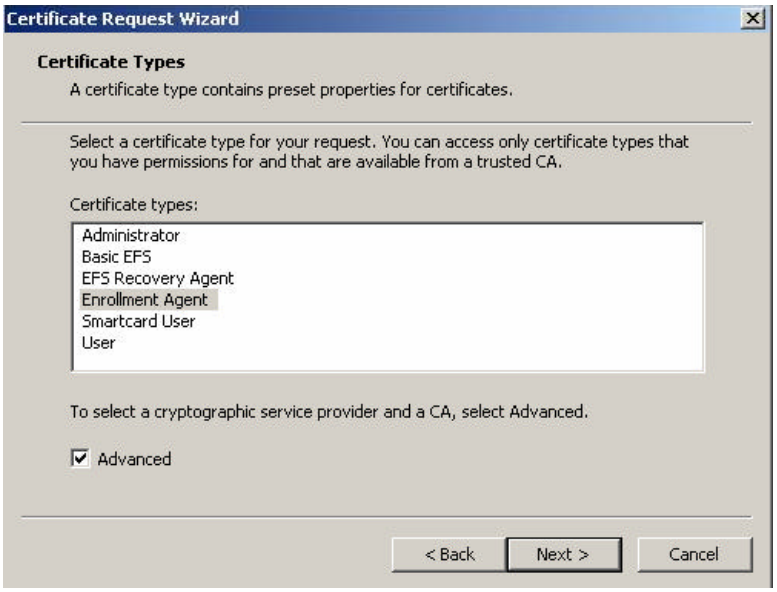

Figure 2: Enrollment Agent certificate

To issue certificates for users start the Microsoft Certificate Services website (http://CAServername/certsrv) and click the link *Request a certificate for a smart card ...*

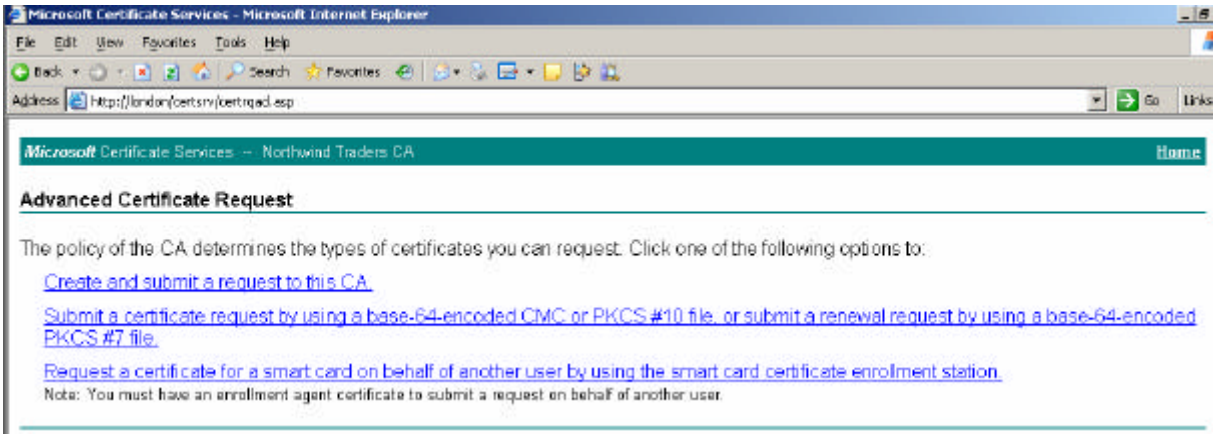

Figure 3: using the Webinterface to issue certificates

In our scenario we are issuing a Smartcard certificate for the users SMIME1 and SMIME2. The Cryptographic Service Provider is Kobil Smart CSP v1.0. Smartcard Service Providers depends on the CSP provided by the Smartcard manufacture. In this example we are using a Kobil Smartcard solution.

Before you can use the Cryptographic Service Provider you must install the CSP into Windows because Windows comes with few Cryptographic Service Provider. Most Smartcard manufactures will install the required CSP by installing the software package from the Smartcard Provider.

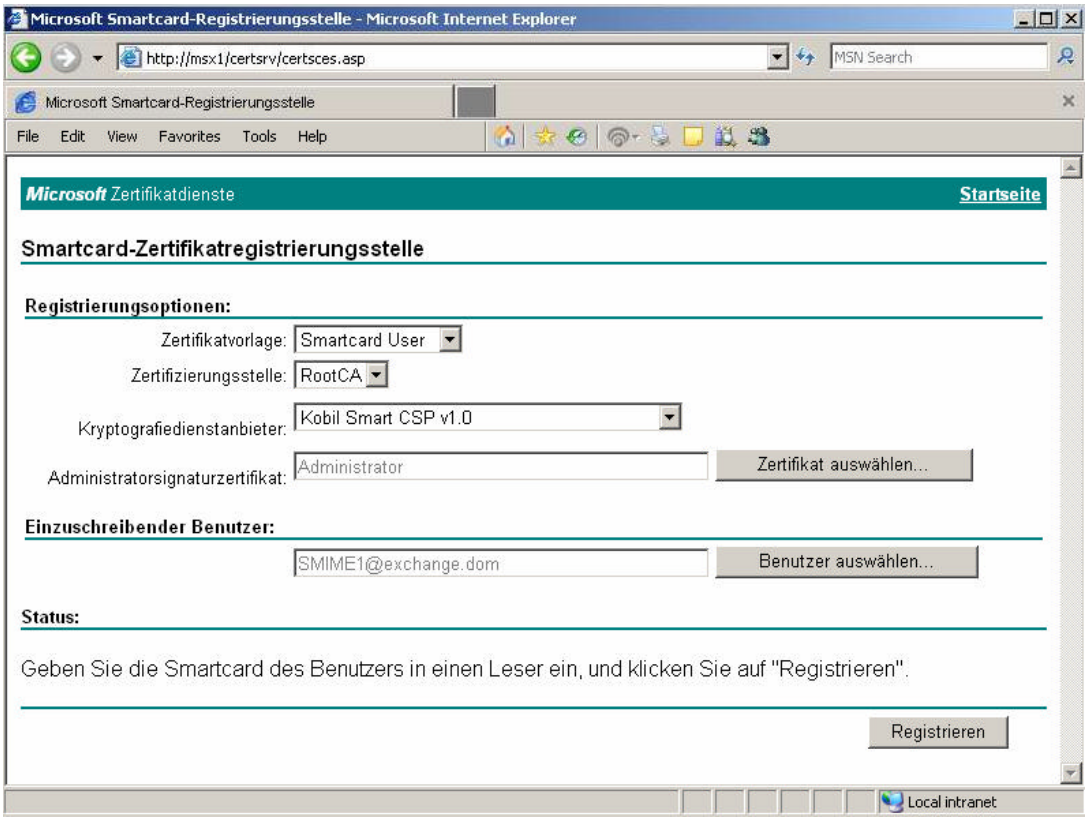

Figure 4: Issuing a Smartcard Certificate for the user SMIME1

You must enter your PIN to write the Certificate to the Smartcard.

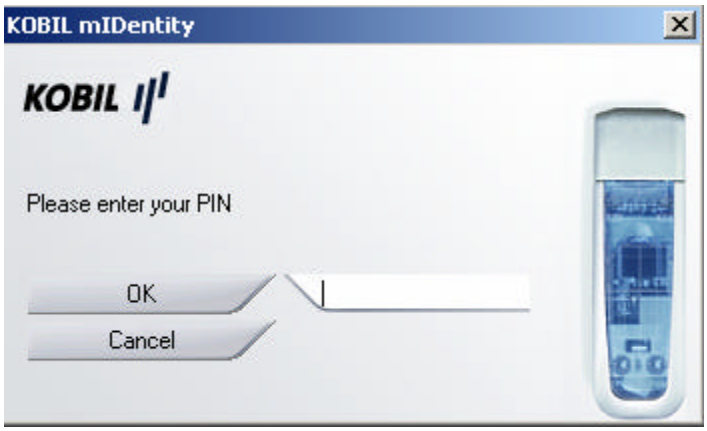

Figure 5 Enter the PIN for Smartcard access

After issuing the Smartcard User certificate have a look into the issued certificate and you can see the purposes of this certificate.

Figure 6: Certificate purposes

Now it is time to give the smartcard to the user and to automatically configure Outlook 2003. One requirement for using S/MIME with Smartcards is that the user issuing the Smartcard must have an Exchange mailbox before issuing an S/MIME certificate so the certificate will be stored in the certificate store of the user. The Private Key is stored on the smartcard. Outlook will automatically take ower the settings from the S/MIME certificate. Start Outlook and navigate to the Security Options and you will see the correct Security settings for S/MIME.

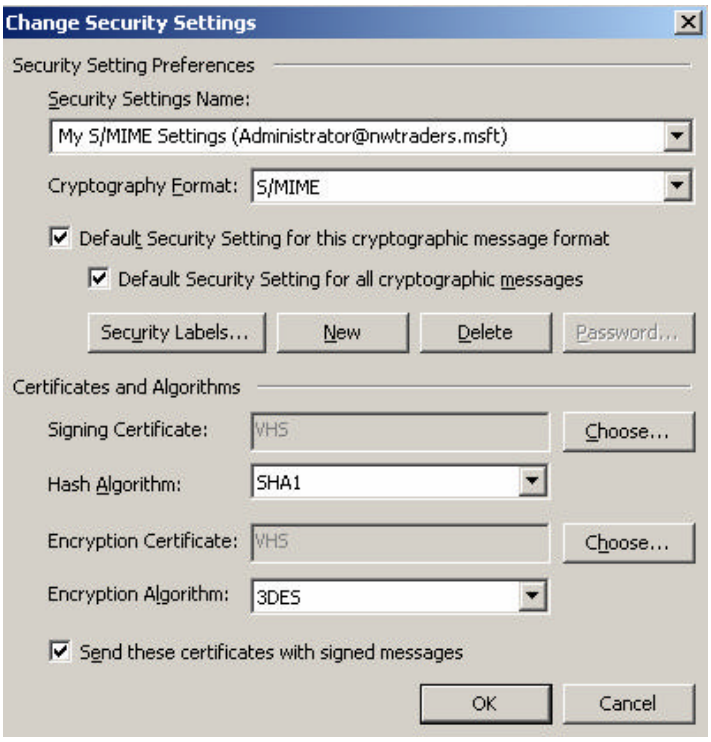

Figure 7: Certificate purposes

Try to send an encrypted E-Mail from SMIME1 to SMIME2 by activating the encryption setting in the mail that you would like to send or in the general settings in Outlook if you want to encrypt every E-Mail send by this user. If you click *Send* in Outlook you will be notified to enter the PIN to access the Smartcard certificate.

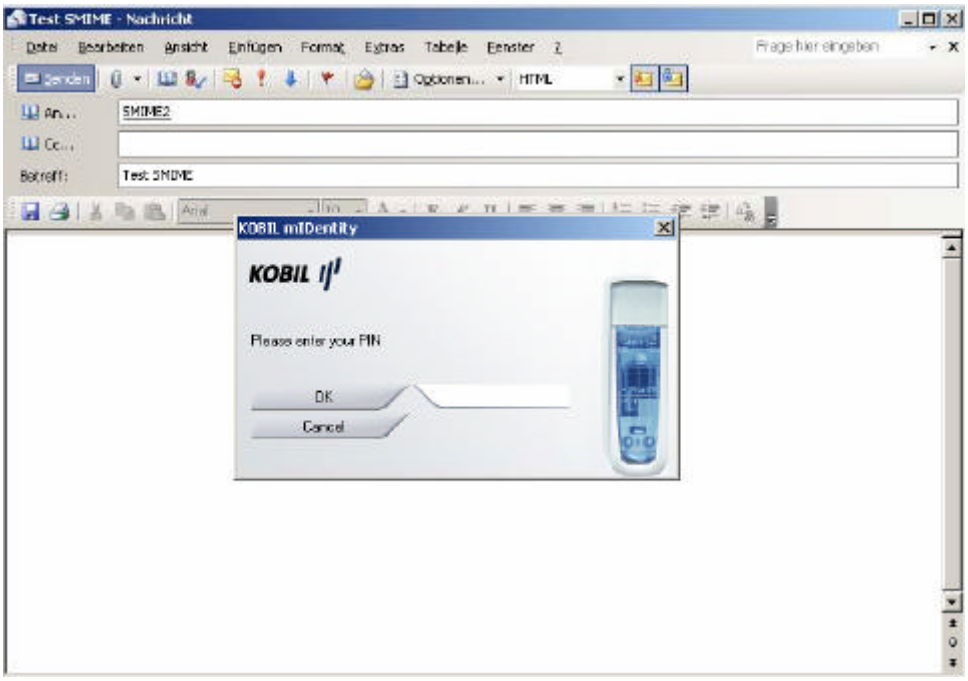

Figure 8: Sending an encrypted E-Mail

The message is now encrypted and can start its travel through the insecure Internet.

Conclusion

In this article I have shown you how to implement secure E-Mail Messaging with Outlook 2003 and Smartcards for your Exchange 2003 users.

Related Links

Public Key Infrastructure for Windows Server 2003
http://www.microsoft.com/windowsserver2003/technologies/pki/default.mspx
Configuring S/MIME Security with Outlook Web Access 2003
http://www.msexchange.org/tutorials/Configuring-SMIME-Security-Outlook-Web-Access-2003.html
Implementing Email Security with Exchange Server 2003
http://www.msexchange.org/tutorials/Email_Security_with_Exchange_2003.html