

# Quick Start Guide for S/MIME in Exchange Server 2003



Product Version:  
Reviewed by:  
Latest Content:  
Author:

Exchange Server 2003  
Exchange Product Development  
[www.microsoft.com/exchange/library](http://www.microsoft.com/exchange/library)  
Exchange Documentation Team



**Microsoft®**

# Quick Start Guide for S/MIME in Exchange Server 2003

**Christopher Budd**

**Published:** August 2003

**Applies To:** Exchange Server 2003

## **Copyright**

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2003 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, Windows, Windows NT, Windows Server, Active Directory, ActiveX, and Outlook are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

## **Acknowledgments**

**Project Editor:** Cathy Anderson

**Contributing Editors:** Diane Forsyth

**Technical Reviewers:** David Cross, Will Duff, David Horton, Janet Piele, John Speare, Jan Suralertrungsri, Jason Urban, Roy Williams

**Graphic Design:** Kristie Smith

**Production:** Bryan Franz, Sean Pohtilla

# Table of Contents

Introduction .....	1
Preparing the Test Lab.....	2
Installing and Configuring Windows Server 2003 Enterprise Certification Authority.....	4
Installing and Configuring Active Directory.....	4
Installing and Configuring Certificate Services .....	5
Configuring Exchange Server 2003 .....	7
Configuring E-Mail Clients.....	8
Configuring Outlook 2003 .....	9
Installing the S/MIME Control in Outlook Web Access .....	9
Configuring Outlook Express for POP3 and IMAP4 .....	10
Testing Digital Signatures and Encryption.....	11
Requesting Digital Certificates for Users.....	12
Testing Digital Signatures and Encryption in Outlook 2003 .....	15
Testing Digital Signatures and Encryption in Outlook Web Access.....	21
Testing Digital Signatures and Encryption in Outlook Express.....	26
Conclusion .....	33
Additional Resources .....	34
Windows Server 2003 Certification Authority .....	34
Outlook 2003 .....	34
Other Web Sites .....	34



---

# Introduction

Microsoft® Exchange Server 2003 introduces important changes in regard to support for message security. Like Exchange 2000 Server, Exchange 2003 provides message security by offering support for both digital signatures and message encryption. These capabilities are provided through support for Secure/Multipurpose Internet Mail Extensions (S/MIME) version 3. As with Exchange 2000, Exchange 2003 fully supports S/MIME version 3 e-mail, allowing users to take advantage of message security services when sending and receiving e-mail messages with users of other S/MIME version 3 e-mail systems. However, Exchange 2003 introduces a significant change by eliminating the Key Management server in favor of functionality provided by Certificate Services in Microsoft Windows Server™ 2003. Exchange 2003 also significantly expands the scope of client support with the introduction of the Microsoft Office Outlook® Web Access S/MIME ActiveX® Control. This control enables Microsoft Internet Explorer 6 with Service Pack 1 (SP1) and later Web clients to send and receive S/MIME messages.

Because of these changes, Exchange administrators may want to begin working with S/MIME in Exchange 2003 in a lab environment to familiarize themselves with these changes and new features. Message security in Exchange 2003 relies on several technological components, some of which may normally be outside the scope of an Exchange administrator's duties and responsibilities. Administrators can use this article to familiarize themselves with these components in a lab environment.

This technical article is intended to provide a "getting started" point for Exchange administrators in deploying a fully functional S/MIME system in a lab environment using technologies from Microsoft. After following this technical article, Exchange administrators will have a fully functional S/MIME environment based on Certificate Services, Exchange 2003, Internet Explorer 6 with the S/MIME ActiveX Control, Outlook Express 6, and Microsoft Office Outlook 2003. In this lab environment, Exchange administrators will be able to see how the different technologies work together to provide the complete S/MIME system.

This technical article does not explain the underlying concepts; it is intended only to provide the steps that are needed to deploy the components in an S/MIME system. The goal of this article is to provide familiarity with the functioning of an S/MIME system, allowing administrators to see the functions and benefits of using S/MIME in their environment. After evaluating the capabilities and benefits of S/MIME, administrators who want to move forward with implementing a full S/MIME deployment in their production environment should consult the appropriate documentation for each of the major components in the S/MIME system.

In addition, this article is intended only to help with the deployment of a lab environment. In the test environment presented in this article, the following practices in particular should be noted as appropriate only for test environments.

- **SSL encryption** The configuration described in this article does not use Secure Sockets Layer (SSL) encryption for HTTP, Post Office Protocol version 3 (POP3), or Internet Message Access Protocol version 4rev1 (IMAP4) access. Although this configuration may be appropriate for a test lab, SSL encryption should be used with these protocols in a production environment. For information about how to configure these protocols to use SSL, see Exchange Server 2003 Help.
- **Enterprise Root Certification Authority** This technical article uses an Enterprise Root certification authority (CA) to issue S/MIME certificates rather than developing a broader CA hierarchy. Although this approach simplifies the deployment of digital certificates, this practice is not recommended for production environments: a successful Microsoft Windows® certification infrastructure requires detailed planning beyond the scope of this article. For information about how to plan and deploy a PKI hierarchy, see "Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure" (<http://go.microsoft.com/fwlink/?LinkId=17800>).
- **Digital Certificate Requirements** This technical article provides instructions about how to manually obtain S/MIME digital certificates by using the default certificate templates in Windows Server 2003 Certification Authority. In a production environment, it is preferable to use certificate autoenrollment, because this is easier for users. In addition, the default certificates do not use features such as strong key protection, which is a requirement for many organizations. In a production environment, you may want to configure certificate templates to conform to your organization's security requirements. For information about autoenrollment, see "Certificate Autoenrollment in Windows Server 2003" (<http://go.microsoft.com/fwlink/?LinkId=17801>). For information about configuring certificate templates, see "Implementing and Administering Certificate Templates in Windows Server 2003" (<http://go.microsoft.com/fwlink/?LinkId=17802>).

---

## Preparing the Test Lab

When you prepare to build a test environment for S/MIME in Exchange 2003, consider the parts that make up a fully functional S/MIME system. This knowledge will help you plan for your lab's needs.

A fully functional Exchange 2003 S/MIME system consists of the following parts:

- Certification authority (CA)
- Exchange 2003
- E-mail clients

Although Exchange 2003 can support any certification authority that generates S/MIME version 3 digital certificates, for purposes of this lab Windows Server 2003 enterprise certification authority will be used. In addition, although any e-mail client that can both connect to Exchange 2003 and support S/MIME version 3 can be used, for purposes of this lab the following clients will be used:

- Outlook 2003 using MAPI
- Outlook Express 6 SP1 using POP3/IMAP4
- Internet Explorer 6 SP1 using Microsoft Office Outlook Web Access via HTTP

When you deploy these technologies in a lab, your S/MIME system can be used for testing S/MIME in Exchange 2003 using all supported client protocols.

As you plan for your lab's needs, you should allocate at least one computer for each part of the S/MIME system. This technical article presumes a dedicated computer for each part of the S/MIME system: thus, three separate computers. Although you can add more computers to your test lab, three computers is the recommended minimum to ensure that your lab more closely mirrors a fully deployed S/MIME system.

**Note** Outlook and Exchange are not supported when running on the same system.

The following sections of the technical article describe the steps needed to install and configure the required software for the computers in your lab. These sections should be followed sequentially. Note that each section presumes that you have completed a default installation of the operating system and base application required for each lab computer.

Table 1 lists the computers used in this technical article, along with their role, operating system, and installed application.

**Table 1 Computers used**

Computer name	Roles	Operating systems	Installed applications
CONT-CA01	Domain controller and enterprise CA	Windows Server 2003 Enterprise Edition	Certificate Services
CONT-EX01	Mailbox server and Outlook Web Access server	Windows Server 2003 Standard Edition	Exchange Server 2003
CONT-WK01	Client workstation	Windows® XP Professional Service Pack 1	Internet Explorer 6 SP1, Outlook Express 6 SP1, Outlook 2003

**Important** When building computers for your lab, make sure that your test computers have the latest security patches applied to them. Use the Microsoft Baseline Security Analyzer (MBSA) to determine what security patches your systems need. For more information about MBSA, see Microsoft Baseline Security Analyzer (<http://go.microsoft.com/fwlink/?LinkId=17809>).

**Important** Make sure lab systems are located on a separate network from your production computers. When building your lab, consult with your organization's security policy if you plan to connect your lab computers to your production network.

When you set up your lab computers, install and configure your systems in the following order:

1. Windows Server 2003 enterprise certification authority
2. Exchange Server 2003
3. E-mail clients

Each of these steps is detailed in the following sections. At the end of these steps you will then be able to use your lab computers to test S/MIME using all of the clients configured here.

---

## Installing and Configuring Windows Server 2003 Enterprise Certification Authority

The first step in setting up your lab is to configure your computer running Windows Server 2003 Enterprise Edition to be an enterprise certification authority. The certification authority is responsible for issuing digital certificates that provide S/MIME functionality. To configure your enterprise certification authority, you perform the following steps.

1. Install and configure Microsoft Active Directory® directory service.
2. Install and configure Certificate Services.

After you complete these steps, your Windows Server 2003 enterprise certification authority will be running and able to issue digital certificates.

**Note** To ensure TCP/IP network connectivity for your lab, you will either have to configure static IP addresses for your test computers, or configure a server running Windows Server 2003 to be a Dynamic Host Configuration Protocol (DHCP) server. For more information, see Windows Server 2003 Help.

---

## Installing and Configuring Active Directory

After you have completed a default installation of Windows Server 2003 Enterprise Edition, you will first need to install and configure Active Directory. This is because Certificate Services enterprise certification authority requires an Active Directory environment to install and configure successfully.

**Note** You must use Windows Server 2003 Enterprise Edition for the system that will be your certification authority. Windows Server 2003 Standard Edition is not designed to be an enterprise certification authority.

### To install Active Directory on Windows Server 2003

1. Either at the console or through a terminal session, log on to CONT-CA01 as a member of the Administrators group.
2. Click **Start**, click **Run**, type **dcpromo**, and then click **OK**.
3. On the first page of the Active Directory Installation Wizard, click **Next**.
  - Note** If this is the first time you have installed Active Directory, you can click **Active Directory Help** to learn more about Active Directory before clicking **Next**.
4. On the next page of the Active Directory Installation Wizard, click **Next**.
5. On the **Domain Controller Type** page, click **Domain Controller for a new domain**, and then click **Next**.
6. On the **Create New Domain** page, click **Domain in a new forest**, and then click **Next**.
7. On the **New Domain Name** page, in the **Full DNS name for new domain** box, type corp.contoso.com, and then click **Next**.
8. On the **Database and Log Folders** page, accept the defaults in the **Database folder** box and the **Log folder** box, and then click **Next**.
9. On the **Shared System Volume** page, accept the default in the **Folder location** box, and then click **Next**.
10. On the **DNS Registration Diagnostics** page, click **Install and configure the DNS server on this computer and set this computer to use this DNS server as its preferred DNS Server**, and then click **Next**.
11. On the **Permissions** page, click **Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems**, and then click **Next**.
12. On the **Directory Services Restore Mode Administrator Password** page, enter a password in the **Restore Mode Password** box, retype the password to confirm it in the **Confirm password** box, and then click **Next**.
  - Note** Consult your organization's security policy to ensure that the password you select meets your organization's security requirements.
13. On the **Summary** page, confirm the information is correct, and then click **Next**.
14. When prompted to restart the computer, click **Restart now**.
15. After the computer restarts, log on to CONT-CA01 as a member of the Administrators group.

At this point, you have successfully installed Active Directory and you can now install and configure Certificate Services.

---

## Installing and Configuring Certificate Services

One capability of Certificate Services that you will want to use in your lab is the Web-based enrollment feature. This feature requires Internet Information Services (IIS) to function. Therefore, before installing Certificate Services, you must first install IIS.

### To install IIS on Windows Server 2003

1. Either at the console or through a terminal session, log on to Cont-CA01 as a member of the Administrators group on the local computer.
2. Click **Start**, point to **Control Panel**, and then click **Add or Remove Programs**.
3. In **Add or Remove Programs**, click **Add/Remove Windows Components**.
4. In the Windows Components Wizard, under **Components**, select **Application Server**.

**Note** Selecting **Application Server** performs a default installation of Internet Information Services (IIS) and includes components that are not necessary for Certificate Services. In most cases, this installation is acceptable for an isolated test environment. However, if you plan to connect your test environment to your production network, consult your organization's security policy to determine which components to install.

5. Click **Next**.
6. After the wizard completes the installation, click **Finish**.

After you install IIS, you can now install Certificate Services.

### To install a Windows Server 2003 Enterprise CA

1. Either at the console or through a terminal session, log on to CONT-CA01 as a member of the Enterprise Administrators and Domain Administrators group.
2. Click **Start**, point to **Control Panel**, and then click **Add or Remove Programs**.
3. In **Add or Remove Programs**, click **Add/Remove Windows Components**.
4. In the Windows Components Wizard, under **Components**, select **Certificate Services**.
5. Read the warning about domain membership, and then click **Yes**.
6. Click **Next**.
7. On the **CA Type** page, click **Enterprise root CA**, and then click **Next**.
8. On the **CA Identifying Information** page, in the **Common name for this CA** box, type CONT-CA01, and then click **Next**.
9. On the **Certificate Database Settings** page, accept the defaults in the **Certificate database** box and the **Certificate database log** box, and then click **Next**.
10. When prompted to stop Internet Information Services, click **Yes**.
11. When asked if you want to enable Active Server Pages (ASPs), click **Yes**.

**Note** Selecting **Yes** enables Active Server Pages in Certificate Services. In most cases, this installation is acceptable for an isolated test environment. However, if you plan to connect your test environment to your production network, consult your organization's security policy to determine if this configuration is appropriate.

12. After the wizard completes the installation, click **Finish**.

At this point, you have successfully configured your enterprise certification authority. You are ready to issue digital certificates to users. The next step in building your lab environment is to configure Exchange 2003 to support S/MIME.

# Configuring Exchange Server 2003

As noted earlier, this section presumes that, after you've completed the installation and configuration of your Active Directory and Certification Authority on CONT-CA01, you have then performed a default installation of Exchange Server 2003 on a default installation of Windows Server 2003. During the installation, add your Exchange server to the same forest and domain as CONT-CA01.

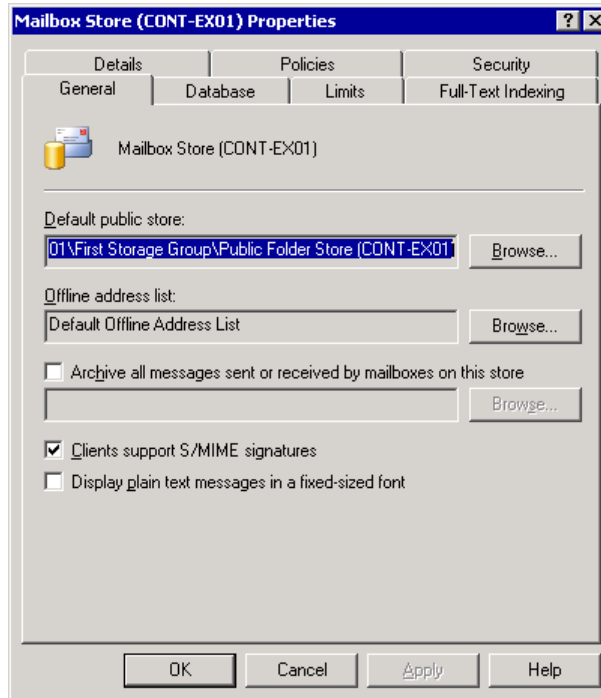
**Important** When you install Exchange 2003, you should use the Exchange Server Deployment Tools to ensure that your installation has completed successfully.

Because Exchange relies primarily on the CA and the e-mail client for S/MIME functionality, the primary task you need to do to the Exchange server is ensure that the message store that holds the user mailboxes is configured to hold S/MIME messages. This setting is enabled by default and does not require configuration. However, if you want to view the setting, use the following steps.

## To view the message store configuration for S/MIME messages

1. Either at the console or through a terminal session, log on to CONT-EX01 using an account that is a member of both:
  - The Administrators group on the local computer
  - A group to which at least the **Exchange View Only Administrators** role has been applied at the administrative group level
2. Click **Start**, point to **All Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
3. Click **Administrative Groups**, click **First Administrative Group**, click **Servers**, click **CONT-EX01**, click **First Storage Group**, right-click **Mailbox Store (CONT-EX01)**, and then click **Properties**.

4. On the properties page, verify that the **Clients support S/MIME signatures** check box is selected (see Figure 1).



**Figure 1** Configuring message store for S/MIME messages

After you verify that the Exchange server is configured to support S/MIME messages, you're ready to install and configure your e-mail clients.

---

## Configuring E-Mail Clients

The final step in installing and configuring your lab is to install and configure your e-mail clients on your client workstation. As previously noted, this section presumes that you have completed a default installation of Windows XP Professional with Service Pack 1 and Outlook 2003. During the installation, add your workstation to the same forest and domain as CONT-CA01.

After you complete the installation, configure at least three user accounts in the domain to use for testing.

---

## Configuring Outlook 2003

Because Outlook settings are stored as part of the user profile on the local workstation, you need to configure Outlook for each user. Although in a production environment this procedure can be automated, for the purposes of this lab, it is easiest to configure profiles manually by logging on to the workstation using each of your user test accounts and performing the following steps.

### To configure Outlook 2003 for each user

1. At the console, log on to CONT-WK01 as a member of the Domain Users group.
2. Click **Start**, point to **All Programs**, point to **Microsoft Office**, and then click **Microsoft Office Outlook 2003**.
3. On the first page of the Outlook 2003 Startup Wizard, click **Next**.
4. On the **Account Configuration** page, select **Yes**, and then click **Next**.
5. On the **Server Type** page, select **Microsoft Exchange Server**, and then click **Next**.
6. On the **Exchange Server Settings** page, in the **Microsoft Exchange Server** box, type the name of the server running Exchange Server 2003 (CONT-EX01).
7. On the **Exchange Server Settings** page, in the **User Name** box, type the user name for the current user account, and then click **Check name**. Ensure that the name resolves correctly.
8. On the **Exchange Server Settings** page, make sure the **Use local copy of Mailbox** check box is selected, and then click **Next**.
9. On the last page, click **Finish**.
10. When prompted, enter the user name and initials in the **User Name** box.

At this point, you have successfully configured Outlook.

---

## Installing the S/MIME Control in Outlook Web Access

To enable S/MIME connectivity for Outlook Web Access, you must download and install the S/MIME ActiveX control. After you install the control on the workstation, it is available for all users, which means you install the control only once. However, installing the control does require administrative privileges on the workstation.

**Important** This technical article does not provide information about configuring Outlook Web Access to use SSL to encrypt information. Therefore, information such as passwords and e-mail messages will be sent in clear text between the Outlook Web Access client and the Exchange server. Although this behavior is appropriate in a controlled lab environment, it is not recommended for use in production. For information about how to install and configure Outlook Web Access to use SSL, see Exchange Server 2003 Help.

### To install the Outlook Web Access S/MIME Control

1. At the console, log on to CONT-WK01 as a member of the Administrators group on the local computer.
2. Click **Start**, point to **All Programs**, and then click **Internet Explorer**.
3. Click **File**, click **Open**, type `http://cont-ex01.corp.contoso.com/exchange` in the **Open** box, and then click **OK**.
4. Type the user name and password in the dialog box.
5. In Outlook Web Access, in the Navigation Pane, click **Options**. If the Navigation Pane is collapsed, click the **Go to options** button.
6. On the **Options** page, under **E-Mail Security**, click **Download**.
7. If any security warnings appear, click **Yes**.

The S/MIME control will be downloaded from the Exchange server and installed to the local computer. At this point, you have successfully configured Outlook Web Access for your test workstation.

---

## Configuring Outlook Express for POP3 and IMAP4

Because Outlook Express settings are stored as part of the user profile on the local workstation, you need to configure Outlook Express for each user to use either POP3 or IMAP4. To do this, log on to the workstation using each test account and perform the following steps.

**Important** This technical article does not provide information about configuring POP3 or IMAP4 to use SSL to encrypt information. Therefore, information such as passwords and e-mail messages will be sent in clear text between the Outlook Express client and the Exchange server. Although this behavior is appropriate in a controlled lab environment, it is not recommended for use in production. For information about how to install and configure POP3 and IMAP4 to use SSL, see Exchange Server 2003 Help.

**Note** Because the differences between configuring Outlook Express for POP3 and IMAP4 are minimal, the following instructions detail how to configure Outlook Express to use IMAP4. If you want to use POP3, substitute POP3 for all IMAP4 references in the following instructions.

### To configure Outlook Express for each user

1. At the console, log on to CONT-WK01 as a member of the Domain Users group.
2. Click **Start**, point to **All Programs**, and click **Outlook Express**.
3. When prompted to set Outlook Express as your default e-mail client, click **No**.
4. On the **Your name** page, enter the name of the current user in the **Display name** box, and then click **Next**.
5. On the **Internet E-Mail Address** page, enter the full Internet e-mail address for the user, for example `yli@corp.contoso.com`, and then click **Next**.

6. On the **E-mail Server Names** page, make the following selection, and then click **Next**:
  - In the **My incoming mail server is a list**, select IMAP.
  - In the **Incoming mail (POP3, IMAP, or HTTP) server** box, type the full name of the Exchange server, cont-ex01.corp.contoso.com.
  - In the **Outgoing mail (SMTP) server** box, type the full name of the Exchange server, cont-ex01.corp.contoso.com.
7. On the **Internet Mail Logon** page, in the **Account name** box enter the user name, clear the **Remember password** check box, and then click **Next**.
8. On the final page, click **Finish**.
9. When prompted to download folders, click **Yes**.

At this point, you have successfully configured Outlook Express for this user account. After you configure Outlook Express for all of your test users, you have completed the configuration of Outlook Express and your other e-mail clients. The next phase is the testing of S/MIME.

---

## Testing Digital Signatures and Encryption

With the CA installed and configured, the Exchange server installed and configured, and, finally, the e-mail clients installed and configured, you can begin testing.

The first step in testing is to obtain a digital certificate for each of your test users. Because S/MIME relies on digital certificates, you must obtain a digital certificate to use S/MIME. This section will help you obtain digital certificates for your test accounts from the Windows Server 2003 CA, and then step you through using those certificates to send and receive digitally signed and encrypted e-mail messages using the e-mail clients that you have configured.

**Note** The following section provides instructions about how to obtain digital certificates for users using either Web-based enrollment or the Microsoft Management Console (MMC) certificates snap-in. In addition to these options, it is possible to configure Windows Server 2003 certification authority to autoenroll users for digital certificates. Because of the configuration required to enable this feature, discussion of this feature is beyond the scope of this article. However, it is strongly recommended that this feature be used in a production environment because of the ease of use it provides to users. For information about configuring autoenrollment, see "Certificate Autoenrollment in Windows Server 2003" (<http://go.microsoft.com/fwlink/?LinkId=17801>).

## Requesting Digital Certificates for Users

Because digital certificates are specific to individual users and are stored as part of the user profile on the local workstation, you need to obtain a digital certificate for each user. There are two ways you can obtain a digital certificate for a user. You can either request one through the MMC or use a Web browser.

**Note** The first time you request a certificate using a Web browser through the Web enrollment form, you must be using an account with Administrator privileges on the local computer. This requirement is because the Web enrollment page uses an ActiveX control that requires Administrator privileges to install successfully.

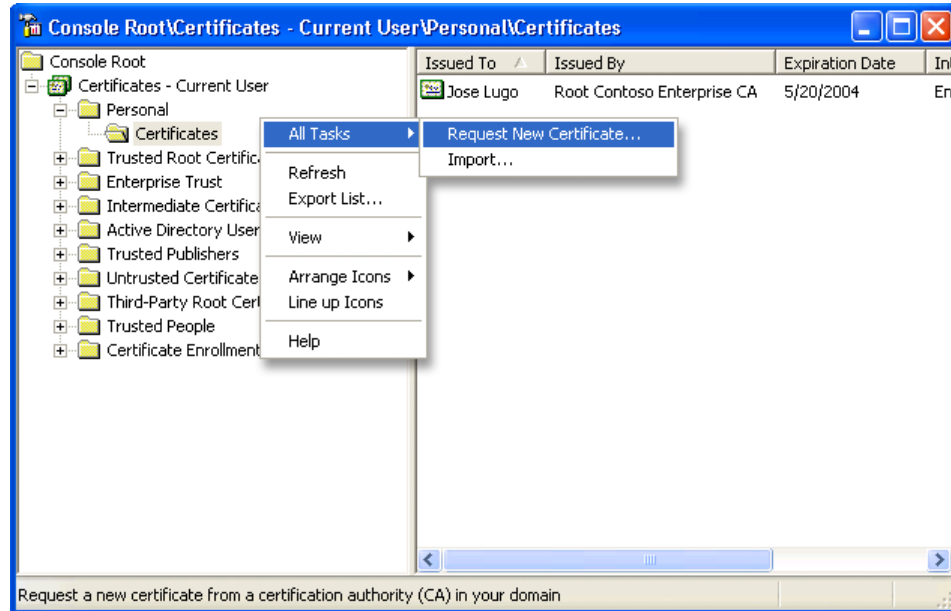
### To obtain a digital certificate using the Web enrollment form

1. At the console, log on to CONT-WK01 as a member of the Administrators group on the local computer for the first request. For all other requests, you can use an account that is a member of the Domain Users group.
2. Click **Start**, point to **All Programs**, and then click **Internet Explorer**.
3. Click **File**, click **Open**, type `http://cont-ca01/certsrv` in the **Open** box, and then click **OK**.
4. On the **Welcome** page, click **Request a certificate**.
5. On the **Request a Certificate** page, click **User Certificate**.
6. On the **User Certificate - Identifying Information** page, click **Submit**.
7. In the **Potential Scripting Violation** dialog box, click **Yes**.
8. On the **Certificate Issued** page, click **Install this certificate**.
9. In the **Potential Scripting Violation** dialog box, click **Yes**.
10. In the **Root Certificate Store** dialog box, click **Yes**.
11. When the **Certificate Installed** page is shown, close Internet Explorer.

### To request a digital certificate using MMC

1. At the console, log on to CONT-WK01 as a member of the Domain Users group.
2. Click **Start**, click **Run**, type `certmgr.msc`, and then click **OK**.
3. In MMC, expand **Certificates - Current User**, and then expand **Personal**.

- In the right pane, right-click and point to **All tasks**, and then click **Request New Certificate** (see Figure 2).



**Figure 2** New certificate request in MMC

- On the first page of the Certificate Request Wizard, click **Next**.
- On the **Certificate Types** page, click **User** in the **Certificate types** list, and then click **Next**.
- On the **Certificate Friendly Name and Description** page, type a descriptive name (such as **Network Certificate**) in the **Friendly name** box, type a description (if you want) in the **Description** box, and then click **Next**.
- On the final page of the wizard, click **Finish**.

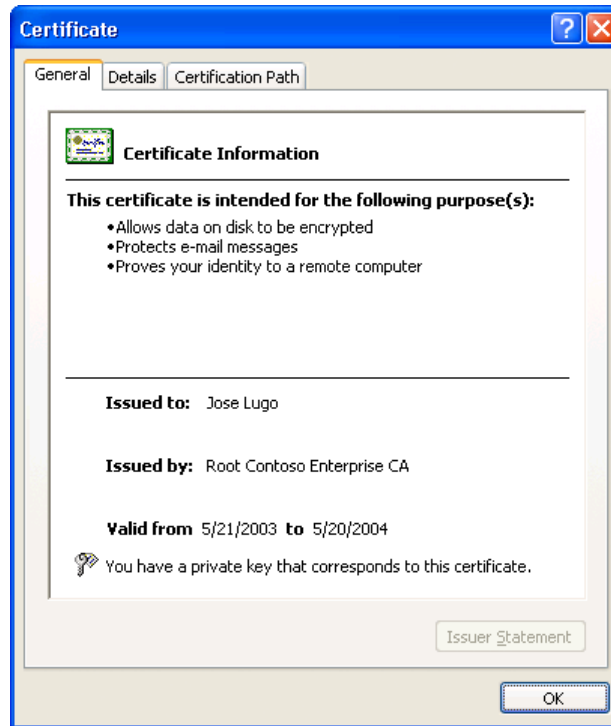
You should see a dialog box stating **The certificate request was successful**.

At this point, the digital certificate for the user is now installed in the local certificate store. To verify that the certificate is there, open the local certificate store by using the MMC.

#### To verify that the certificate has been installed

- At the console, log on to CONT-WK01 as a member of the Domain Users group.
- Click **Start**, click **Run**, type **certmgr.msc**, and then click **OK**.
- In MMC, expand **Certificates - Current User**, and then expand **Personal**.

4. In the right pane, you should see the certificate you just installed. Double-click the certificate. Figure 3 shows the certificate.



**Figure 3 User's digital certificate in the local certificate store**

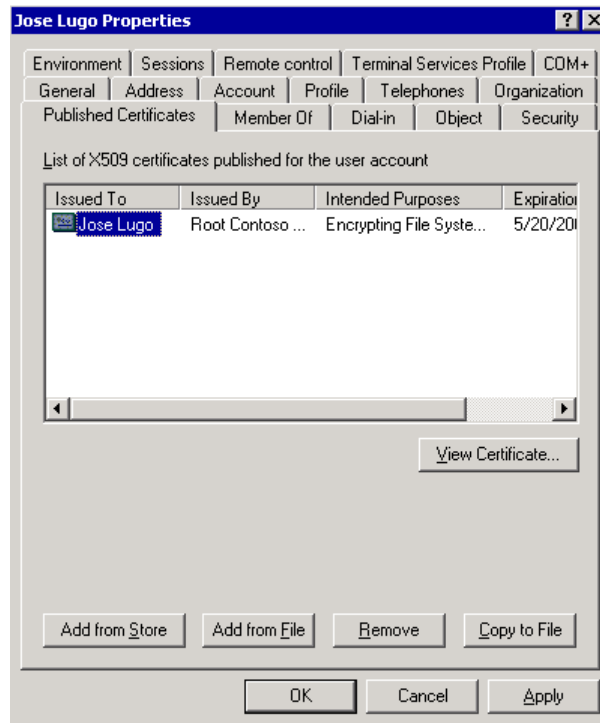
When you request a digital certificate using either the MMC or the Web enrollment form, the Windows CA automatically stores the user's digital certificate in Active Directory. Both Outlook and Outlook Web Access retrieve digital certificates that are stored in Active Directory. This means that, for those S/MIME operations where you must have a copy of the other party's digital certificate (specifically when sending encrypted e-mail messages to another party or verifying e-mail messages that have been digitally signed by another party), Outlook Web Access and Outlook can retrieve those digital certificates for you.

To verify that the digital certificate has been added to the user's account in Active Directory, you can view the certificate in the user's account in Active Directory.

#### **To verify that the certificate has been added to a user's Active Directory account**

1. Either at the console or through a terminal session, log on to CONT-CA01 as a member of the Certification Authority Administrators group.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
3. Click **View**, click **Advanced Features**.
4. On the left, click the **Users** folder.

5. On the right, double-click one of the test users.
6. Click the **Published Certificates** tab.
7. In the **List of X509 certificates published for the user account** list, you should see the user's digital certificate from the Windows CA (see Figure 4) along with any other digital certificates stored for this user in Active Directory.



**Figure 4** User's digital certificate in Active Directory

**Note** Although the certificate in the certificate store and the certificate in Active Directory look identical, there is an important difference between these two certificates. The certificate in Active Directory stores a copy of only the user's public key, and the certificate in the personal store has a private key associated with it, in addition to the public key.

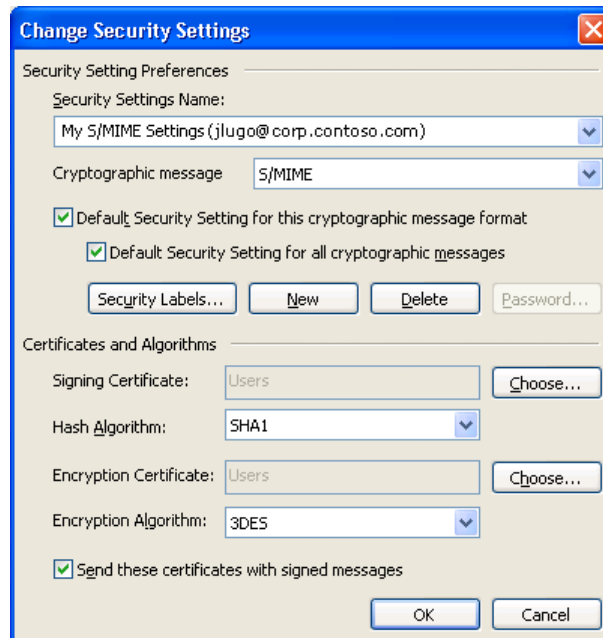
## Testing Digital Signatures and Encryption in Outlook 2003

Before you use your digital certificate to sign messages in Outlook, you must configure Outlook to use the digital certificate you just installed. Once again, because this information is stored on a per-user basis, you will need to configure each of your test user accounts.

### To configure Outlook to use a digital certificate

1. At the console, log on to CONT-WK01 as a member of the Domain Users group.
2. Click **Start**, point to **All Programs**, point to **Microsoft Office**, and then click **Microsoft Office Outlook 2003**.
3. Click **Tools**, and then click **Options**.
4. Click on the **Security** tab and click **Settings**.
5. Outlook populates the **Change Security Settings** dialog box with default information (see Figure 5). Click **OK** to accept the defaults.

**Note** If a user has more than one digital certificate in the local computer store, you must specify which digital certificate you want Outlook to use. To specify the certificate, under **Certificates and Algorithms**, click both **Choose** buttons.



**Figure 5 Security settings in Outlook**

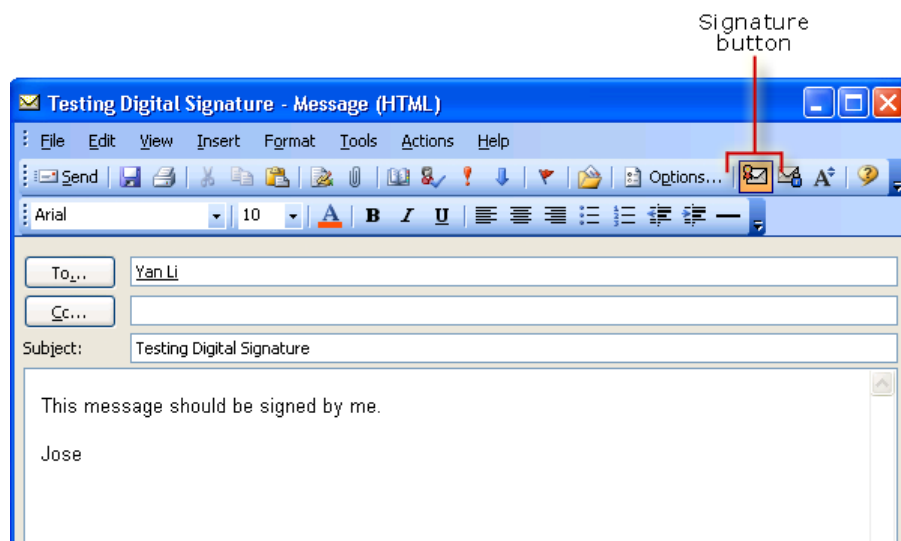
6. Click **OK** to close the **Options** dialog box.

**Note** After you configure these settings, the **Add digital signature to this message** button and **Encrypt message contents and attachments** button are automatically added to the new mail message form when Word is enabled as the e-mail editor. In Outlook 2003, Microsoft Word is enabled as the e-mail editor by default and these settings make these buttons visible by default. If you do not use Word as the e-mail editor, you will not see these buttons by default. To make these buttons appear, you can re-enable Word as the e-mail editor or customize the Outlook e-mail editor. For information about how to make these changes, see Outlook 2003 Help.

Now that Outlook is configured to use the digital certificate you installed for this user, you can test sending and receiving digitally signed and encrypted messages.

### To send a digitally signed message using Outlook

1. At the console, log on to CONT-WK01 as a member of the Domain Users group.
2. Click **Start**, point to **All Programs**, point to **Microsoft Office**, and then click **Microsoft Office Outlook 2003**.
3. To compose a new message, click **New**.
4. Add a recipient for the test message and fill out the message fields.
5. Ensure that the **Add digital signature to this message** button is selected (see Figure 6). Because you want to test only digital signing, ensure that that the **Encrypt message contents and attachments** button is not selected.



**Figure 6** Digitally signed message in Outlook

6. Click **Send**.

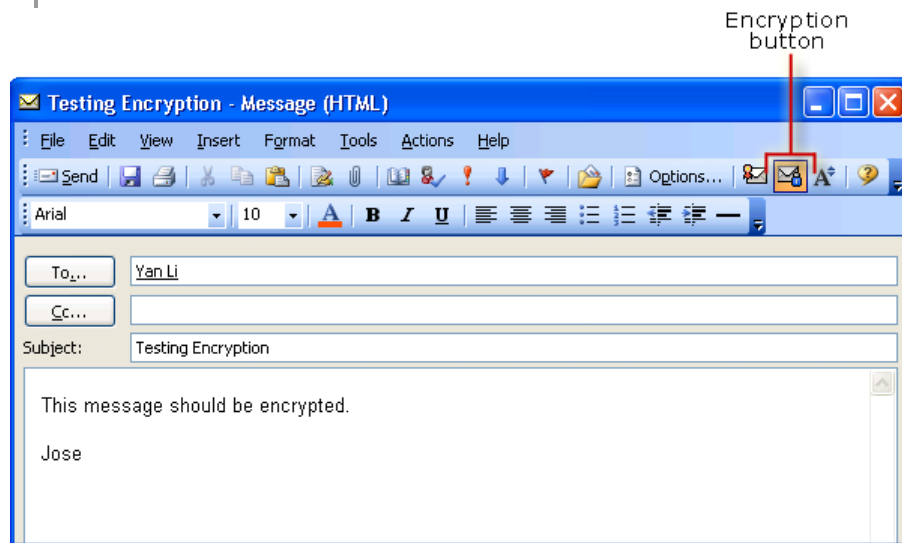
At this point, your digitally signed message has been sent to the recipient, who can then verify the digital signature.

### To send an encrypted message using Outlook

1. At the console, log on to CONT-WK01 as a member of the Domain Users group.
2. Click **Start**, point to **All Programs**, point to **Microsoft Office**, and then click **Microsoft Office Outlook 2003**.
3. To compose a new message, click **New**.
4. Add a recipient for the test message and fill out the message fields.

5. On the toolbar, ensure that the **Encrypt message contents and attachments** button is selected (see Figure 7). Because you want to test only encryption, ensure that the **Add digital signature to this message** button is not selected.

**Important** To successfully send an encrypted e-mail message, the recipient must already have a digital certificate. If you attempt to send an encrypted e-mail message to a user who does not have a digital certificate, you will receive an error. Make sure you have followed the instructions in the section "Requesting Digital Certificates for Users" for all your test users before sending e-mail messages to them.



**Figure 7 Encrypted message in Outlook**

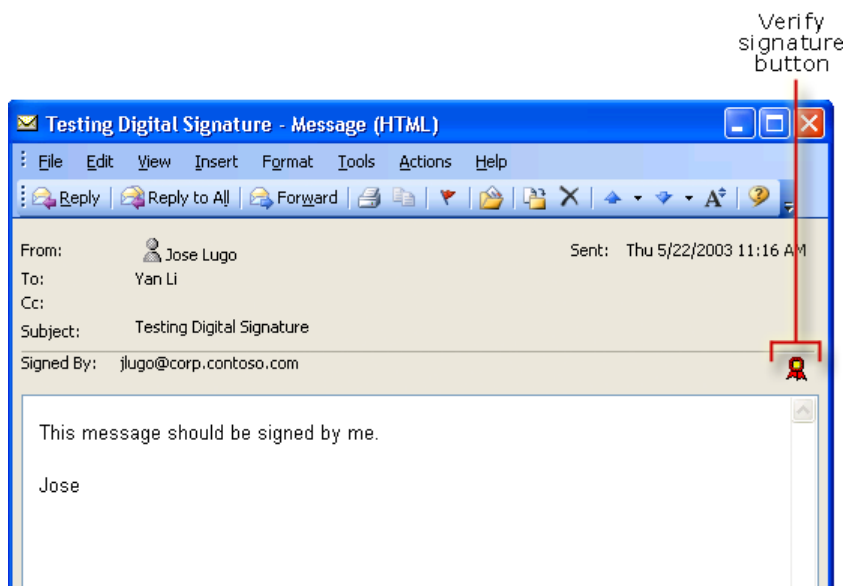
6. Click **Send**.

At this point, your encrypted message has been sent to the recipient, who can then open it and read it.

#### **To view a digitally signed message using Outlook**

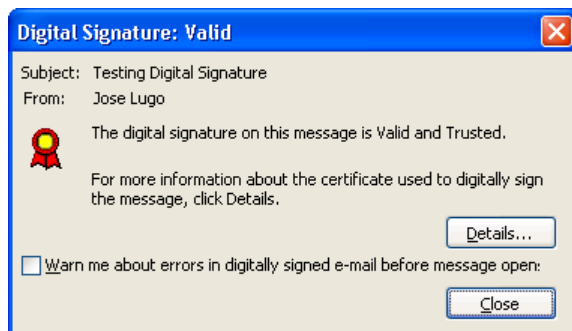
1. At the console, log on to CONT-WK01 as a member of the Domain Users group.
2. Click **Start**, point to **All Programs**, point to **Microsoft Office**, and then click **Microsoft Office Outlook 2003**.
3. In the **Inbox**, locate the digitally signed test message and double-click it.

- When the message opens, click the **Verify signature** button to verify the signature (see Figure 8).



**Figure 8 Verify signature button in Outlook**

- After you click the **Verify signature** button, the **Digital Signature** dialog box is displayed (see Figure 9), indicating that the digital signature is valid.



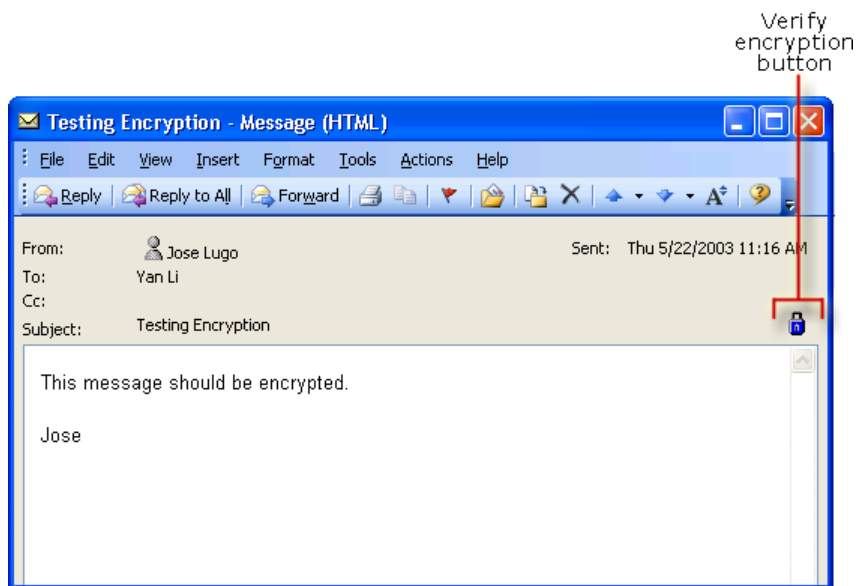
**Figure 9 Digital signature verified in Outlook**

At this point, you have verified the digital signature of the message.

### To view an encrypted message using Outlook

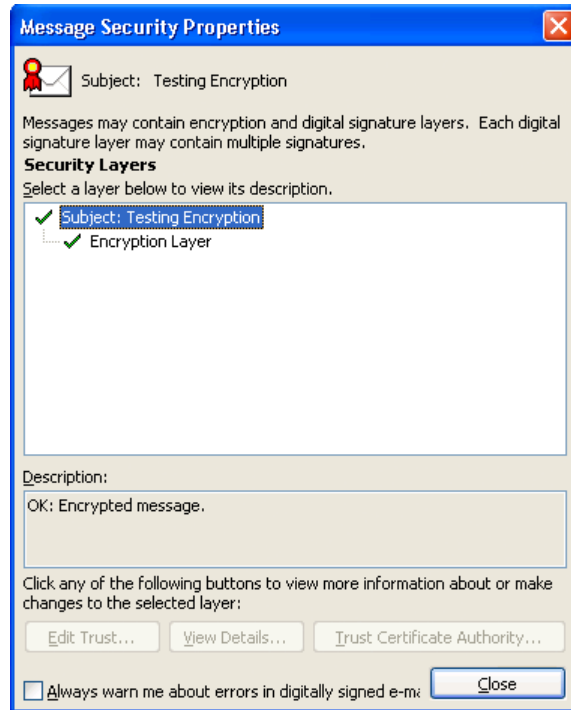
- At the console, log on to CONT-WK01 as a member of the Domain Users group.
- Click **Start**, point to **All Programs**, point to **Microsoft Office**, and then click **Microsoft Office Outlook 2003**.
- In the **Inbox**, locate the encrypted test message and double-click it.

4. When the message opens, click the **Verify encryption** button to verify the encryption (see Figure 10).



**Figure 10** Verify encryption button in Outlook

5. After you click the **Verify encryption** button, the **Message Security Properties** dialog box is displayed (see Figure 11), indicating that the encrypted message is valid.



**Figure 11 Encryption verified in Outlook**

At this point, you have verified the encryption of the message.

After you complete these steps, you will have tested all elements of using S/MIME in Outlook 2003. This information lets you see how an S/MIME system that uses Outlook will function for your users.

---

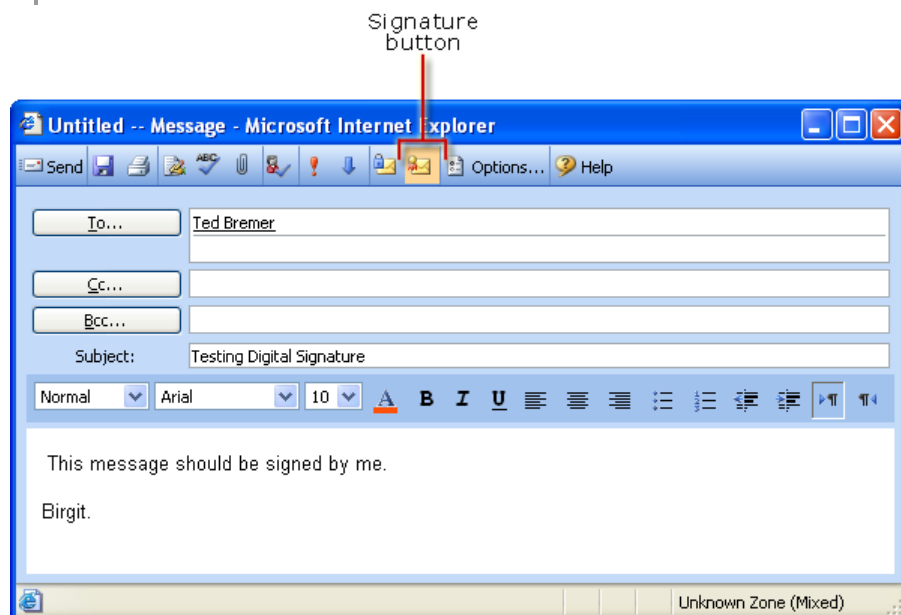
## Testing Digital Signatures and Encryption in Outlook Web Access

Using S/MIME in Outlook Web Access is similar to using S/MIME in Outlook. In both cases, the e-mail client uses digital certificates from the local certificate store (which you viewed using the MMC) and from Active Directory (which you viewed using Active Directory Users and Computers). Because of these similarities, users who are familiar with using S/MIME in Outlook should be able to transfer this knowledge to Outlook Web Access.

### To send a digitally signed message using Outlook Web Access

1. At the console, log on to CONT-WK01 as a member of the Domain Users group.
2. Click **Start**, point to **All Programs**, and then click **Internet Explorer**.
3. Click **File**, click **Open**, type `http://cont-ex01.corp.contoso.com/exchange` in the **Open** box, and then click **OK**.
4. Type the user name and password in the dialog box.
5. To compose a new message, click **New**.
6. Add a recipient for the test message and fill out the message fields.
7. On the toolbar, there are two new icons: one for encrypting and one for signing messages. Ensure that the **Add digital signature to this message** button is selected (see Figure 12). Because you want to test only digital signing, ensure that the **Encrypt message contents and attachments** button is not selected.

**Important** To successfully send an encrypted e-mail message, the recipient must already have a digital certificate. If you attempt to send an encrypted e-mail message to a user who does not have a digital certificate, you will receive an error. Make sure you have followed the instructions in the section "Requesting Digital Certificates for Users" for all your test users before sending an e-mail message to them.



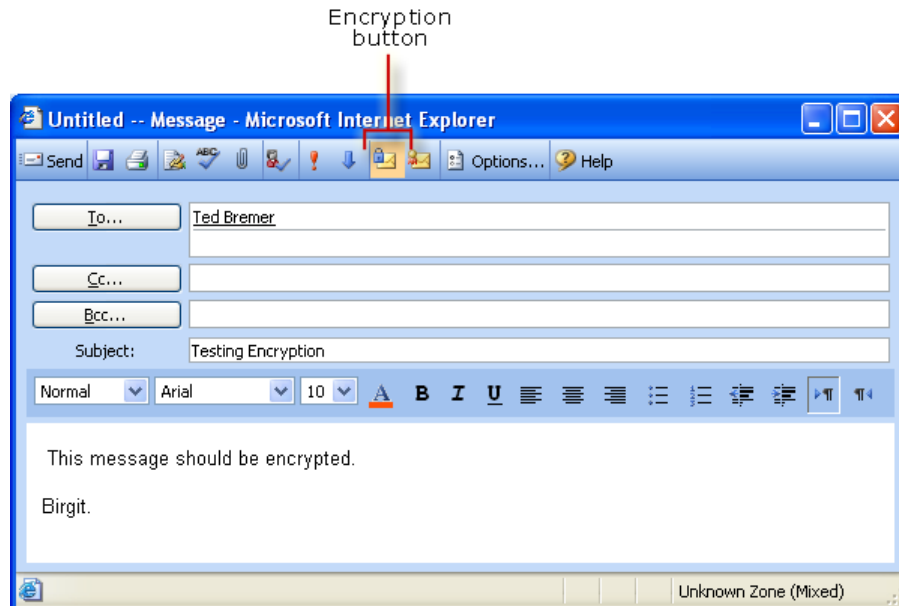
**Figure 12** Digitally signed message in Outlook Web Access

8. Click **Send**.

At this point, your digitally signed message has been sent to the recipient, who can then verify the digital signature.

### To send an encrypted message using Outlook Web Access

1. At the console, log on to CONT-WK01 as a member of the Domain Users group.
2. Click **Start**, point to **All Programs**, and then click **Internet Explorer**.
3. Click **File, Open** and type `http://cont-ex01.corp.contoso.com/exchange` in the **Open** box and click **OK**.
4. Type the user name and password in the dialog box.
5. To compose a new message, click **New**.
6. Add a recipient for the test message and fill out the message fields.
7. On the toolbar, ensure that the **Encrypt message contents and attachments** button is selected (see Figure 13). Because you want to test only encryption, ensure that that the **Add digital signature to this message** button is not selected.



**Figure 13 Encrypted message in Outlook Web Access**

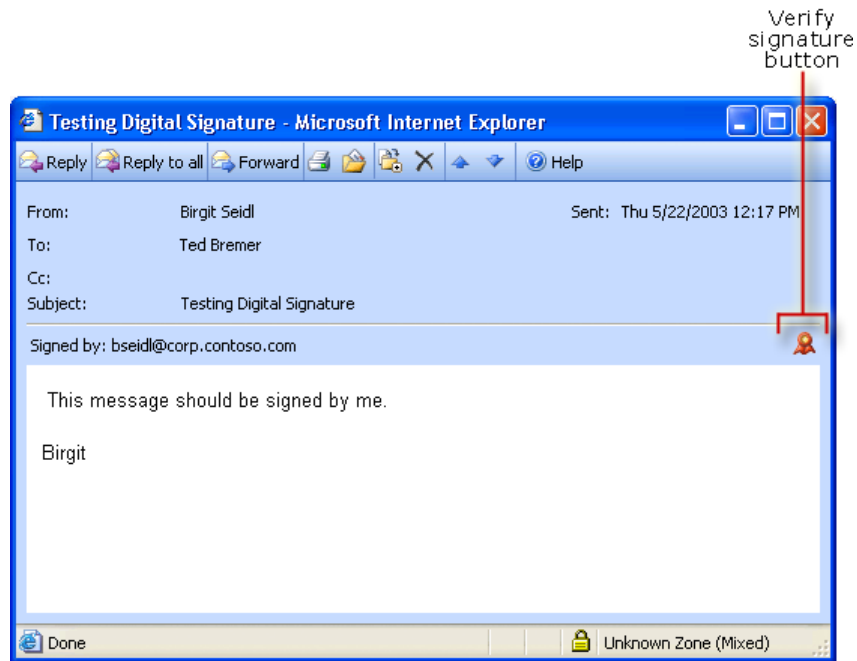
8. Click **Send**.

At this point, your encrypted message has been sent to the recipient, who can open it and read it.

### To view a digitally signed message using Outlook Web Access

1. At the console, log on to CONT-WK01 as a member of the Domain Users group.
2. Click **Start**, point to **All Programs**, and then click **Internet Explorer**.
3. Click **File**, click **Open**, type `http://cont-ex01.corp.contoso.com/exchange` in the **Open** box, and then click **OK**.
4. Type the user name and password in the dialog box.
5. In **Inbox**, locate the digitally signed test message and double-click it.

6. When the message opens, click the **Verify signature** button to verify the signature (see Figure 14)



**Figure 14** Verify signature button in Outlook Web Access

7. After you click the **Verify signature** button, the **Digital Signature** dialog box is displayed (see Figure 15), indicating that the digital signature is valid.



**Figure 15** Digital signature verified in Outlook Web Access

At this point, you have verified the digital signature of the message.

#### **To view an encrypted message using Outlook Web Access**

1. At the console, log on to CONT-WK01 as a member of the Domain Users group.
2. Click **Start**, point to **All Programs**, and then click **Internet Explorer**.



## Testing Digital Signatures and Encryption in Outlook Express

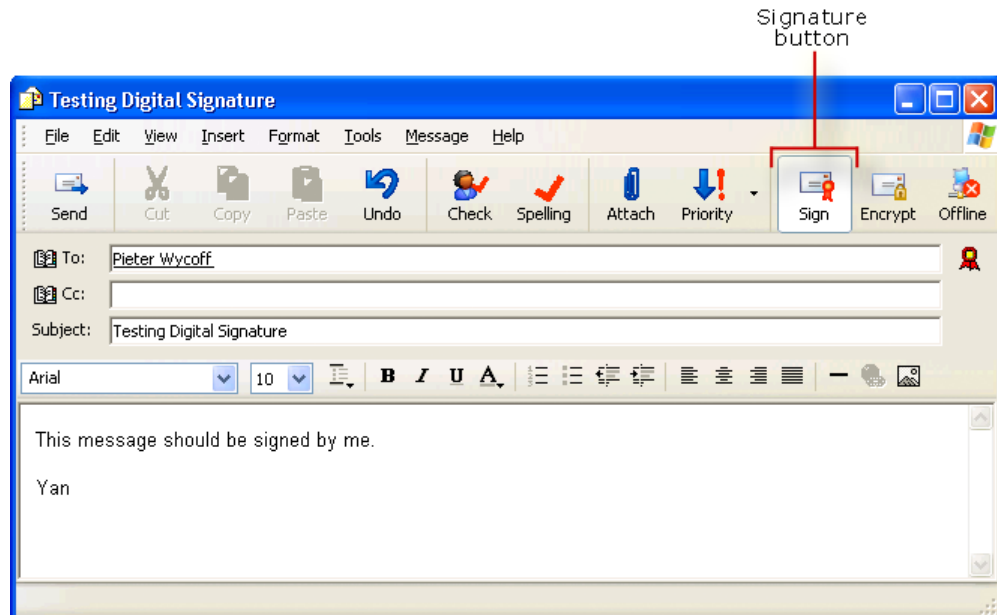
Unlike Outlook and Outlook Web Access, Outlook Express does not automatically use Active Directory to locate another user's e-mail addresses and digital certificates. Instead, Outlook Express uses the Windows Address Book. You can access information in Active Directory by using the search feature in Outlook Express, which is automatically configured to look up information in Active Directory. As an alternative, you can also populate the Windows Address Book with information about recipients before you send an e-mail message to them using Outlook Express.

**Note** If a user has more than one digital certificate in the local computer store, you must specify which digital certificate you want Outlook Express to use. To specify the certificate, click **Tools**, click **Accounts**, click the **Mail** tab, click **Properties**, click the **Security** tab, and then, under both **Signing certificate** and **Encrypting preferences**, click **Select**.

### To send a digitally signed message using Outlook Express

1. At the console, log on to CONT-WK01 as a member of the Domain Users group.
2. Click **Start**, point to **All Programs**, and click **Outlook Express**.
3. When prompted, type the user's password.
4. To compose a new message, click **Create Mail**.
5. To add a recipient from Active Directory, click **To**.
6. Under **Type name or select from list**, click **Find**.
7. In the **Look in** list, click **Active Directory**, type the name of the recipient in **Name**, and then click **Find Now**.
8. Select the name, and then click **To**.
9. Click **OK** to close the **Select Recipients** box.

- On the toolbar, there are two new icons: one for encrypting messages and one for signing messages. Ensure that the **Sign** button is selected (see Figure 17). Because you want to test only digital signing, ensure that the **Encrypt** button is not selected.



**Figure 17 Digitally signed message in Outlook Express**

- Click **Send**.

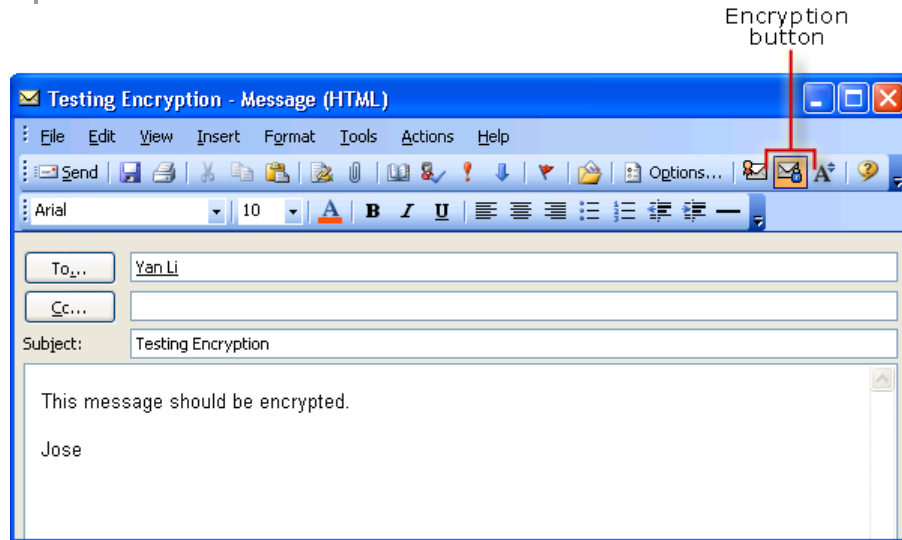
At this point, your digitally signed message has been sent to the recipient, who can verify the digital signature.

### To send an encrypted message using Outlook Express

- At the console, log on to CONT-WK01 as a member of the Domain Users group.
- Click **Start**, point to **All Programs**, and click **Outlook Express**.
- When prompted, type the user's password.
- To compose a new message, click **Create Mail**.
- To add a recipient from Active Directory, click **To**.
- Under **Type name or select from list**, click **Find**.
- In the **Look in** list, click **Active Directory**, type the name of the recipient in **Name**, and then click **Find Now**.
- Select the name, and then click **To**.
- Click **OK** to close the **Select Recipients** box.

10. On the toolbar, ensure that the **Encrypt** button is selected (see Figure 18). Because you want to test only encryption, ensure that the **Sign** button is not selected.

**Important** To successfully send an encrypted e-mail message the recipient must already have a digital certificate. If you attempt to send an encrypted e-mail message to a user who does not have a digital certificate, you will receive an error. Make sure you have followed the instructions in the section "Requesting Digital Certificates for Users" for all your test users before sending e-mail messages to them.



**Figure 18 Encrypted message in Outlook Express**

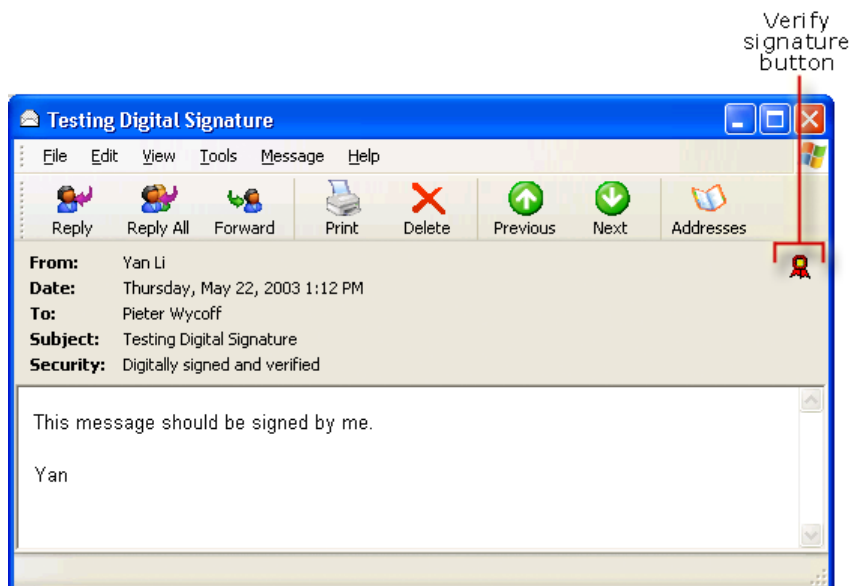
11. Click **Send**.

At this point, your encrypted message has been sent to the recipient, who can open it and read it.

#### **To view a digitally signed message using Outlook Express**

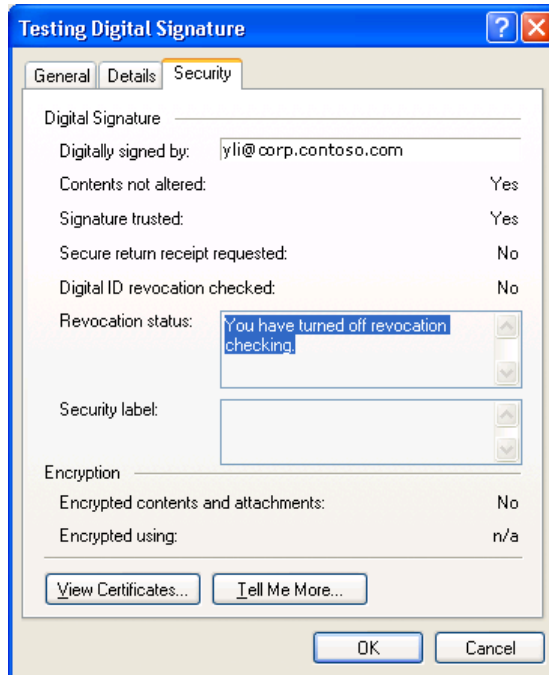
1. At the console, log on to CONT-WK01 as a member of the Domain Users group.
2. Click **Start**, point to **All Programs**, and click **Outlook Express**.
3. When prompted, enter the user's password.
4. In the **Inbox**, locate the digitally signed test message and double-click it.
5. When the message opens, Outlook Express displays a message explaining digital signatures. Select the **Don't show me this Help screen again** check box, and then click **Continue**.

6. To verify the signature, click the **Verify signature** button (see Figure 19).



**Figure 19** Verify signature button in Outlook Express

7. After you click the **Verify signature** button, the **Testing Digital Signature** dialog box is displayed (see Figure 20), indicating that the digital signature is valid.



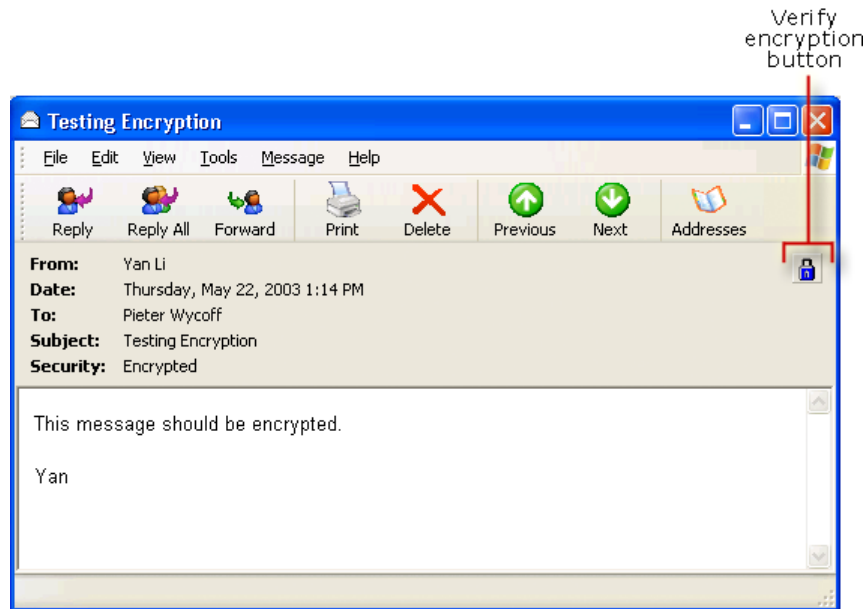
**Figure 20 Digital signature verified in Outlook Express**

At this point, you have verified the digital signature of the message.

### **To view an encrypted message using Outlook Express**

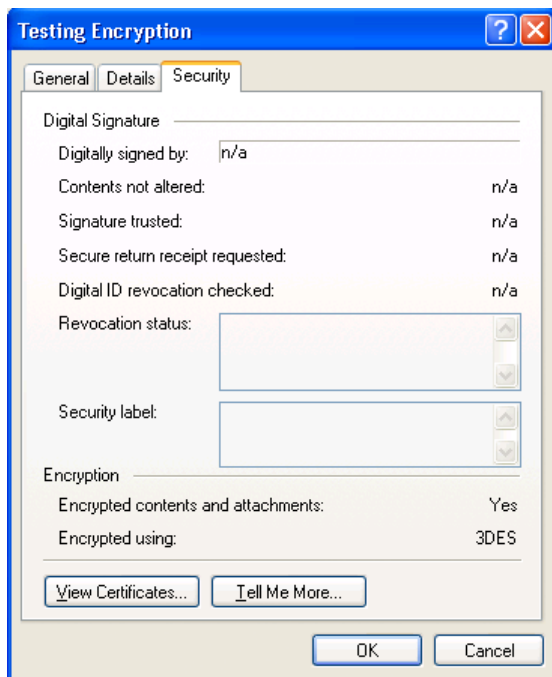
1. At the console, log on to CONT-WK01 as a member of the Domain Users group.
2. Click **Start**, point to **All Programs**, and click **Outlook Express**.
3. When prompted, enter the user's password.
4. In the **Inbox**, locate the encrypted test message and double-click it.
5. When the message opens, Outlook Express displays a message explaining encryption. Select the **Don't show me this Help screen again** check box, and then click **Continue**.

- To verify the signature, click the **Verify encryption** button (see Figure 21).



**Figure 21** Verify encryption button in Outlook Express

7. After you click the **Verify encryption** button, the **Testing Encryption** dialog box is displayed (see Figure 22), indicating that the encrypted message is valid.



**Figure 22 Encryption verified in Outlook Express**

At this point, you have verified the encryption of the message.

After you complete these steps, you will have tested all elements of using S/MIME in Outlook Express. This information lets you see how an S/MIME system that uses Outlook Express will function for your end-users.

## Conclusion

By following the steps in this technical article, you should have a fully functioning test environment that will enable you to see how an S/MIME system built on Exchange 2003 operates. This article also shows you how to perform some basic steps to understand S/MIME functionality:

- How certificates are issued
- How S/MIME clients use those certificates
- How to send and receive e-mail messages that have been signed and encrypted

After you complete the tasks described in this article, use your lab to learn more about the different parts of an S/MIME system through continued trial and experimentation. For example, you can use your lab to learn how certificate revocation and key recovery works in Certificate Services. For more information about these topics, see [Certificate Services Help](#).

## Additional Resources

---

### Windows Server 2003 Certification Authority

- Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure  
(<http://go.microsoft.com/fwlink/?LinkId=17800>)
  - Certificate Autoenrollment in Windows Server 2003  
(<http://go.microsoft.com/fwlink/?LinkId=17801>)
  - Implementing and Administering Certificate Templates in Windows Server 2003  
(<http://go.microsoft.com/fwlink/?LinkId=17802>)
  - Key Archival and Management in Windows Server 2003  
(<http://go.microsoft.com/fwlink/?LinkId=17803>)
  - Planning and Implementing Cross-Certification and Qualified Subordination Using Windows Server 2003  
(<http://go.microsoft.com/fwlink/?LinkId=17806>)
  - Windows Server 2003 PKI Operations Guide  
(<http://go.microsoft.com/fwlink/?LinkId=17807>)
- 

### Outlook 2003

- Overview of Cryptography in Outlook 2003  
(<http://go.microsoft.com/fwlink/?LinkId=17808>)
- 

### Other Web Sites

- Microsoft Baseline Security Analyzer  
(<http://go.microsoft.com/fwlink/?LinkId=17809>)

**Does this article help you?** Give us your feedback. On a scale of 1 (poor) to 5 (excellent), how do you rate this article?

Mail feedback to [exchdocs@microsoft.com](mailto:exchdocs@microsoft.com).

For the latest information about Exchange, see the following Web pages:

- Exchange Server 2003 Technical Library  
<http://www.microsoft.com/exchange/library>
- Exchange Server 2003 Tools and Updates  
<http://www.microsoft.com/exchange/updates>
- Exchange Technical White Papers (self-extracting executable)  
<http://go.microsoft.com/fwlink/?LinkId=10687>