NICCA User Guide for digitally signing email
Using Digital Signature Certificate (DSC) in Outlook Express

1. DESCRIPTION

This guide explains the procedure for using the NICCA issued digital certificate in Microsoft Outlook Express.

2. OUTLOOK EXPRESS AND CERTIFICATES

If the sender has multiple mail accounts configured in his/her Outlook Express, the sender will need a separate certificate for each one because each certificate is tied to a unique email address. Outlook Express automatically selects the correct certificate based on the account the sender uses to send messages.

3. ENABLING SECURITY SETTINGS FOR MAIL ACCOUNT

Ensure that the required certificates are present in the IE browser certificate store.

1. Select **Tools > Internet options**
2. Click **Content** Tab
3. Click **Certificate** Button
4. Under **Personal Certificates** the account certificate must be present.

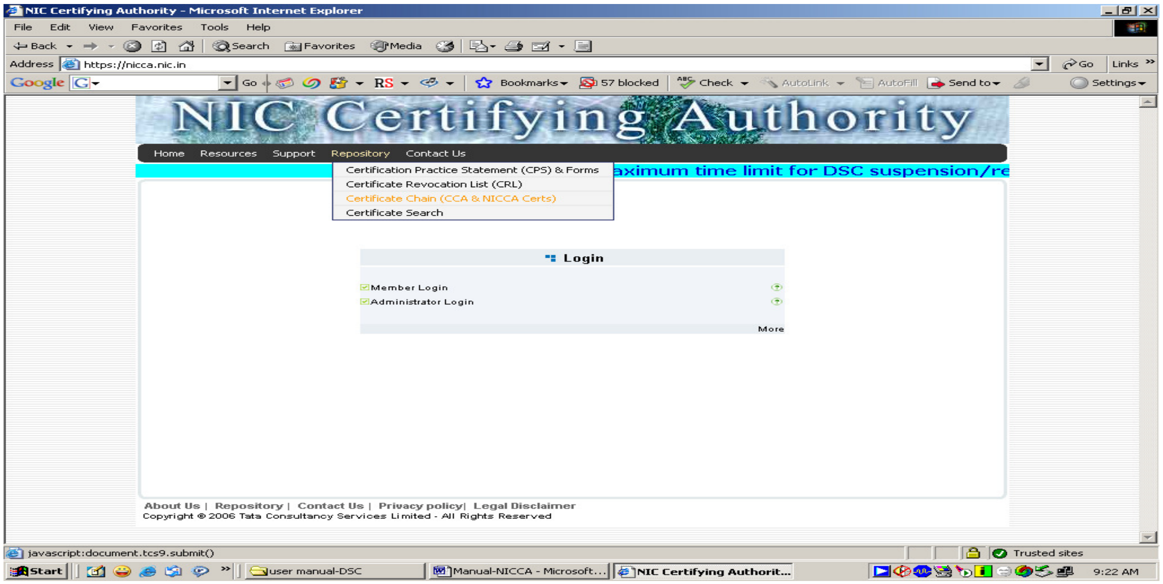
Following steps will enable signing and encrypting all the outgoing messages from the sender’s account.

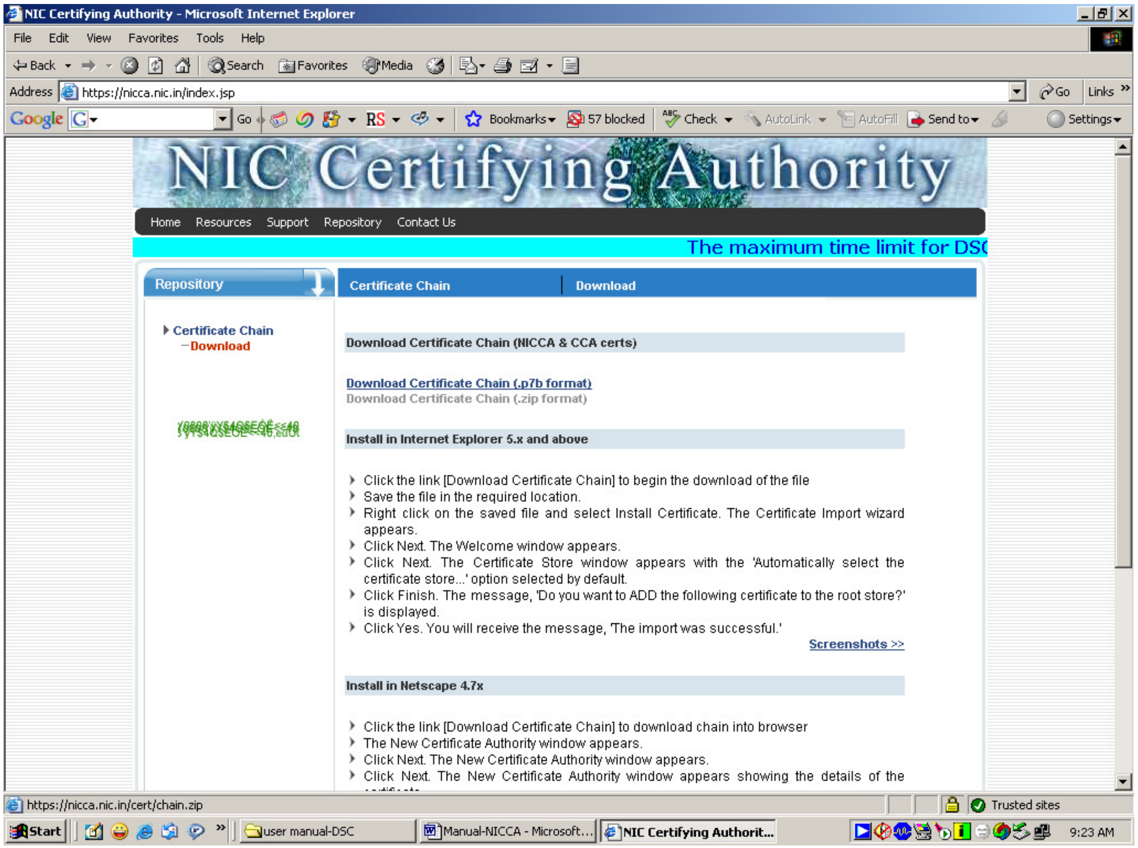
1. Select Options… from the Tools menu.
2. Select the Security tab of the Options dialog.
3. Check Digitally sign all outgoing messages so that it is turned on.
4. Click on OK to dismiss the Options dialog.

3.1 DOWNLOADING & INSTALLING CHAIN CERTIFICATES

Note: For Users having Internet Explorer 6 or 7 Please import the certificate chain using the following procedure.

Download chain.zip file from Repository tab on website https://nicca.nic.in. Click on Certificate Chain (CCA & NICCA Certs)>Download>Download Certificate Chain (.zip format). Unzip chain.zip file and extract **chain2.p7b** from chain.zip file on Desktop.


NIC Certifying Authority - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://nicca.nic.in
Go Links
NIC Certifying Authority
Home Resources Support Repository Contact Us
Certification Practice Statement (CPS) & Forms
Certificate Revocation List (CRL)
Certificate Chain (CCA & NICCA Certs)
Certificate Search
aximum time limit for DSC suspension/re
Login
Member Login
Administrator Login
More
About Us | Repository | Contact Us | Privacy policy | Legal Disclaimer
Copyright © 2006 Tata Consultancy Services Limited - All Rights Reserved
javascript:document.tcs9.submit()
Trusted sites
Start
user manual-DSC
Manual-NICCA - Microsoft...
NIC Certifying Authorit...
9:22 AM


NIC Certifying Authority - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://nicca.nic.in/index.jsp
Go Links
NIC Certifying Authority
Home Resources Support Repository Contact Us
The maximum time limit for DSC
Repository
Certificate Chain
—Download
Certificate Chain Download
Screenshots >>
https://nicca.nic.in/cert/chain.zip
Trusted sites
Start user manual-DSC Manual-NICCA - Microsoft... NIC Certifying Authorit... 9:23 AM

Download Certificate Chain (NICCA & CCA certs)

Download Certificate Chain (.p7b format)
Download Certificate Chain (.zip format)

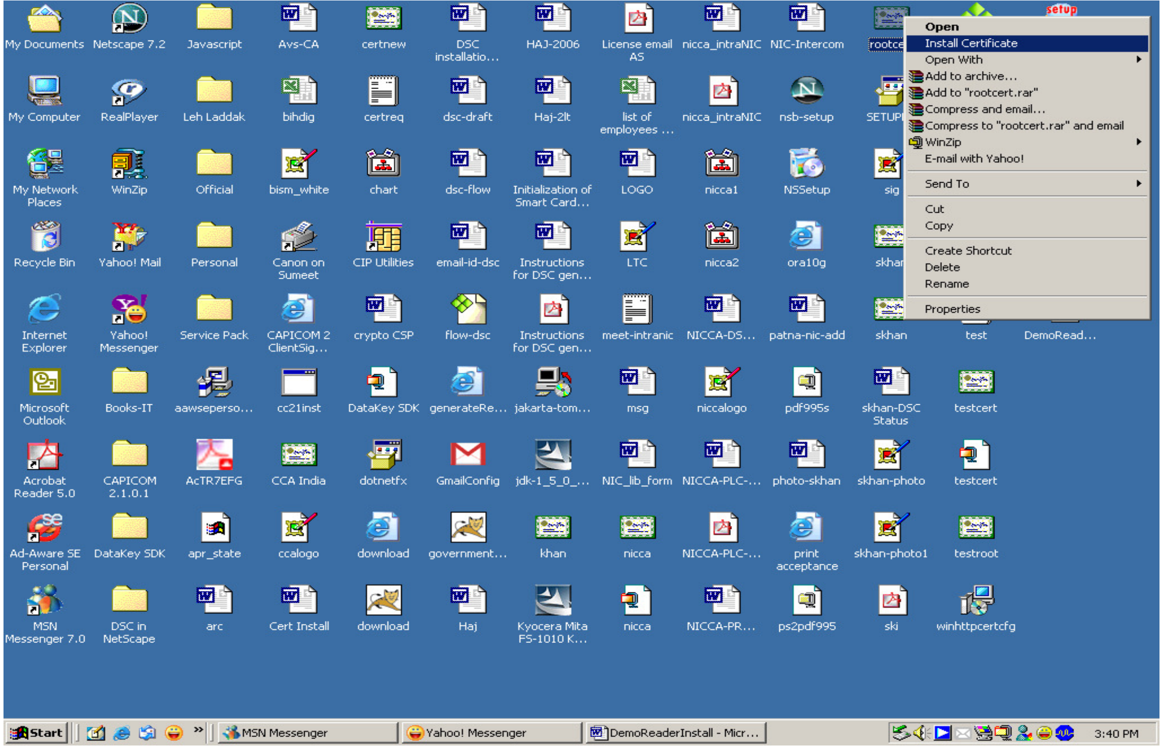
Install in Internet Explorer 5.x and above

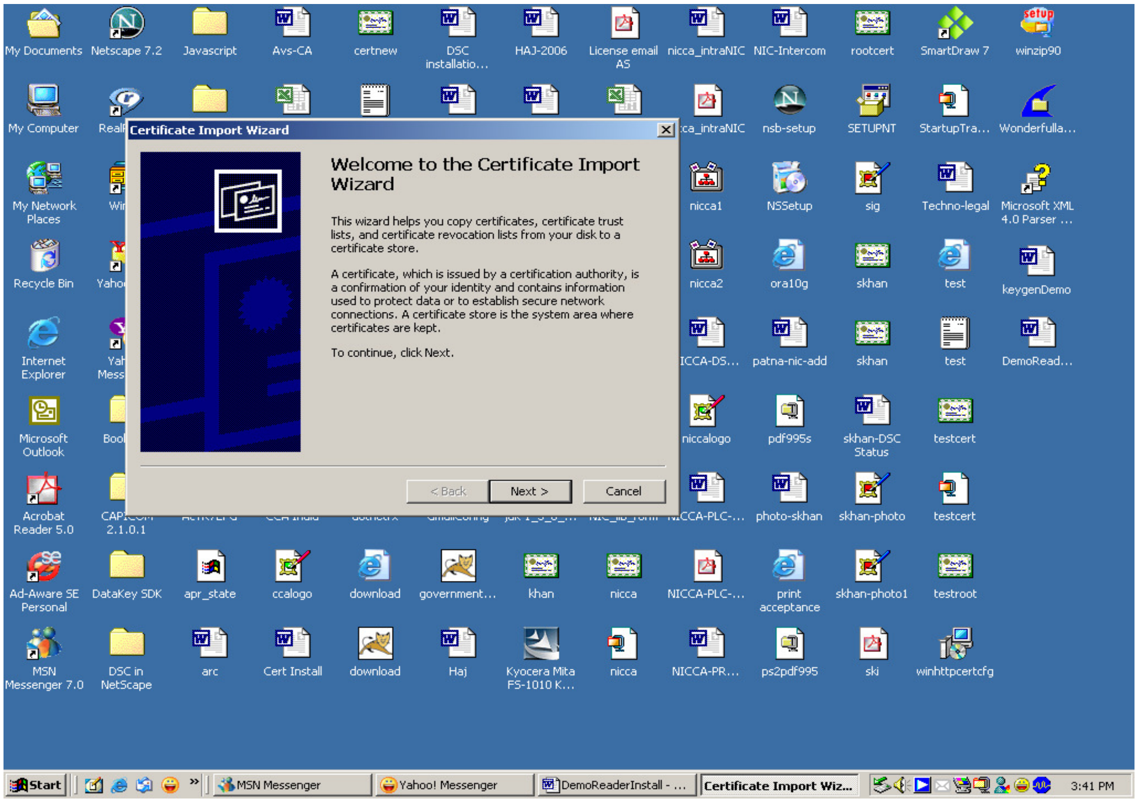
- Click the link [Download Certificate Chain] to begin the download of the file
- Save the file in the required location.
- Right click on the saved file and select Install Certificate. The Certificate Import wizard appears.
- Click Next. The Welcome window appears.
- Click Next. The Certificate Store window appears with the 'Automatically select the certificate store...' option selected by default.
- Click Finish. The message, 'Do you want to ADD the following certificate to the root store?' is displayed.
- Click Yes. You will receive the message, 'The import was successful.'

Install in Netscape 4.7x

- Click the link [Download Certificate Chain] to download chain into browser
- The New Certificate Authority window appears.
- Click Next. The New Certificate Authority window appears.
- Click Next. The New Certificate Authority window appears showing the details of the

Right Click on **chain2.p7b** file on Desktop & Click **Install Certificate** & click **Next, Next & Finish.**



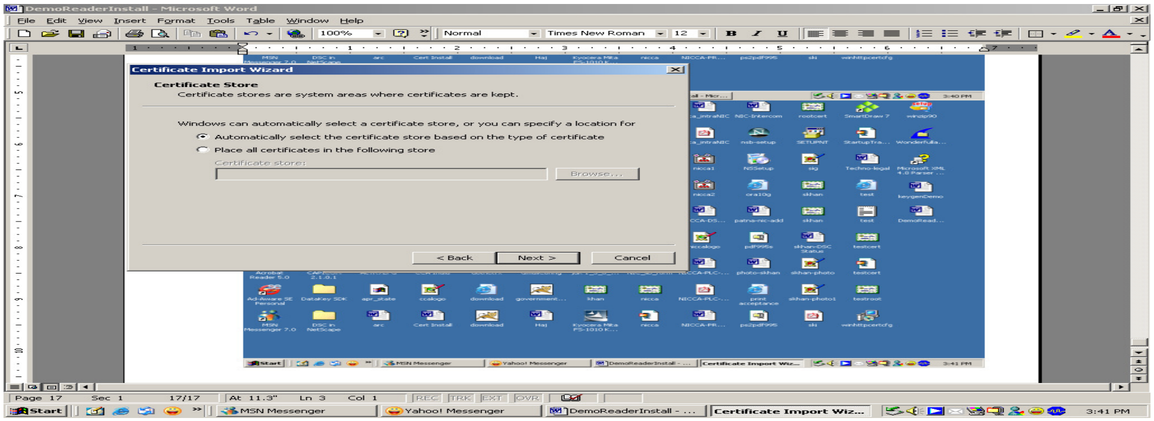


Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.



Certificate Store

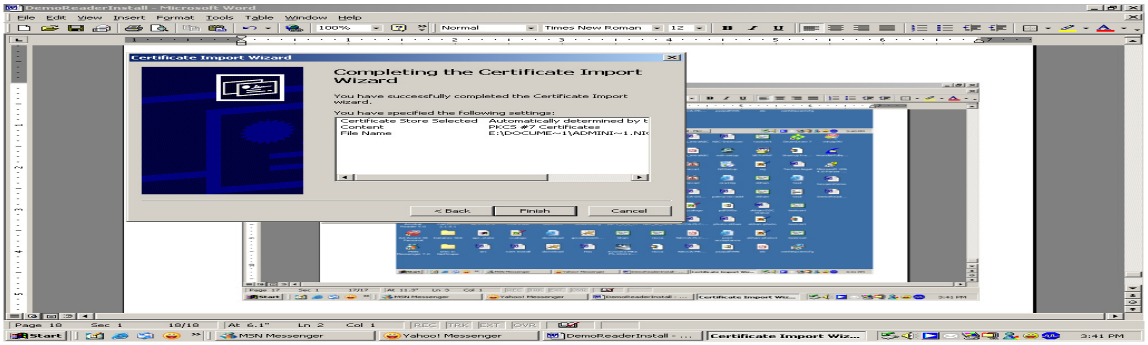
Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:



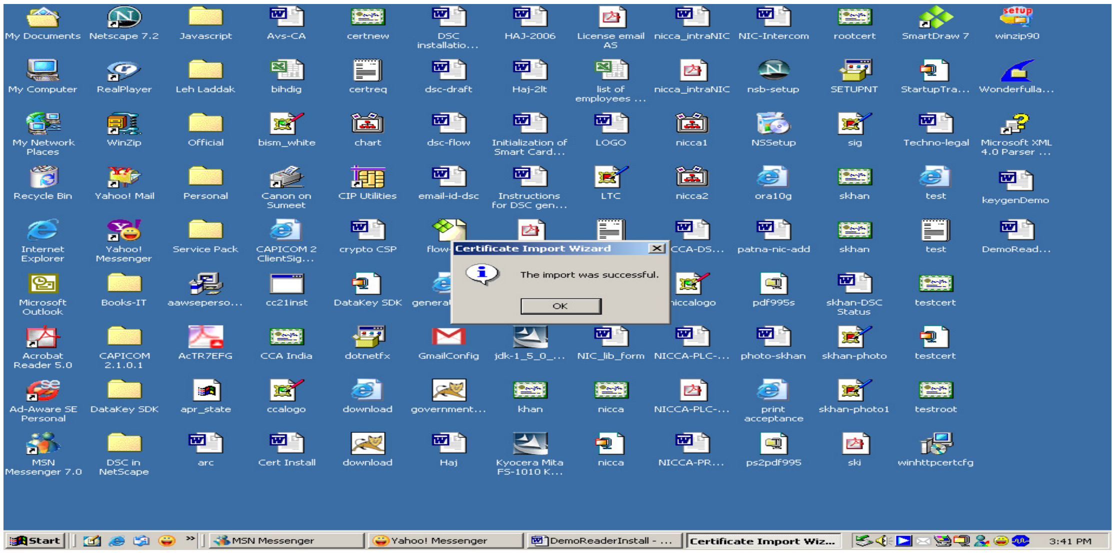
Completing the Certificate Import Wizard

You have successfully completed the Certificate Import wizard.

You have specified the following settings:

```
Certificate Store Selected    Automatically determined by t
Content                       PKCS #7 Certificates
File Name                     E:\DOCUME~1\ADMINI~1.NI
```

Click **OK**



Certificate Import Wizard

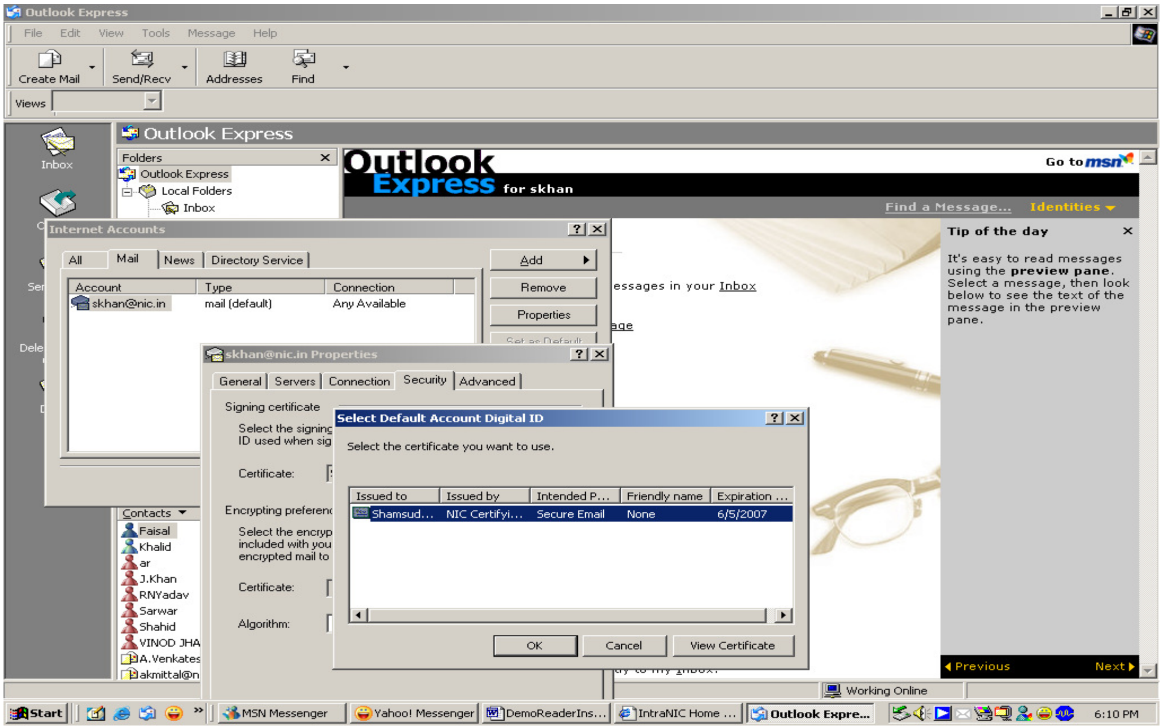
The import was successful.

3.2 SETTINGS TO CHOOSE A VALID DIGITAL CERTIFICATE

1. Select your mails account and select Properties for that account for which the sender has obtained Digital Certificate.
2. Select the Security tab of the Properties dialog.
3. Click on the Signing Certificate - Select… button.
4. Select the certificate the sender wants to use from the Select Certificate dialog, then click on OK.

The user's mail account is now configured and ready for use in Outlook Express!

Configure your email-id (same as email-id in the DSC) in the Outlook Express, insert your smart card in the reader/ikey token in USB & select the Certificate from **OE>Tools>Accounts>Mail>Properties>Security>Signing Certificate Select>OK**



Account	Type	Connection
skhan@nic.in	mail (default)	Any Available

Select the signing ID used when sig

Select the encryp included with you encrypted mail to

Select the certificate you want to use.

Issued to	Issued by	Intended P...	Friendly name	Expiration ...
Shamsud...	NIC Certifyi...	Secure Email	None	6/5/2007

Tip of the day

It's easy to read messages using the **preview pane**. Select a message, then look below to see the text of the message in the preview pane.

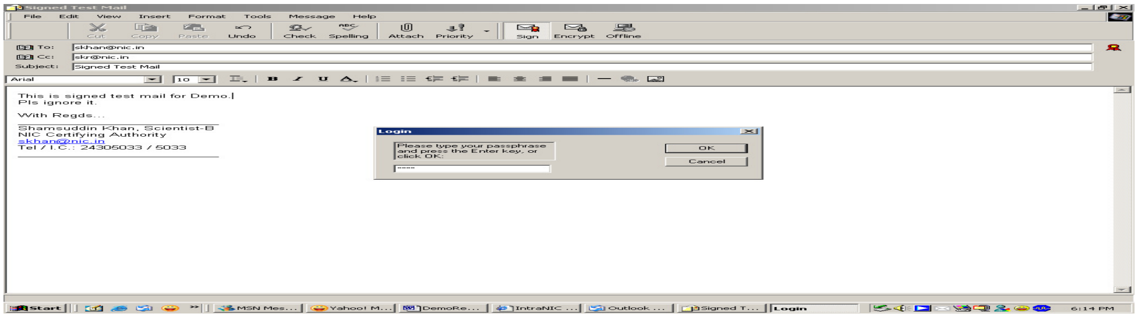
4. SENDING & RECEIVING SIGNED EMAIL IN OUTLOOK EXPRESS

Incase the sender does not want to activate the option to sign and encrypt all outgoing messages but wants to sign certain outgoing messages, it is possible with Outlook Express. The sender has the option of only signing the message to authenticate to the recipient the identity of the sender. Here the private key of the sender is used to sign the message and a copy of the digital certificate (containing the public key of sender) is send along with the message.

1. Create a new email by clicking on the New Mail button.
2. The New Message composition window will open.
3. Click on the Sign button in the menu bar or select the Digitally Sign item from the Tools menu as in the figure.

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.
1. Select Accounts… from the Tools menu.
2. Select the Mail tab of the Accounts dialog.

Click **Create Mail** on OE and Click **Sign** toggle on-off button **ON.**
Write Message & Click **Send**, OE will ask to enter passphrase/PIN of Smart Card/USB Token in the new window as below:


Signed Test Mail
File Edit View Insert Format Tools Message Help
Cut Copy Paste Undo Check Spelling Attach Priority Sign Encrypt Offline
Arial 10
Login
OK
Cancel
Start

To: skhan@nic.in
Cc: skr@nic.in
Subject: Signed Test Mail

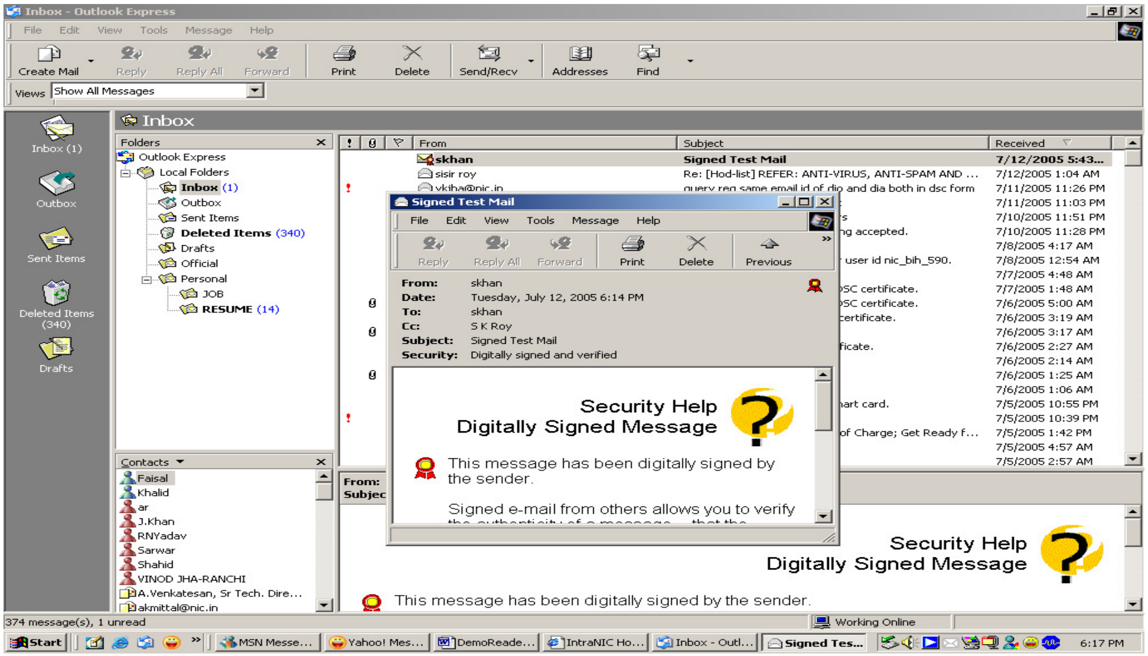
This is signed test mail for Demo.
Pls ignore it.

With Regds...

Shamsuddin Khan, Scientist-B
NIC Certifying Authority
skhan@nic.in
Tel / I.C.: 24305033 / 5033

Please type your passphrase and press the Enter key, or click OK:

Enter **passphrase/PIN** (by default: PASSWORD or 1234) to send the message. Click **Send/Recv** to get the new message on OE. Select the new message to read.



From	Subject	Received
skhan	Signed Test Mail	7/12/2005 5:43…
sisir roy	Re: [Hod-list] REFER: ANTI-VIRUS, ANTI-SPAM AND …	7/12/2005 1:04 AM
vkjha@nic.in	query reg same email id of dio and dia both in dsc form	7/11/2005 11:26 PM

From: skhan
Date: Tuesday, July 12, 2005 6:14 PM
To: skhan
Cc: S K Roy
Subject: Signed Test Mail
Security: Digitally signed and verified

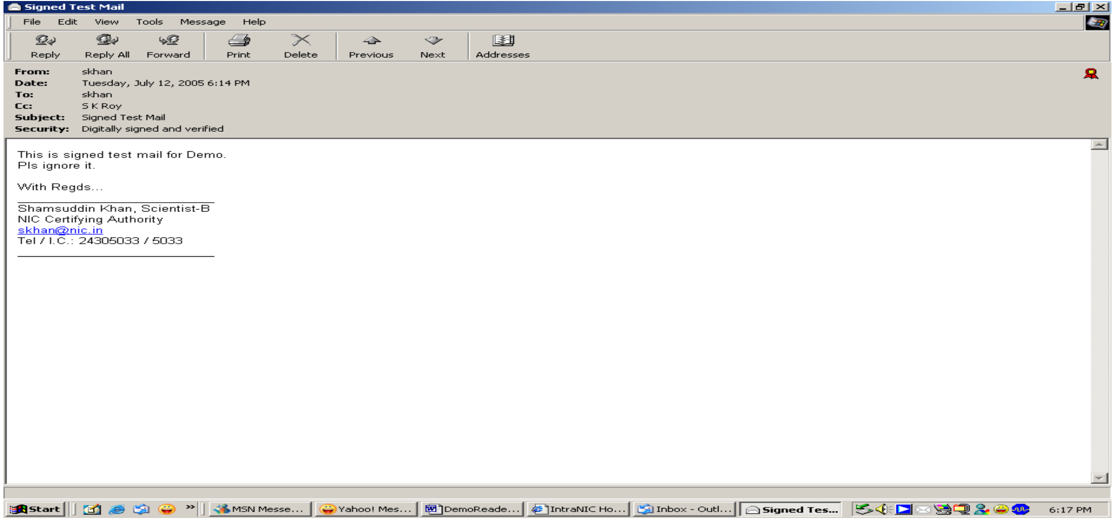
Security Help
Digitally Signed Message

This message has been digitally signed by the sender.

Signed e-mail from others allows you to verify

374 message(s), 1 unread

Click **Continue** to view the message.



From: skhan
Date: Tuesday, July 12, 2005 6:14 PM
To: skhan
Cc: S K Roy
Subject: Signed Test Mail
Security: Digitally signed and verified

This is signed test mail for Demo.
Pls ignore it.

With Regds...

Shamsuddin Khan, Scientist-B
NIC Certifying Authority
skhan@nic.in
Tel / I.C.: 24305033 / 5033

4.1 SENDING SIGNED MESSAGE

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 by clicking on the encrypt button.

4.2 SENDING ENCRYPT ED MESSAGE

1. Create a new email by clicking on the New Mail button. The New Message composition window will open.
2. Click on the Encrypt button in the menu bar or select the Encrypt item from the Tools menu as shown below.

Note: The sender is only able to encrypt this email if the sender has the public key of the recipient. If the sender attempt to send an encrypted email to someone for whom the sender do not have a public key, Outlook Express will warn the sender that this is not possible and offer the sender the choice of sending unencrypted or not sending.

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.

4.3 RECEIVING SIGNED MESSAGE

When the user receives a signed message, Outlook Express 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.

5. MANAGING DIGITAL CERTI FICATES WITH OUTLOOK EXPRESS

Sending an encrypted message to a correspondent requires the sender to have a copy of their digital certificate. The easiest way to get a copy of someone's digital certificate is to get them to send the sender a digitally signed message incase the encryption and signing certificates are the same. Else he sends the certificate attached to the mail. To store a contact's digital certificate:

1. Open the signed message from Outlook Express.
2. From the File menu select Properties.
3. Click the Security tab.
4. Click View Certificates.
5. Click the Add to Address Book button.

To import someone's digital certificate that exists in a directory or on the user's hard-drive, download the digital certificate, and add it to the Outlook's address book:

1. Select an address
2. Choose File from the main menu then Properties. Click the Digital Ids tab.
3. Click the Import button.
4. Search for the digital certificate file and click Open.

5.1 IMPORTING A DIGITAL CERTIFICATE

To view details of the digital certificates of recipient

1. Open the Address book (Tools > Address Book) and double click on the correspondent entry that the user would like to view.
2. Select the Digital Ids tab in the Properties dialog box.
3. Select the Digital Certificate that user wants to view and click the Properties button.
4. Open the Address book (Tools > Address Book) and double click on the entry that the sender would like to view.
5. Select the Digital Ids tab in the Properties dialog box.
6. Select the Digital Certificates that user want to remove and click the Remove button.

~~~OOO~~~
~~~