



# **Encryption in a Windows Environment:**


**EFS File, 802.1x Wireless, IPSec Transport, and S/MIME Exchange**

**Rand Morimoto**

**SAMS**

[www.sampublishing.com](http://www.sampublishing.com)

What This Short Cut Will Cover .....	3
Security the Manual Way .....	5
Installing a Windows Certificate of Authority Server .....	16
Implementing Encrypted File System (EFS) .....	23
Implementing IPSec-Encrypted Transport Communications .....	29
Implementing 802.1x Wireless Encryption .....	33
Implementing Secured Email Communications with Exchange 2003 .....	39
Summary and Other Resources .....	49



Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this work, and the publisher was aware of a trademark claim, the designations have been printed with initial capital letters or in all capitals.

The author(s) and publisher have taken care in the preparation of this work, but make no expressed or implied warranty of any kind and assume no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.

Visit us on the Web: [www.sampublishing.com](http://www.sampublishing.com)

Copyright © 2007 Pearson Education, Inc.

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, write to:

Pearson Education, Inc.  
Rights and Contracts Department  
One Lake Street  
Upper Saddle River, NJ 07458  
United States of America  
Fax: (201)236-3290

ISBN 0-768-66829-8

First release, June 2006

## SECTION 2

### Security the Manual Way

the public portion of their certificates with the others with whom they want to communicate using encrypted messaging.

To acquire a certificate, do the following:

1. Go to a certificate provider such as VeriSign (<http://www.verisign.com/products-services/security-services/pki/pki-application/email-digital-id/index.html>), and sign up and purchase a Digital ID.
2. Follow the instructions to download and install the certificate in your Outlook client.
3. Have the user you want to communicate with do the same.

This process of purchasing, downloading, and installing a certificate only needs to be done once a year.

#### NOTE

If you use multiple computers, you need to install the certificate on each machine that runs the Outlook client in order to send and receive encrypted email messages.

After you have downloaded and installed the certificate on your computer, you need to configure Outlook to support the certificate. To do so, do the following:

1. Launch Outlook.
2. Choose Tools | Options, and then click on the Security tab.
3. Click the Settings button.
4. Enter **Email Encryption** for the Security Settings Name, choose S/MIME for Cryptographic Format, and then select the check boxes for Default Security Setting for This Cryptographic Message Format and Default Security Setting for all Cryptographic Messages.
5. Choose SHA1 for Hash Algorithm and 3DES for Encryption Algorithm.
6. Select the Send These Certificates with Signed Messages option.
7. The settings should look similar to the ones shown in Figure 7. Click OK to accept these settings, and then OK again.

## Installing a Windows Certificate of Authority Server



**FIGURE 7** Configuring Microsoft Outlook to support the encryption certificate.

Depending on the user's computer sophistication, he might have difficulties signing up, downloading, and installing the certificate, as well as configuring his Outlook client to send emails. Additionally, because the certificates are individual-based, *each* individual user has to do this process himself every year and for

every system on which he conducts email communications. As you will see in the “Implementing Secured Email Communications with Exchange 2003” section, the issuance of certificates and the configuration of the user's Outlook client can be completed automatically using autoenrollment of certificates, as well as using group policy objects in Windows 2003 Active Directory.

## Installing a Windows Certificate of Authority Server

The manual processes noted in the previous section showed what is involved in manually enabling security in a Windows and Exchange environment. Beyond the complexity of users having to perform critical system tasks to enable and access secured information, the security provided by these manual methods is not even that good. A simple compromise of a shared key can invalidate the security of files, access systems, and secured communications. The better method is to use a certificate-based security system using encryption to provide a significantly higher level of security. Additionally, by automating the process, users do not have to be involved in the encryption, transport, or communications between their laptop or desktop, and the network.

## SECTION 3

### Installing a Windows Certificate of Authority Server

This section covers the creation of a certificate of authority server system that issues certificates and the process known as *autoenrollment of certificates* that automatically issues certificates to users and computers in a Windows 2003 Active Directory environment.

#### NOTE

This section assumes that you have a Windows 2003 server that has been fully patched with the latest Windows 2003 service pack and updates and that the server is connected to a Windows 2003 Active Directory network. If you are creating this system in a limited lab environment, the certificate server can be added on the same server system as the global catalog server so that a single domain controller and certificate server can be used.

### Adding the Certificate Service to a Server

The *Certificate Service* is the Windows service that allocates certificates to be issued to users and computers. It is nothing more than a service added to an existing Windows 2003 server system.

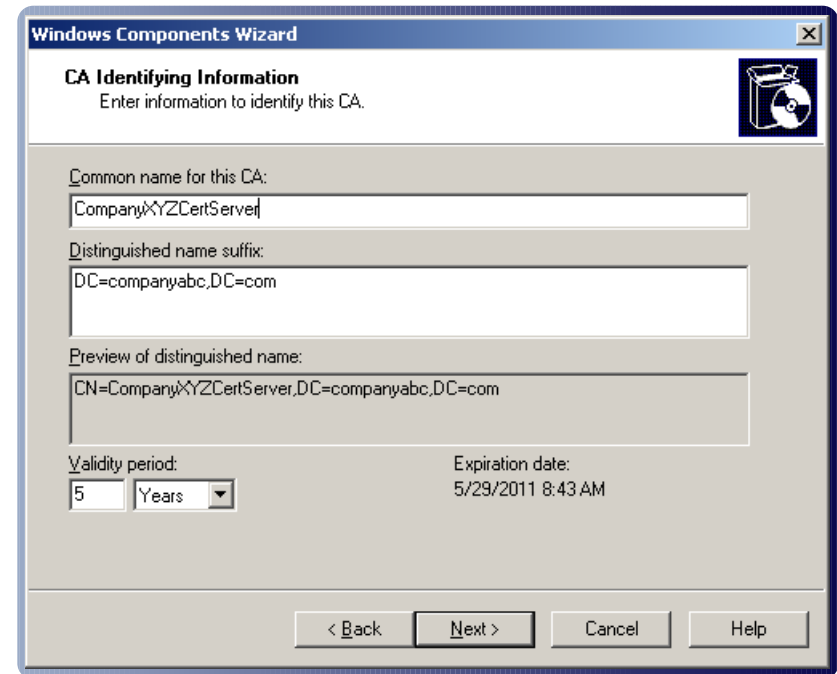
To install the Certificate Service to a system, do the following:

1. On the server that will become your certificate server, click on Start | Settings | Control Panel.
2. Double-click on Add or Remove Programs, and then click on Add/Remove Windows Components.
3. Select the check box for Certificate Services. The warning note that pops up will inform you that once you install Certificate Services on this system, you cannot change the server name or domain membership. Assuming you are okay with this, click Yes to continue.
4. If you have not installed IIS Web Services on this system yet, in the Windows Components screen, highlight Application Server and click on Details.
5. Select the Internet Information Services (IIS) check box, and then click OK. Then click Next to begin the installation of the Certificate Services and IIS components.
6. Assuming this is the first certificate server in your environment, choose Enterprise Root CA for the type of certificate of authority server, and then click Next.

## SECTION 3

### Installing a Windows Certificate of Authority Server

7. For the common name for this CA, enter a name. Typically, the name of the server is selected; however, a distinguishable name such as **xyzCertServer** (where xyz is a short name of the company) can help identify the certificate server in the future.
8. Leave the Distinguished Name Suffix and the Validity Period as is. The CA Identifying Information page should look similar to what is shown in Figure 8. Then click Next.
9. Click Next through the defaults of the Certificate Database Settings page (click Yes through the warning that IIS must be temporarily stopped). Click Finish after the installation of the component files has been completed.



**FIGURE 8** Certificate identifying information settings.

## Configuring Autoenrollment of Certificates

After the certificate service has been installed on the system, the administrator of the network can issue certificates to users and computers. However, rather than manually generating and issuing certificates, the

## SECTION 3

### Installing a Windows Certificate of Authority Server

best practice is to have the certificate server automatically issue certificates to users and computers in Active Directory. This is known as *autoenrollment of certificates*.

Autoenrollment of certificates requires the following:

1. A certificate template needs to be created.
2. The template needs to be added to the Certificate of Authority server.
3. A group policy needs to be created to automatically deploy the certificate to the user or computer.

With autoenrollment of certificates, rules are created that define which certificates should be issued to a user or computer. For example, a rule can be created for the autoenrollment of a certificate, allowing a user to have her certificates automatically created for the encryption of data files. With autoenrollment of encrypted files, the user can simply save files to a shared location, and the files stored in that location will be encrypted.

To have certificates automatically installed for the users in Active Directory, do the following:

1. On the certificate server you just created, launch the Certificate Template Microsoft Management Console (MMC) by clicking Start | Run and typing **mmc.exe**; then click OK.
2. Click File | Add/Remove Snap-in, and then click Add.
3. Select Certificate Templates, and then click Add.
4. Click Close, and then click OK.
5. Click on the Certificate Templates folder.
6. Right-click on the User Template and select Duplicate Template.
7. For the Template Display Name, enter **AutoEnroll User**.
8. Make sure the Publish Certificate in Active Directory and the Do Not Automatically Reenroll If a Duplicate Certificate Exists in Active Directory options are both checked. The screen should look similar to Figure 9.