CERTIFYING AUTHORITY

User Guide – Using Certificate in Microsoft Outlook 2000

CONFIDENTIAL

CONTACT

TATA CONSULTANCY SERVICES - [E-SECURITY: PKI SERVICES]

6TH FLOOR, 5-9-62, KHAN LATEEF KHAN ESTATE

FATEH MAIDAN ROAD, HYDERABAD - 500 001

TEL: +91 (40) 55671020 (D) / 5567000, EXT. - 1020

FAX: +91 (40) 55782930

WWW.TCS.COM / WWW.TCS-CA.TCS.CO.IN

Table of Contents

NOTICE OF PROPRIETARY INFORMATION

ALL INFORMATION CONTAINED IN OR DISCLOSED IN THIS DOCUMENT, HEREINAFTER CALLED 'CONFIDENTIAL INFORMATION'. BY ACCEPTING THIS MATERIAL, THE RECIPIENT AGREES THAT THIS CONFIDENTIAL INFORMATION WILL BE HELD IN CONFIDENCE, AND WILL NOT BE REPRODUCED, DISCLOSED OR USED EITHER IN WHOLE OR IN PART, WITHOUT PRIOR PERMISSION FROM TATA CONSULTANCY SERVICES.

DESCRIPTION

This guide explains the procedure for using the TCS-CA issued digital certificate in Microsoft Outlook 2000.

MICROSOFT OUTLOOK 2000 AND CERTIFICATES

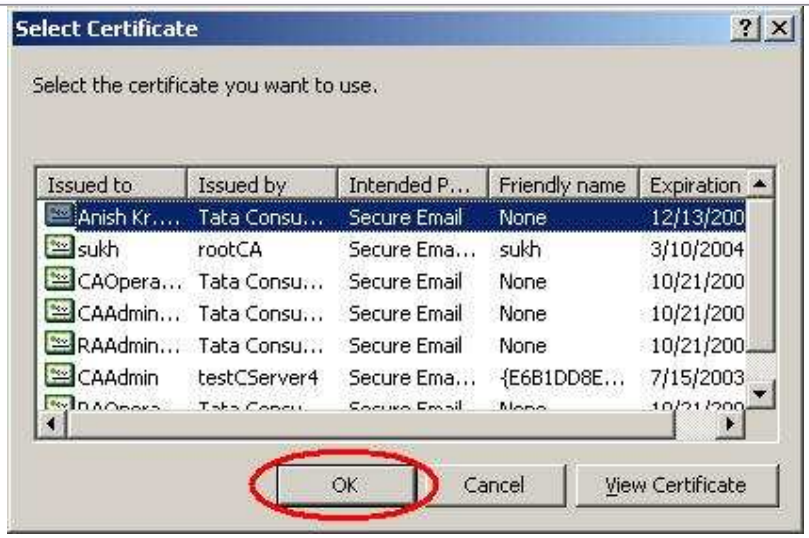
Microsoft Outlook 2000 supports a standard called Secure Multi-Purpose Internet Mail Extensions (S/MIME), which uses RSA encryption technology. At the core of any S/MIME client, the sender will find support for the Public Key Cryptography Standards (PKCS). S/MIME clients (including Outlook 98 and Netscape Communicator) use the PKCS #7 Cryptographic Message Syntax, which defines the basic structure of the digital signature and envelope.

SETTINGS TO CHOOSE VALID DIGITAL CERTIFICATES

1. Select **Options…** from the **Tools** menu.
2. Select the **Security** tab of the **Options** dialog.

3. Click on the “Setup Secure Email” tab as shown in the above screen-shot.
4. You will be displayed the Security Settings page as follows

5. Enter some name for the Security Settings
6. Click on the Choose button for the Signing Certificate as shown in the above screen-shot for choosing your signing certificate.
7. You will be given a list of Signing Certificates installed in your IE browser to choose from. Select your signing certificate and click on “OK”.

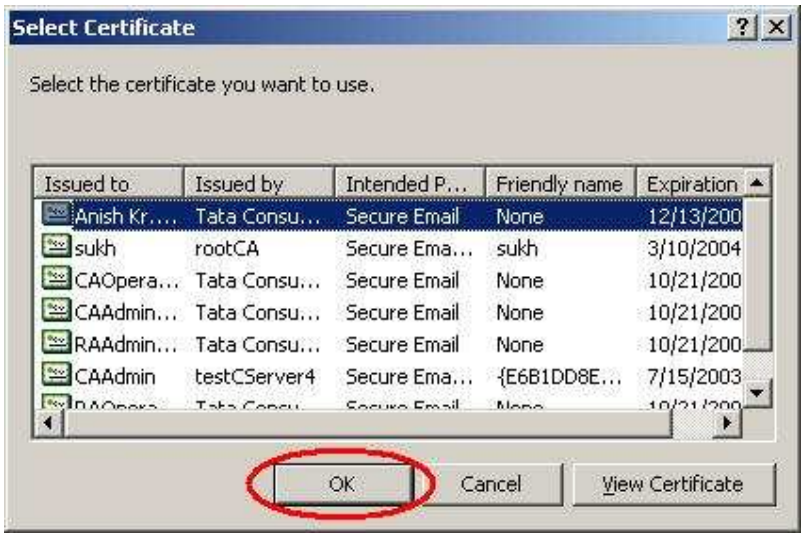


Please Note : The email address in the certificate should match your Microsoft Outlook email account.

8. Your signing certificate will be selected. Then click on the Choose button for encryption certificate as shown in the above screen-shot for choosing your encryption certificate.

9. You will be given a list of Signing Certificates installed in your IE browser to choose from. Select your signing certificate and click on “OK”.

Please Note : The email address in the certificate should match your Microsoft Outlook email account.



10. Your signing certificate will be selected.
11. Please check the box to send these certificates with signed messages.

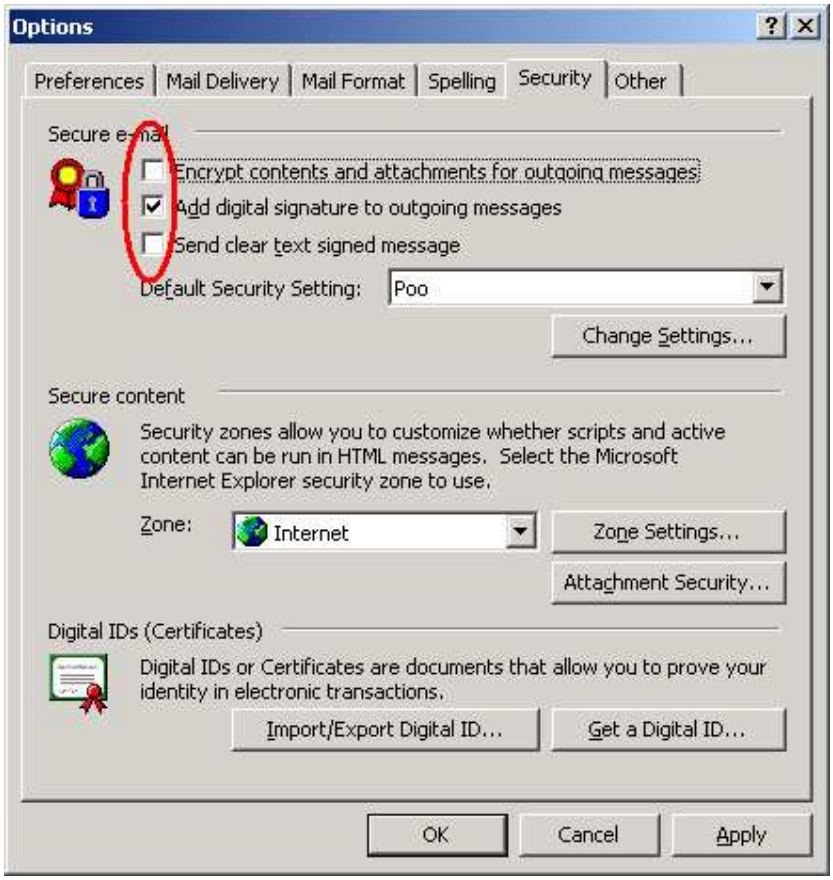

Change Security Settings
Security Setting Preferences
Security Settings Name:
Anish
Secure Message Format:
S/MIME
Default Security Setting for this Secure Message Format
Default Security Setting for all secure messages
Security Labels...
New
Delete
Password...
Certificates and Algorithms
Signing Certificate:
Anish Kr. Srivastava
Choose...
Hash Algorithm:
SHA1
Encryption Certificate:
Anish Kr. Srivastava
Choose...
Encryption Algorithm:
3DES
Send these certificates with signed messages
OK
Cancel

ENABLING SECURITY SETTINGS FOR MAIL ACCOUNT

Following steps will enable signing and encrypting all the outgoing messages from the sender's account. Before that you need to install the required certificates in the IE browser. Make sure both the Signing and Encryption certificates are installed in the IE browser (Personal Store)

SETTINGS TO SIGN AND ENCRYPT ALL OUTGOING MESSAGES

1. Select **Options…** from the **Tools** menu.
2. Select the **Security** tab of the **Options** dialog.
3. Check **Digitally sign all outgoing messages** so that it is turned on.



Note: Microsoft Outlook 2000 includes the option to digitally sign and/or encrypt all the outgoing messages. The sender shall confirm that most of the sender's correspondents use mail software that can

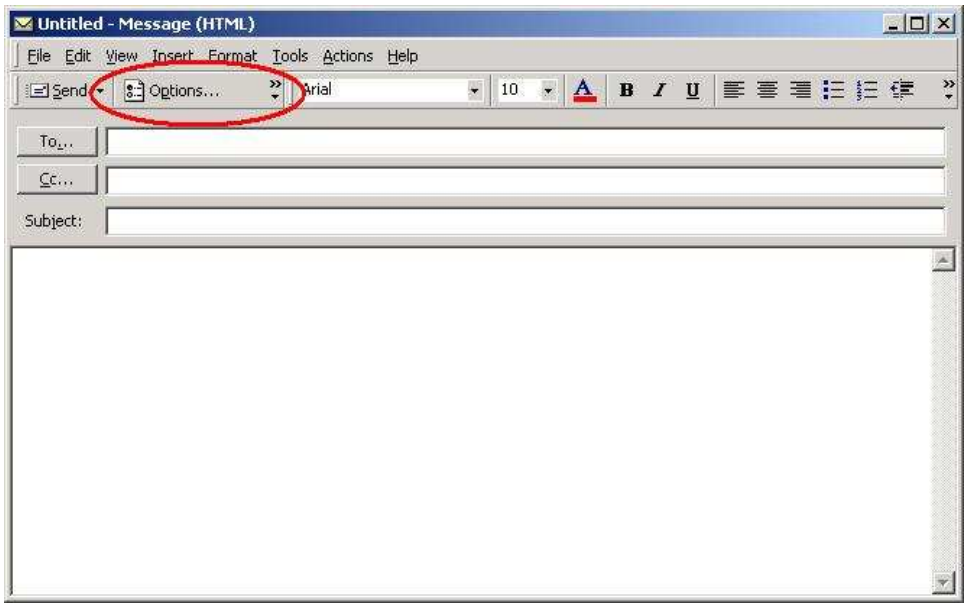
accept digital certificates, while configuring this option. For the overwhelming majority of email users, it's best to choose secure email option one message at a time.

Note: While sending mails if the sender's digital certificate does not exist, Outlook will warn that the message cannot be signed and prompt if the user wants to send an unsigned message instead. **Similarly while encrypting the message, if the recipient's digital certificate is not available the Outlook warns that the certificate is not available and if the user wants to send the message as an unencrypted message.**

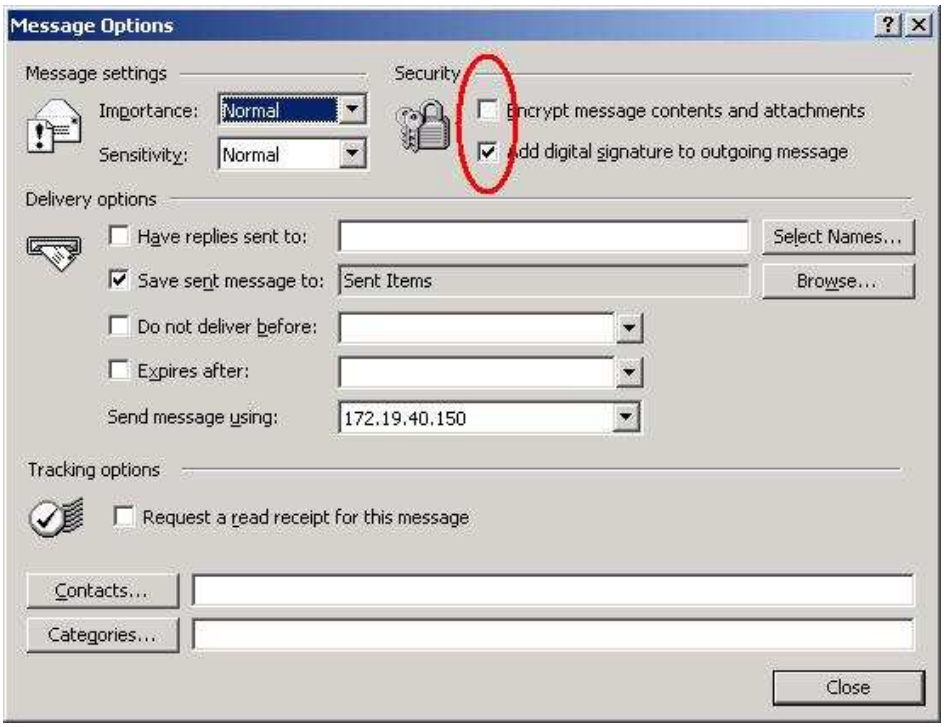
SENDING INDIVIDUAL SIGNED AND ENCRYPTED OUTGOING MESSAGES

Incase the sender does not want to activate the option to sign and encrypt all outgoing messages but wants to sign/encrypt certain outgoing messages, it is possible with Microsoft Outlook 2000.

1. Create a new email by clicking on the **New Mail** button.
2. The **New Message** composition window will open.
3. Click on the **Options button from the menu bar.**



4. Check the boxes for Signing/Encrypting the mail as required.



5. Close the dialogues.
6. Click on the send button to send the message.
7. If you have chosen the encryption option and don't have the encryption certificate for the recipient, then the message will not be encrypted. The following dialogue will be shown.

8. Click on Send Unencrypted button. In this case, the mail will be digitally signed but not encrypted.

When the sender send a signed email, the sender's private key is used to digitally sign the message. Depending on the private key security level the sender established when the sender first installed the sender's personal digital certificate, when the sender click on the *Send* button, the sender may receive

either an **OK/Cancel** prompt or a prompt for the sender's private key password. If the sender selected a private key security level of *"Low",* the message will be sent without warnings or prompts.

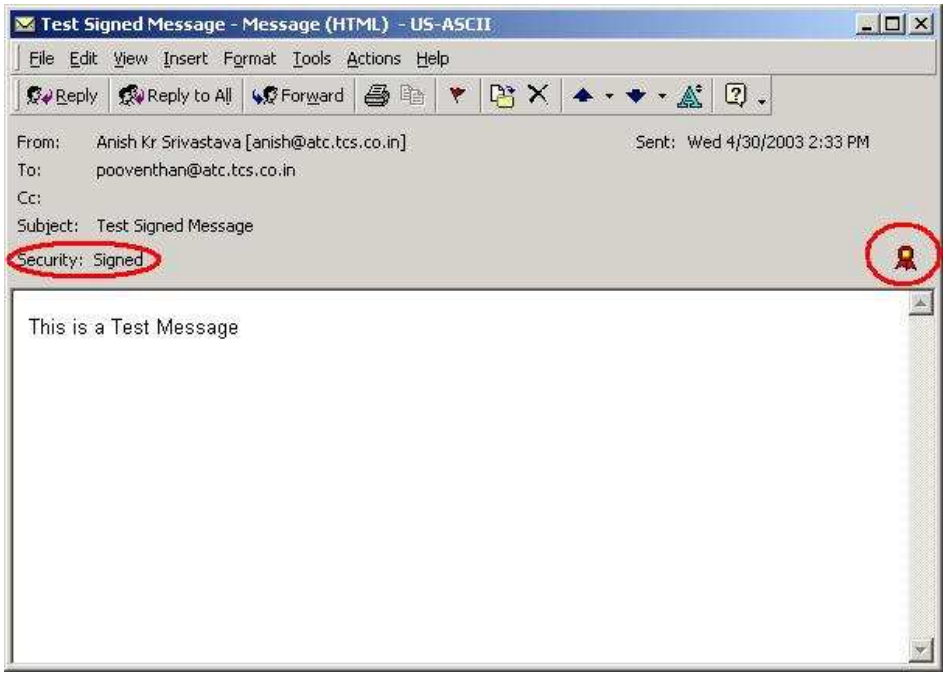
The sender can send encrypted email to anyone who has a digital certificate. Simply ask the sender's correspondent to send the sender a signed email or the certificate file as an attachment. Once the sender has received a signed email, the sender's email program will store the sender correspondent's digital certificate in the sender's email address book. Once the sender have the other persons digital certificate in the sender's email address book, the sender can encrypt all email to the correspondent.

RECEIVING SIGNED MESSAGE OR ENCRYPTED MESSAGE

While receiving signed messaged from others, the receiver can click on the **from** name at the top of the message using the **right mouse button** and can add the other's digital certificate to the address book. When this is done the certificate and public key information is stored in the address book and you will be now able to send encrypted email to this person.

When the user receives a signed message, the recipient email program uses the public key attached with the message to verify the signature.

When the sender receives email, which is signed, and/or encrypted, the message will have the appropriate icon attached to it. The following is a typical signed mail.



The red icon indicates that the message is a signed message.

The blue padlock indicates that it is an encrypted mail. The receiver can click on these icons to examine the details of the certificate used to sign and/or encrypt this message. The following is the screenshot for the signed mail.


Digital Signature: Valid
Message: Test Signed Message
This message is digitally signed by:
C=IN; S=Andhra Pradesh; L=Hyderabad; OU=Class 3 Certificate; OU=ATC; O=India PKI; O=Tata Consultancy Services;
Signature: Valid
Contents not altered after message was signed
Certificate not revoked
Certificate not expired
Certificate trusted
Always warn me before opening messages with invalid signatures
View Certificate...
Edit Trust...
OK