المركز الوطني للتصديق الرقمي
National Center for Digital Certification

PKI USER MANUAL

JANUARY 2, 2013

Document Classification:

Confidential

VERSION 2.0

NCDC – Brief Introduction

1. About NCDC

The Government of Saudi Arabia has embarked on an ambitious e-transaction program, recognizing that there is a tremendous opportunity to better utilize information technology to improve the quality of care/service, lower the cost of operations, and increase customer satisfaction. To ensure the secure, efficient transmission and exchange of information electronically, the Kingdom of Saudi Arabia has created a National Public key Infrastructure. Named the National Centre for Digital Certification (NCDC), the NCDC is created by an act of law and its mandate is stipulated in the Saudi e-transaction law.
NCDC provides trust services to secure the exchange of information between key stakeholders. Participants include:

- Government employees
- Citizens
- Businesses

2. Government Certification Authority

Government Certification Authority (Government-CA) is owned by the Ministry of Communication and Information Technology (MCIT). Government-CA is the Certification Authority under the NCDC-Root-CA. NCDC-Root-CA has issued a digitally signed CA Certificate to the Government-CA. The Government-CA is responsible for issuing and managing Digital Certificates to Government employees, entities, non-human subscribers (like Servers and Network Devices) within the Government domain, through Certificate Service Providers (henceforth referred as CSPs) within the framework.

3. NCDC ESP Kit

Every user participating in the PKI usage will be provided with an NCDC ESP Kit, which will contain the following

1. Digital Certificate
2. Entrust Entelligence Security Provider (ESP) for Windows
3. Entrust Entelligence Security Provider (ESP) for Outlook
4. SafeNet USB token Drivers

4. Digital Certificates

The digital equivalent of an ID card used in conjunction with a public key encryption system. Also called a "digital ID," "digital identity certificate," "identity certificate" and "public key certificate," digital certificates are issued by a trusted third party known as a "certification authority" (CA) such as NCDC Government Certification Authority
Every subscriber participating in the PKI usage will obtain a Digital Signature Certificate (DSC) issued by Government CA. Before issuance of the Digital Certificate, the subscriber has to fill a request form and get the required approvals from the Authorizing Person.
Subscriber's identity then verified by the Registration office and a Digital Certificate is issued. The Subscriber can perform the followings using the issued Digital Certificate

1. Digital Signing and Verification of an Email
2. Encrypting and Decrypting an Email

3. Digital Signing and Verification of a Document
4. Encrypting and Decrypting a Document

5. Entrust Entelligence Security Provider (ESP)

Entrust Entelligence Security Provider (ESP) is a desktop security solution and is an enterprise-wide security platform for Windows desktops, domain controllers, and authentication servers that allows organizations to deploy the digital identities that enable the strong authentication, encryption and digital signature capabilities within a number of authentication applications and other applications such as data encryption and secure email.

6. Secure Storage Device – Safenet ikey USB tokens

SafeNet USB token offers a compact hardware solution for authentication and digital identity management. SafeNet USB token offers onboard key generation, key storage, encryption, and digital signing capabilities add high-assurance security to user login, digitally sign emails, holding master keys for disk encryption, VPN authentication, and other secure client applications.

7. Pre-Requisites

The following pre-requisites are needed before installation of ESP and SafeNet USB token Drivers

1. End user Operating System – Windows XP or Vista
2. Microsoft Outlook installed for the Entelligence Security Provider for Outlook

8. Help Desk Contacts

For any assistance or technical support please contact NCDC operations centre by sending an email to helpdesk@ncdc.gov.sa or via helpdesk Telephone numbers:
(01)452 2086 / (01)452 2037 / (01) 452 2196

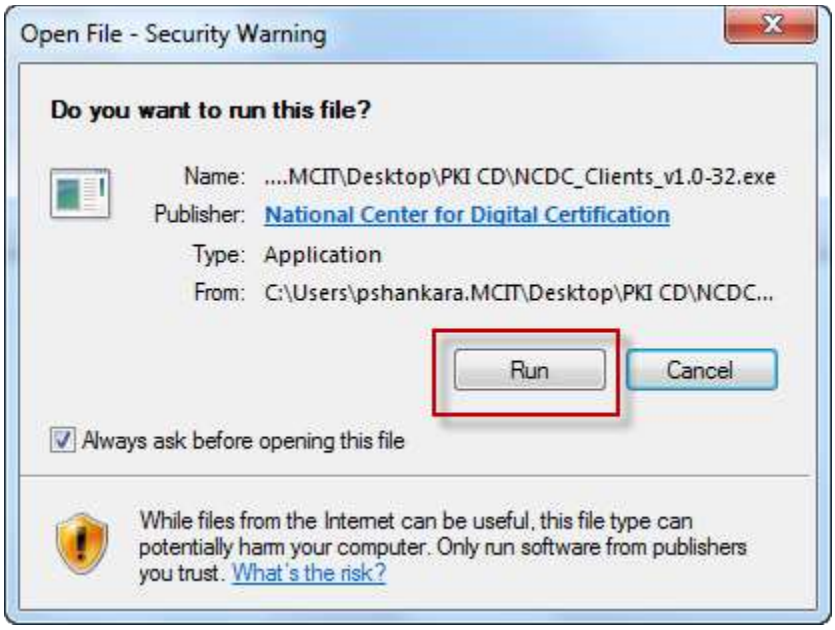
Installation of ESP and USB Token Drivers

Every subscriber will be provided with a PKI CD which will have the software's for ESP and SafeNet USB token or the subscriber can download the NCDC Clients Packager from NCDC Web Repository (http://web.ncdc.gov.sa)

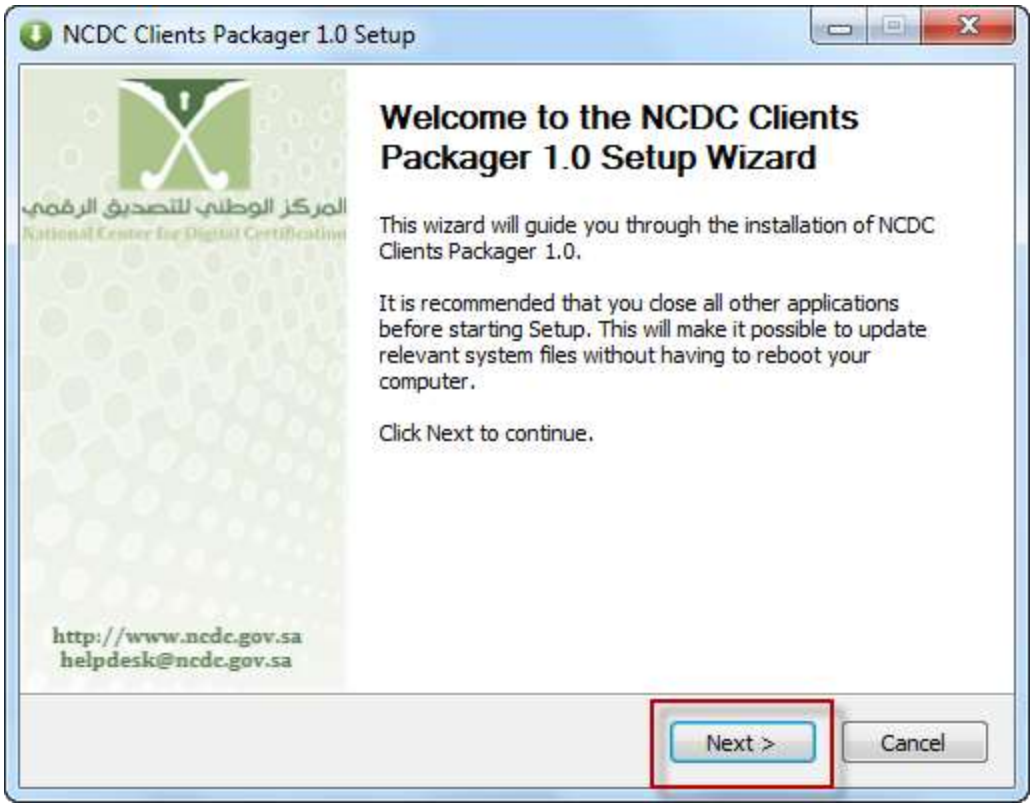
a. To run the Installation from CD
   - Insert the PKI CD into the CD Drive
   - You will find the NCDC Clients Packager, to install the packager Right Click and select **Open**

b. If you have downloaded the NCDC Clients Packager from NCDC Web Repository (http://web.ncdc.gov.sa), save the Packager on desktop and to install the packager Right Click and select **Open**

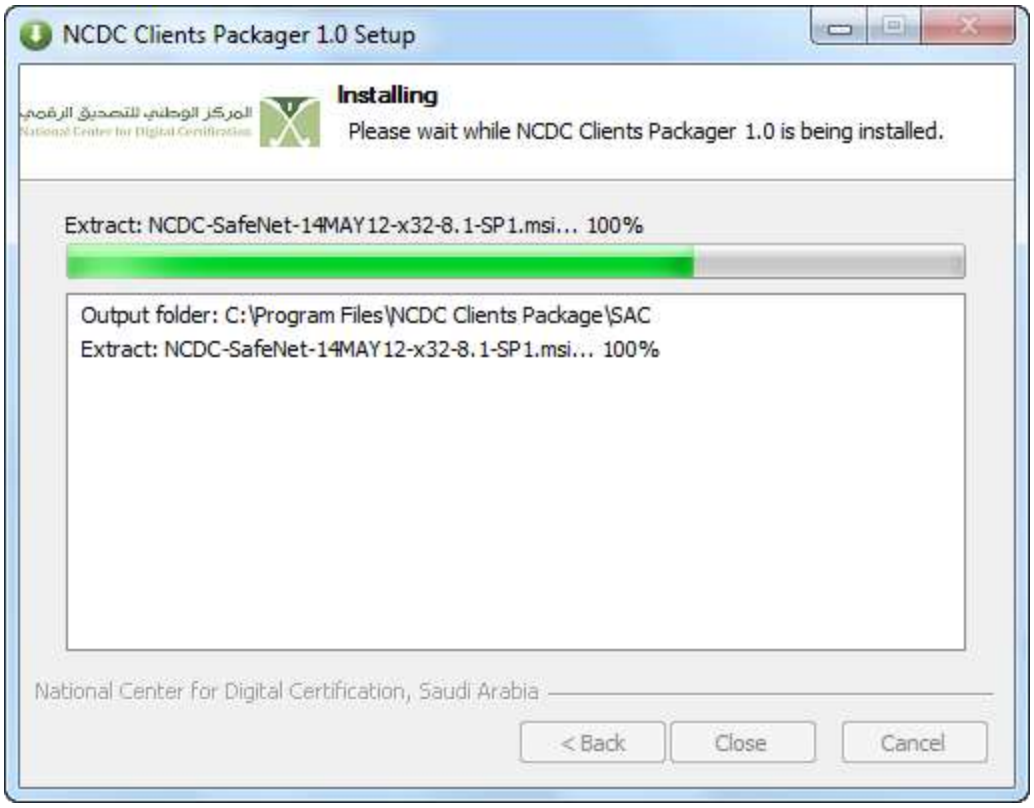
- Click "**Run"** on the Open File Security Warning window to proceed the installation



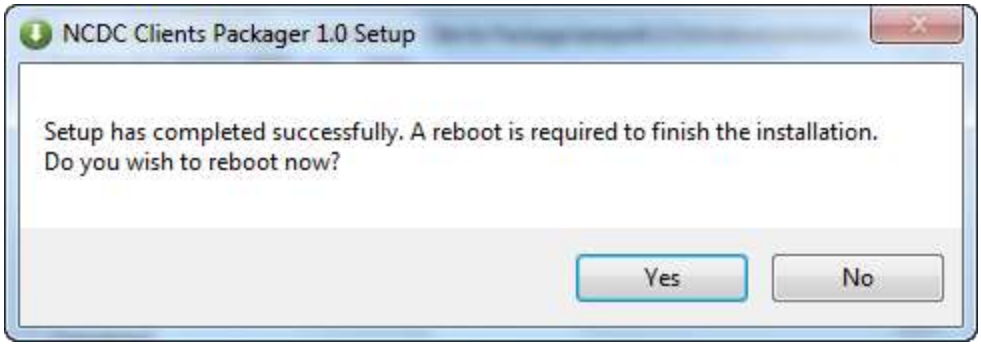
- Click **"Next"** to continue the installation.



- Accept the License Agreement when prompted and Click "**Install"**
- Wait for the Packager to install the components



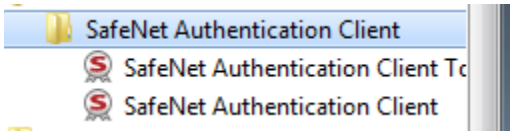
- Upon successful installation, you will be prompted to restart the computer. Click **Yes** to reboot.



c. Upon successful installation of Entrust Entelligence Security Provider (ESP) for Windows, the subscriber can view an Icon in the system tray.

d. Upon successful installation of Entrust Entelligence Security Provider (ESP) for outlook, the subscriber can view 2 new options added to the Outlook New Message Window

e. To check that the SafeNet USB token driver has been successfully installed. Click on **Start>Programs>SafeNet>SafeNet Authentication Client>SafeNet Authentication Client**



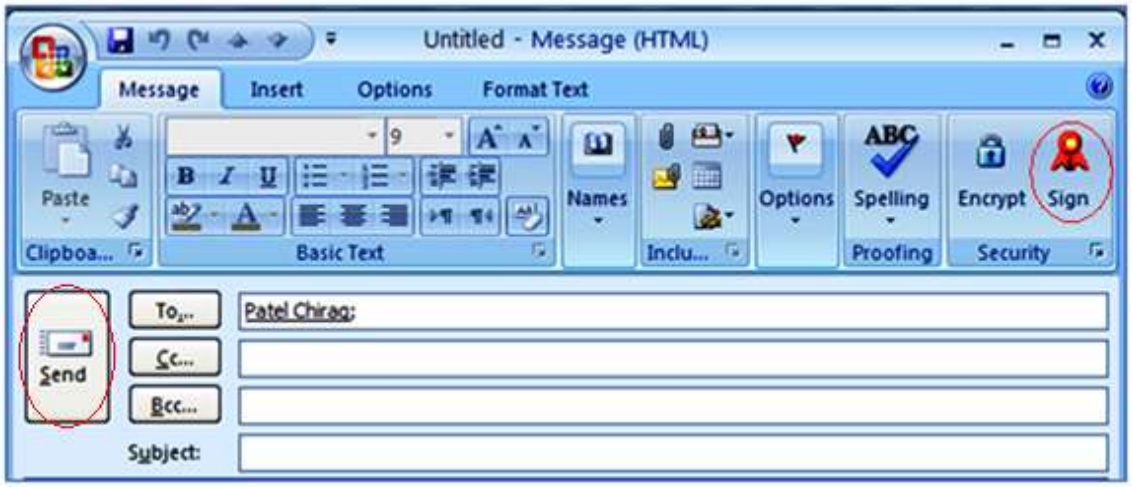
To Digitally Sign an e-Mail Message

The following steps will be invoked to execute this procedure:

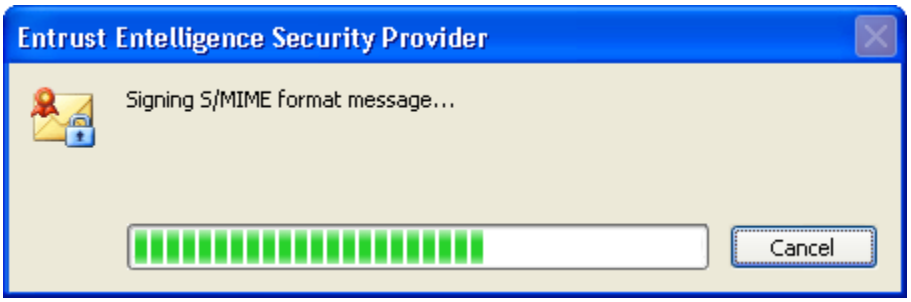
1. Ensure that Entrust Entelligence Security Provider (ESP) for Outlook and SafeNet Tokens Drivers are installed and the token is inserted in the USB slot to perform this procedure

2. Open a New Mail in Microsoft Outlook

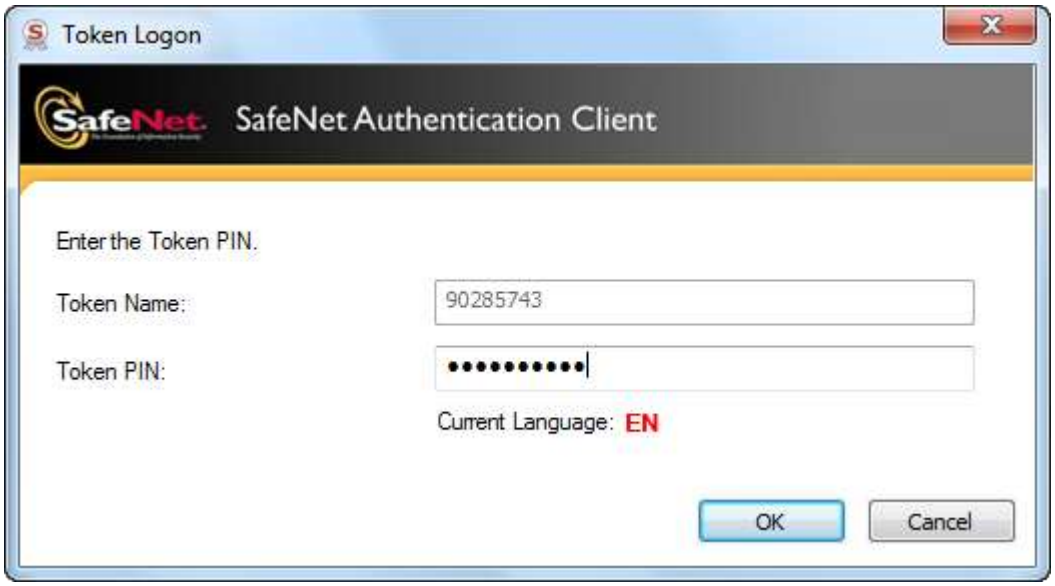
3. Select the recipients to whom you like to send a Digitally Signed Mail. Click on Sign Button on the Tool Bar and Click "**Send**"



4. Entrust Entelligence Security Provider (ESP) for Outlook will Digitally Sign the email



5. The Wizard will prompt to provide the USB Token PIN; after Providing the PIN, Click "**OK**"

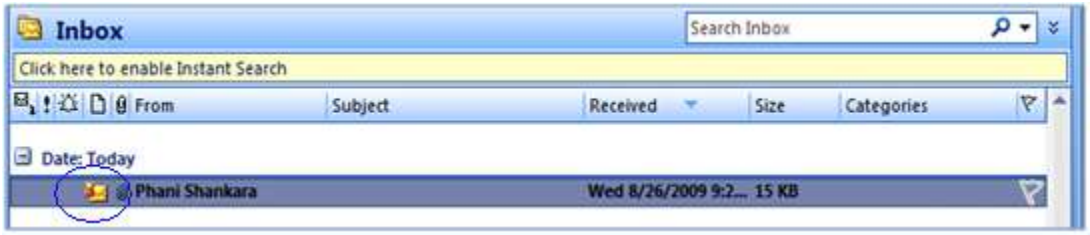


6. The signed message is now sent to the recipient and the process is completed.

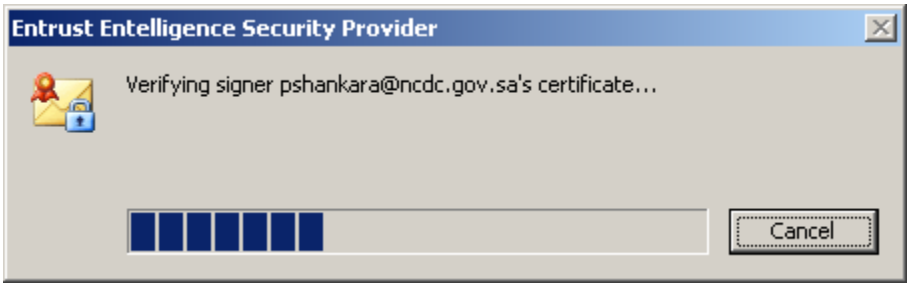
To Verify a Digitally Signed e-Mail Message

The following steps will be invoked to execute this procedure:

1. The recipient of the Digitally Signed Mail will receive the messages with a mail envelope with **RED** Seal Symbol

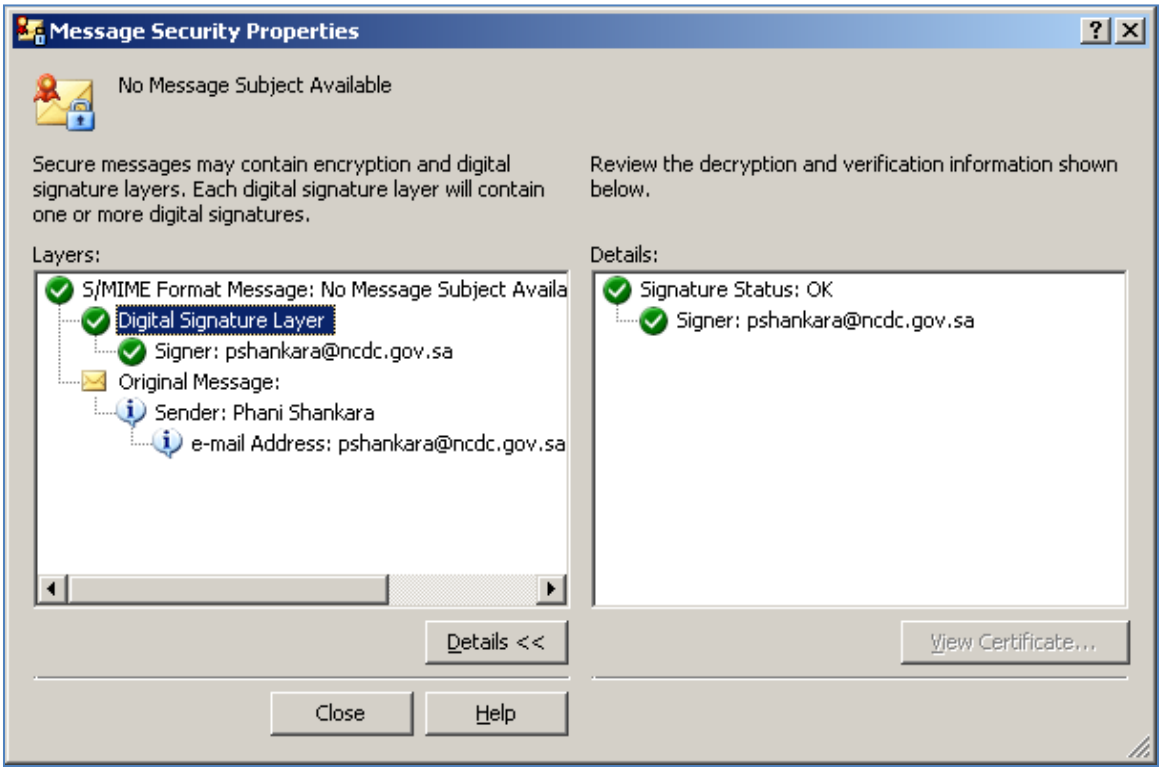


2. On clicking the Digitally Signed Mail, Entrust Entelligence Security Provider (ESP) will verify the sender's signature



3. The Digitally signed mail will now open in reading pane mode and the recipient can verify that the mail that was Digitally Signed as shown below

4. The recipient can click on the Digitally Signed Icon and view the Message Security Properties



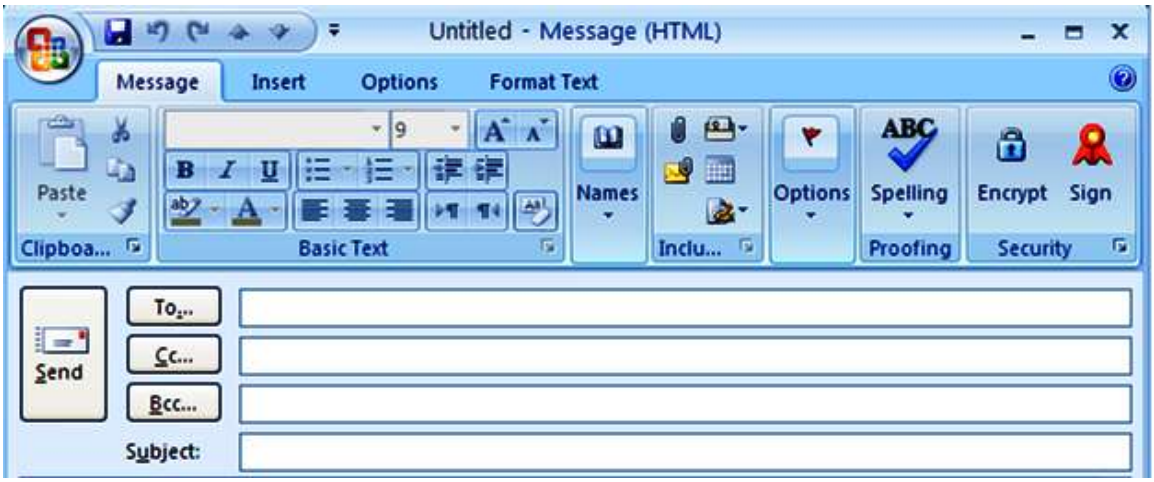
To Encrypt an Email

The following steps will be invoked to execute this procedure:

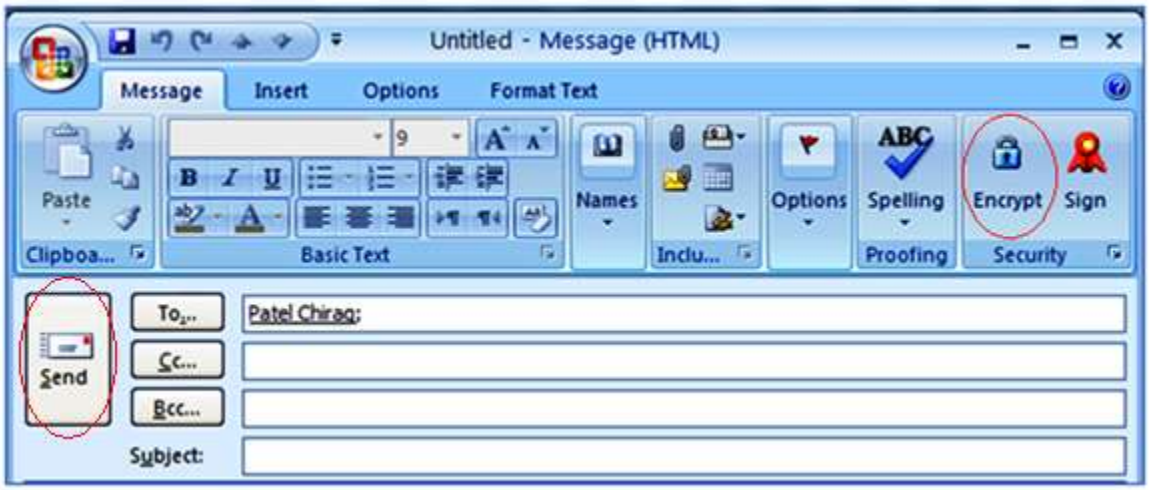
1. Ensure that ESP for Outlook and SafeNet Tokens Drivers are installed and the token is inserted in the USB slot to perform this procedure

2. Ensure that the Person to whom you are encrypting the mail is part of NCDC PKI Trust Network and his public key certificates available in the LDAP.

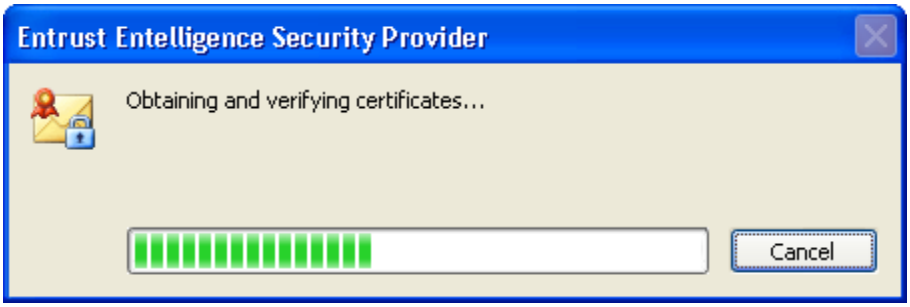
3. Open a New Mail in Microsoft Outlook



4. Select the recipients to whom you wish to send an Encrypted Mail and Click on Encrypt Button on the Tool Bar and Click "**Send**"



5. Entrust Entelligence Security Provider (ESP) for Outlook will obtain the recipients Public key and encrypt the mail



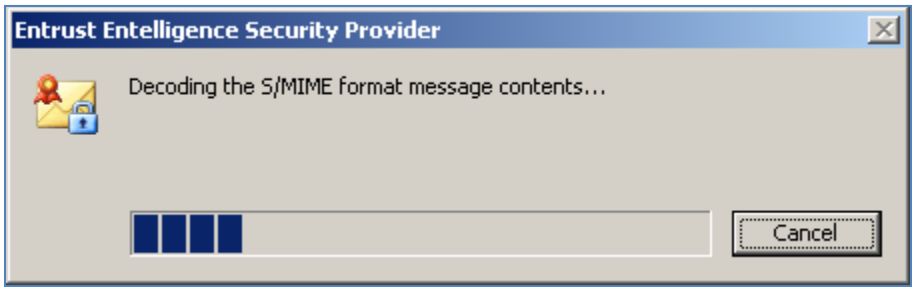
6. The Encrypted e-Mail will be sent to the selected recipient and the process will be completed.

9. To Decrypt an Email

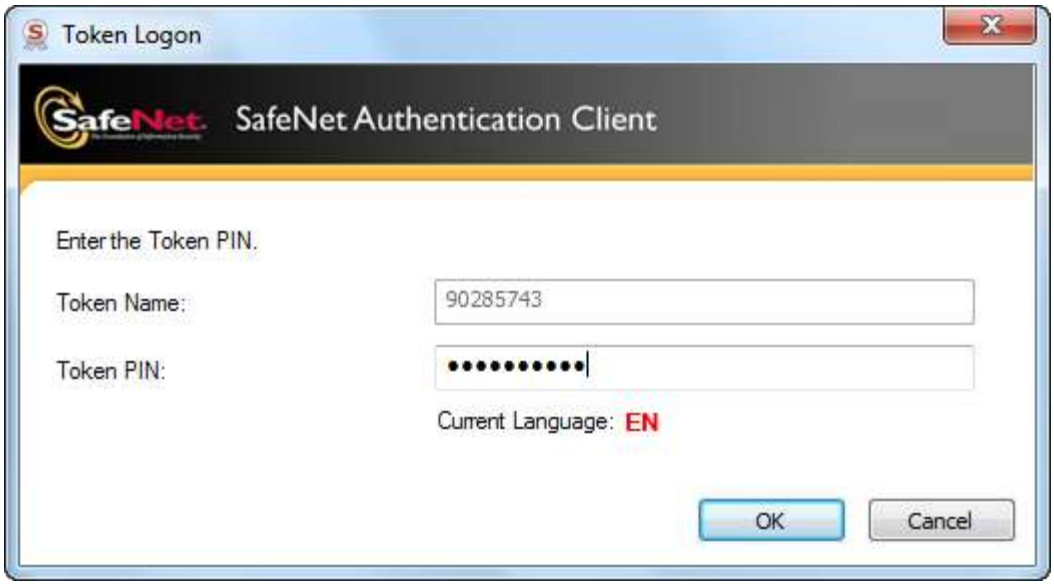
The following steps will be invoked to execute this procedure:

1. The recipient of the Encrypted Mail will receive the messages with a mail envelope with **BLUE** Lock Symbol

2. On clicking the Encrypted Email, Entrust Entelligence Security Provider (ESP) will decode the message contents

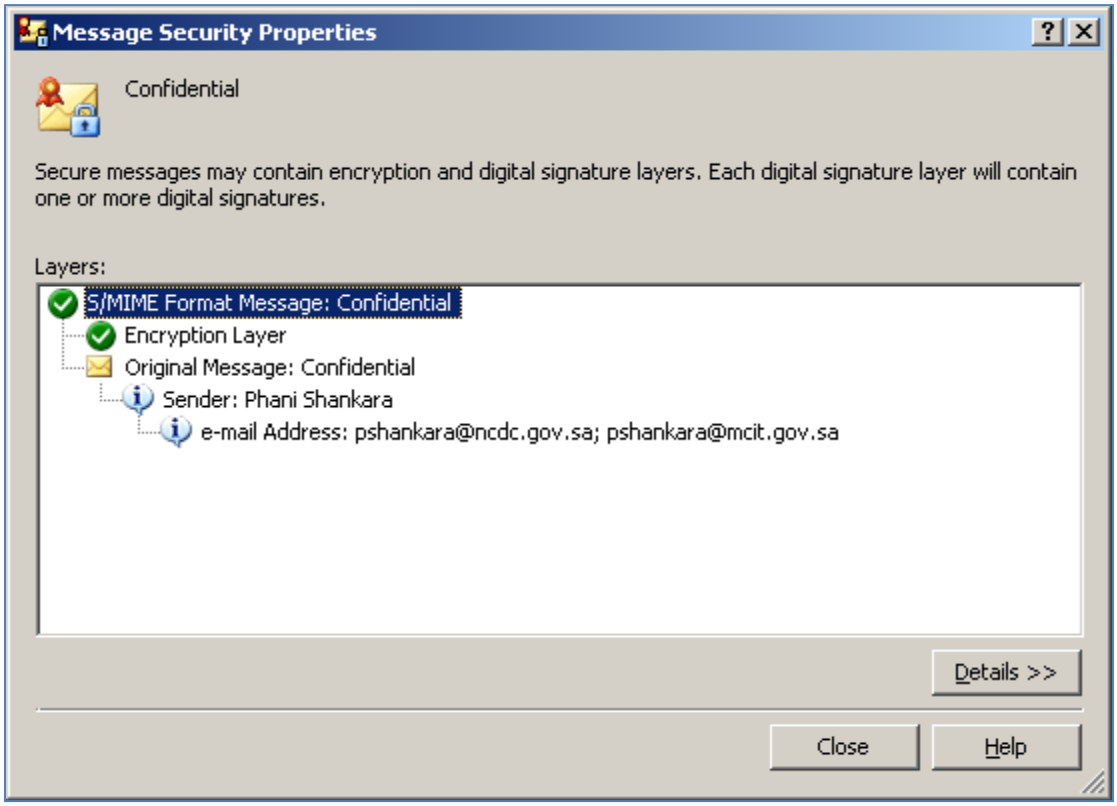


3. The Wizard will prompt to provide the USB Token PIN after Providing the PIN, Click "**OK**"


Token Logon
SafeNet Authentication Client
Enter the Token PIN.
Token Name:
90285743
Token PIN:
Current Language: EN
OK
Cancel

4. The Encrypted mail will now open in reading pane mode and the recipient can verify that the mail was Encrypted as shown below

5. The recipient can click on the Encrypted Icon and view the Message Security Properties

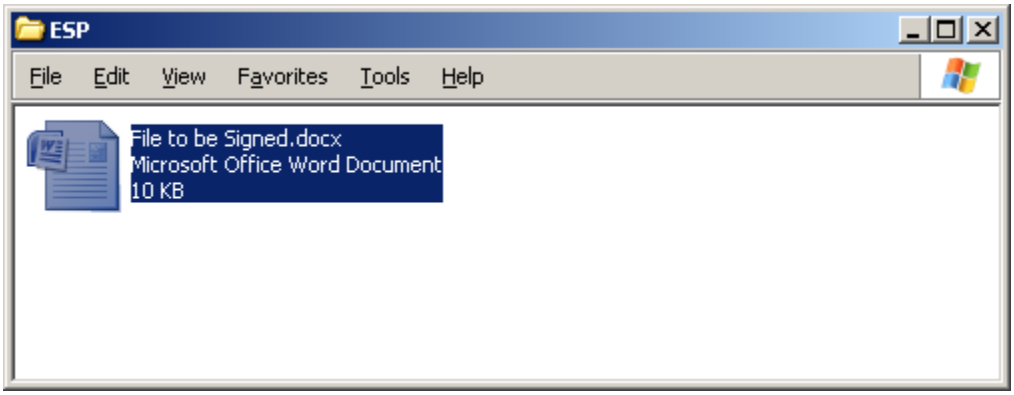


10. To Digitally Sign a Document

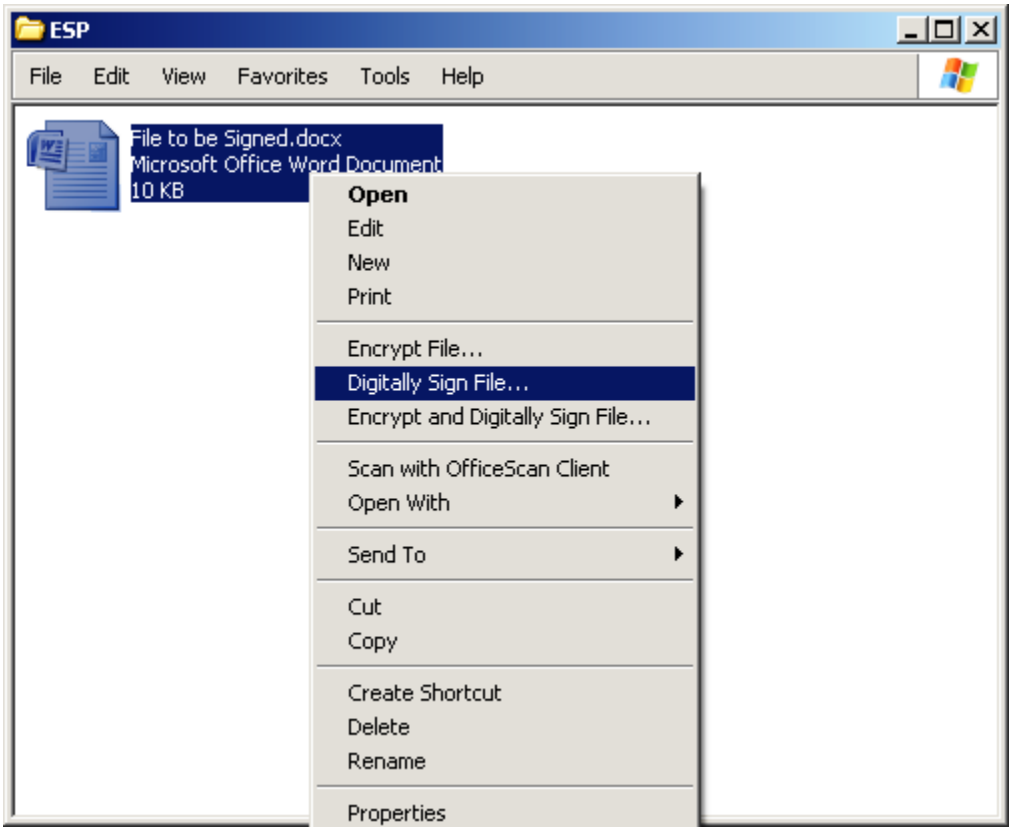
The following steps will be invoked to execute this procedure:

1. Ensure that ESP for Windows and SafeNet Tokens Drivers are installed and the token is inserted in the USB slot to perform this procedure

2. Select a file which you like to Digitally Sign

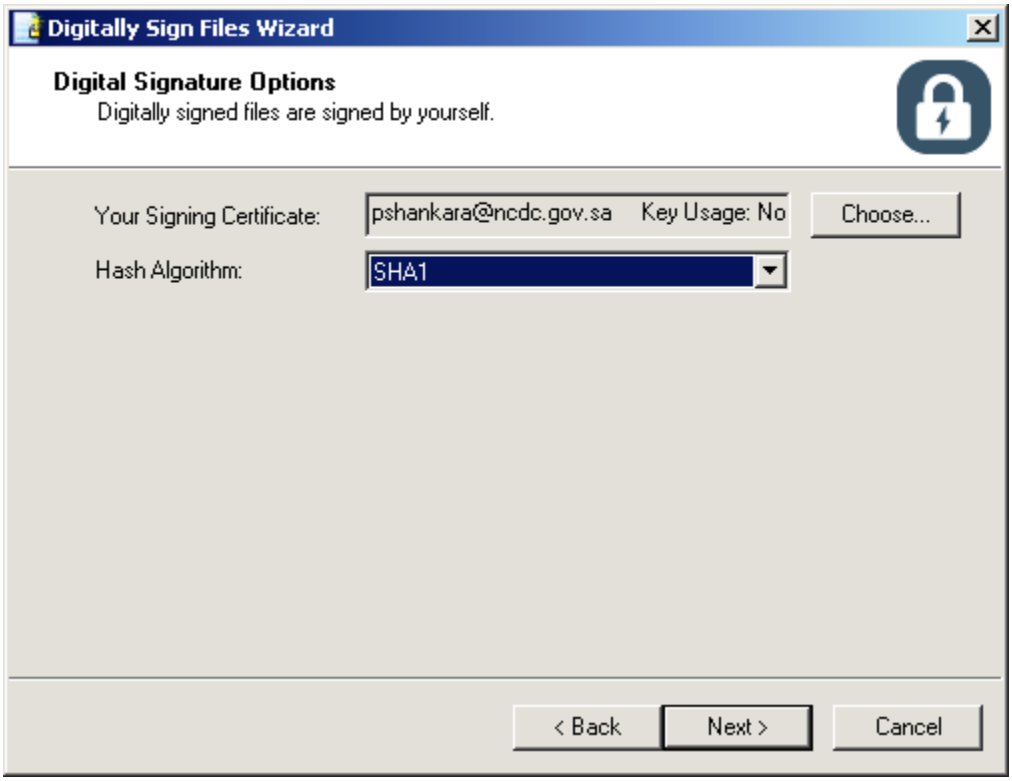


3. Right Click on the file and select the option of "**Digitally Sign File**"

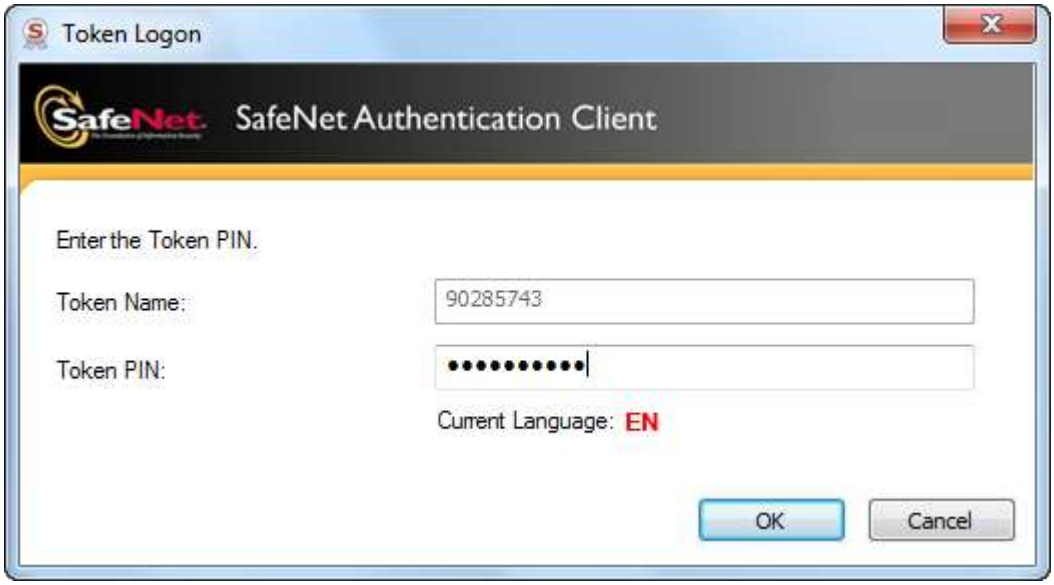


4. The Digitally Sign files Wizard would open which will guide you through the process of digitally signing of files, click "**Next**"

5. The signing certificate and the Hash algorithm "SHA1" will appear, click “**Next**”

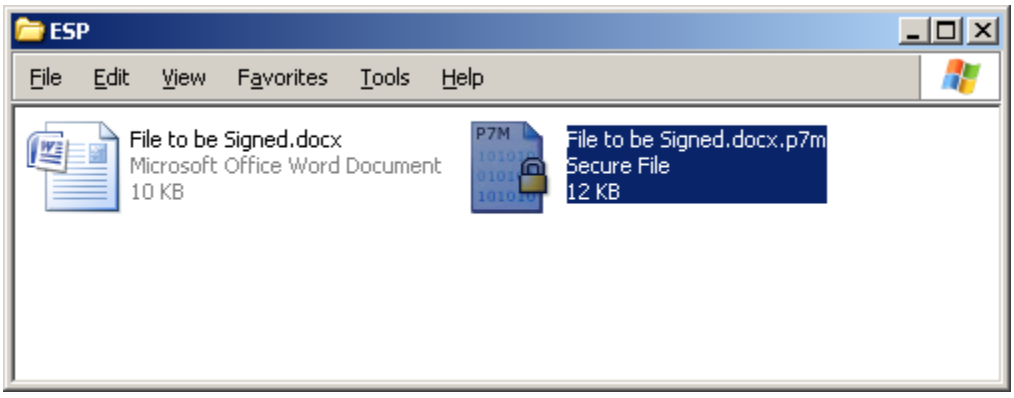


6. The Wizard will prompt to provide the USB Token PIN after Providing the PIN, Click "**OK**"



7. Click on "**Finish**" to complete the Digital Signing Process.

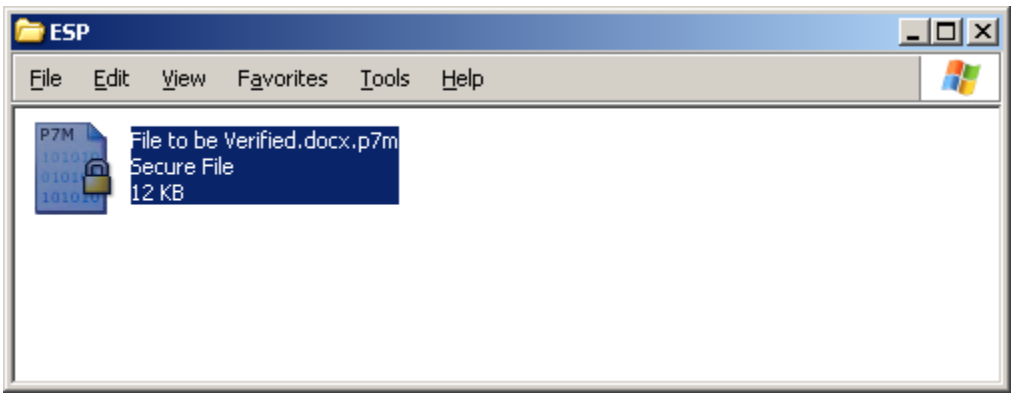
8. The output of the Digitally Signed file will be in a new format (.p7m)



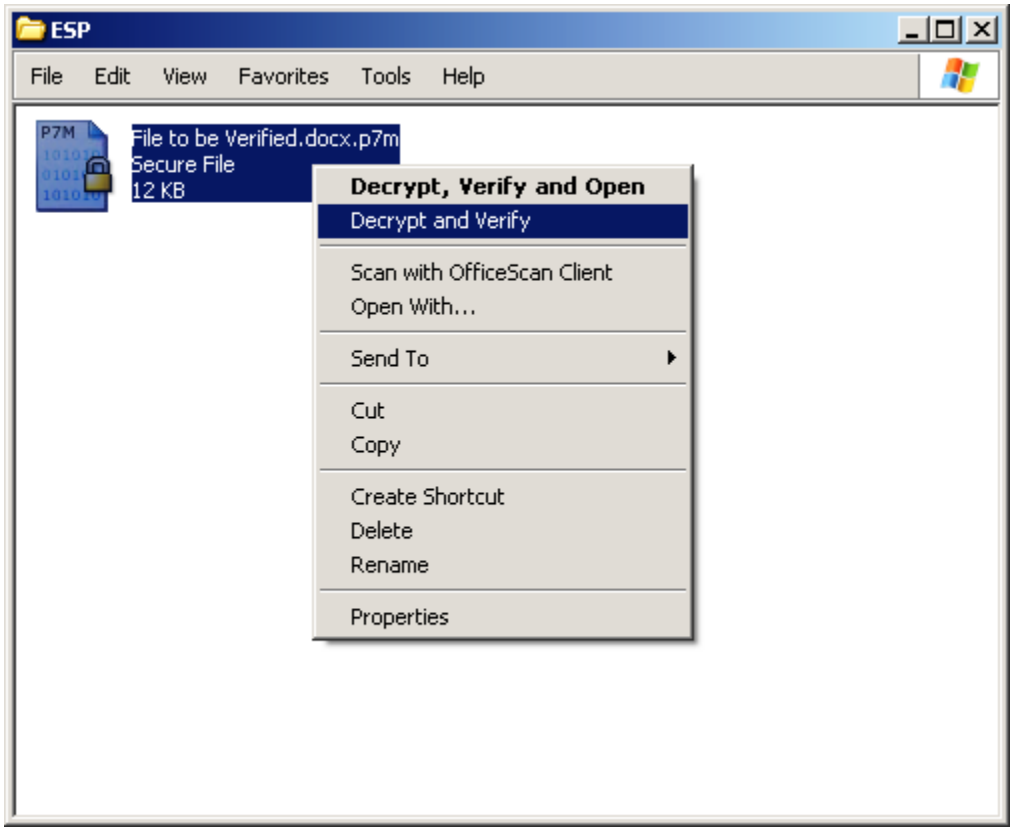
To Verify a Digitally Signed Document

The following steps will be invoked to execute this procedure:

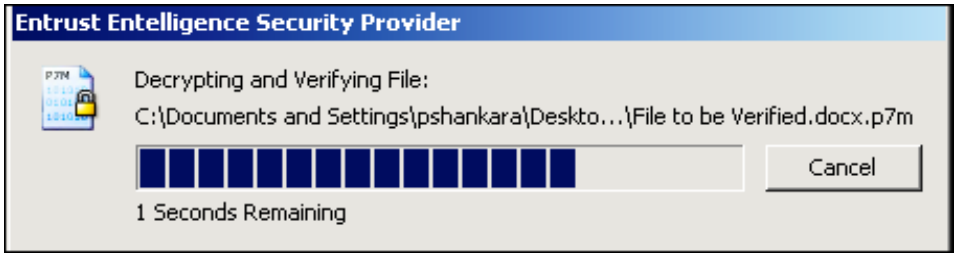
1. Select a Digitally Signed file to verify



2. Right click on the Signed file and Select the "**Decrypt and Verify**"



3. Entrust Entelligence Security Provider (ESP) will start the verification process



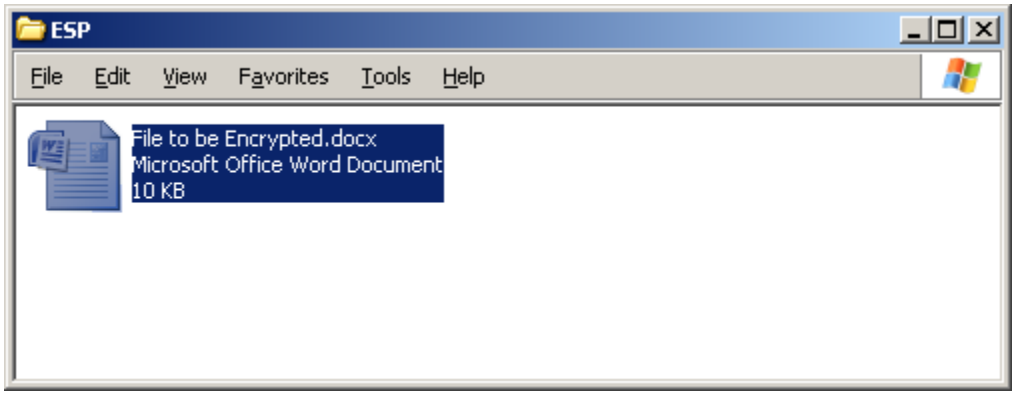
4. Once the process is completed, the original file can be obtained

To Encrypt a Document

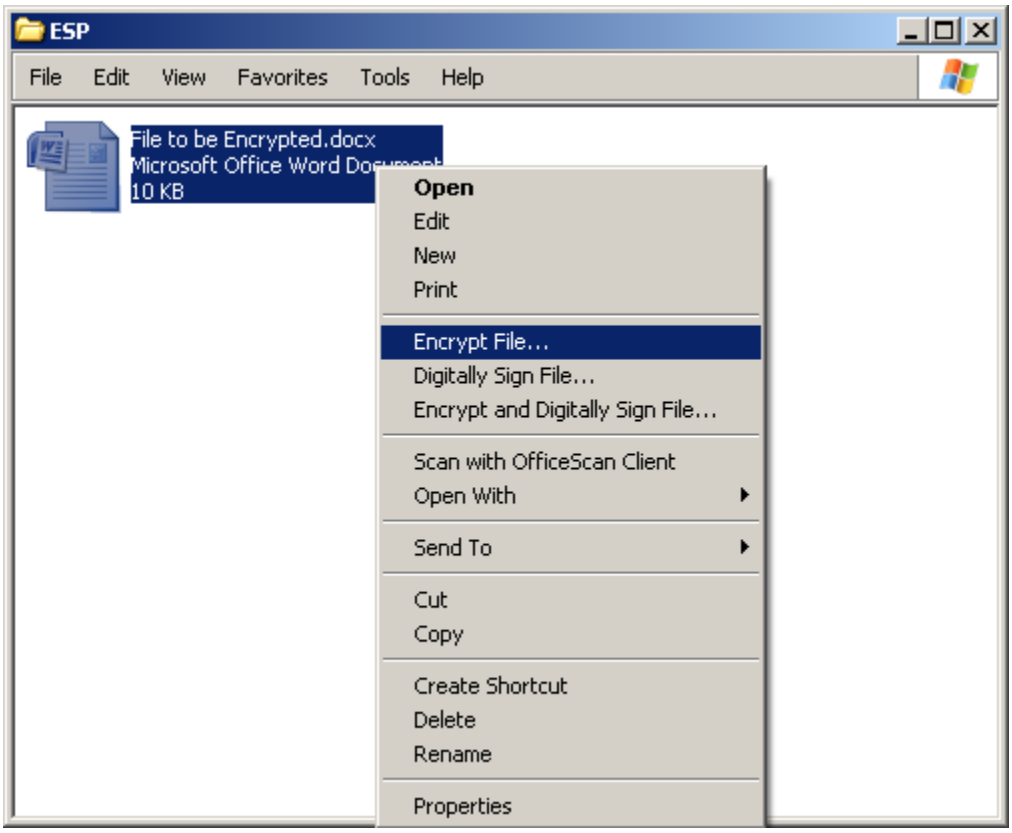
The following steps will be invoked to execute this procedure:

1. Ensure that ESP for Windows and SafeNet Tokens Drivers are installed and the token is inserted in the USB slot to perform this procedure

2. Select a file which you wish to Encrypt

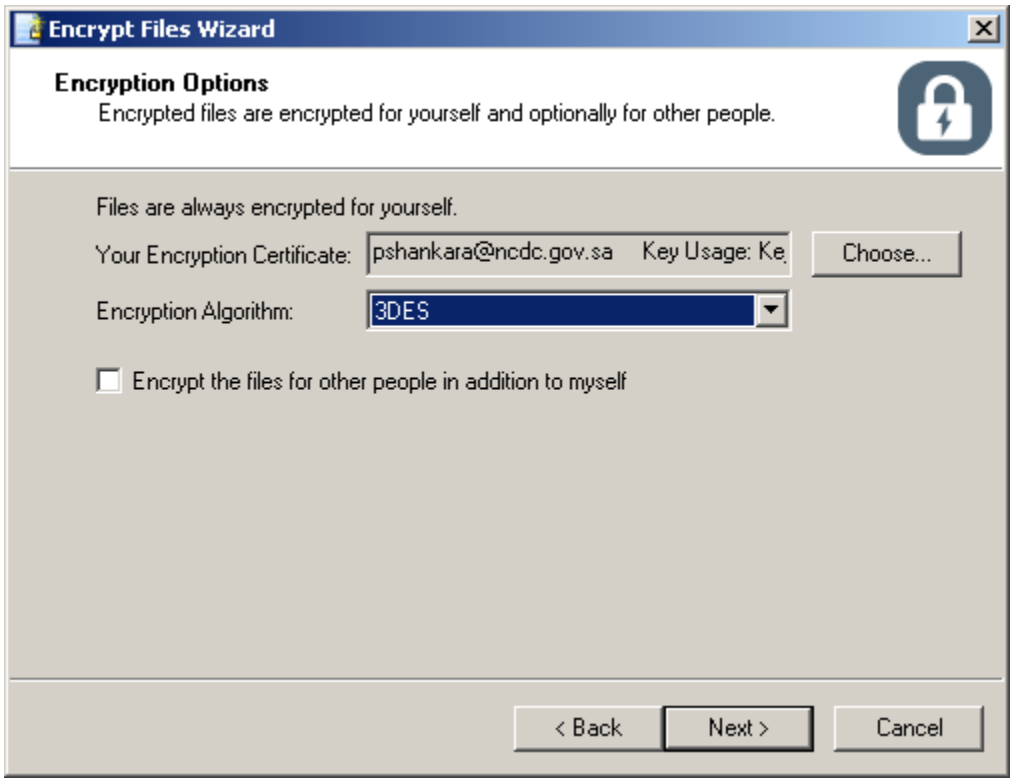


3. Right Click on the file and select the option of **"Encrypt File**"

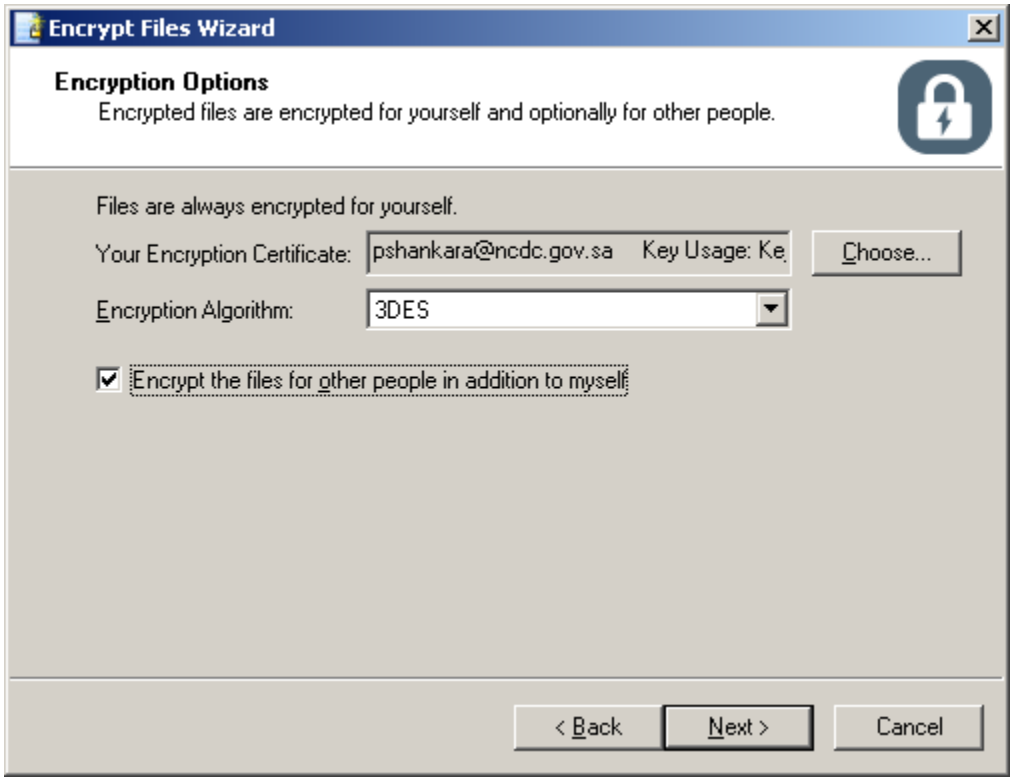

ESP
File Edit View Favorites Tools Help
File to be Encrypted.docx
Microsoft Office Word Document
10 KB
Open
Edit
New
Print
Encrypt File...
Digitally Sign File...
Encrypt and Digitally Sign File...
Scan with OfficeScan Client
Open With
Send To
Cut
Copy
Create Shortcut
Delete
Rename
Properties

4. The Encrypt files Wizard would open which will guide you through the process of Encrypting of files, click “**Next**”

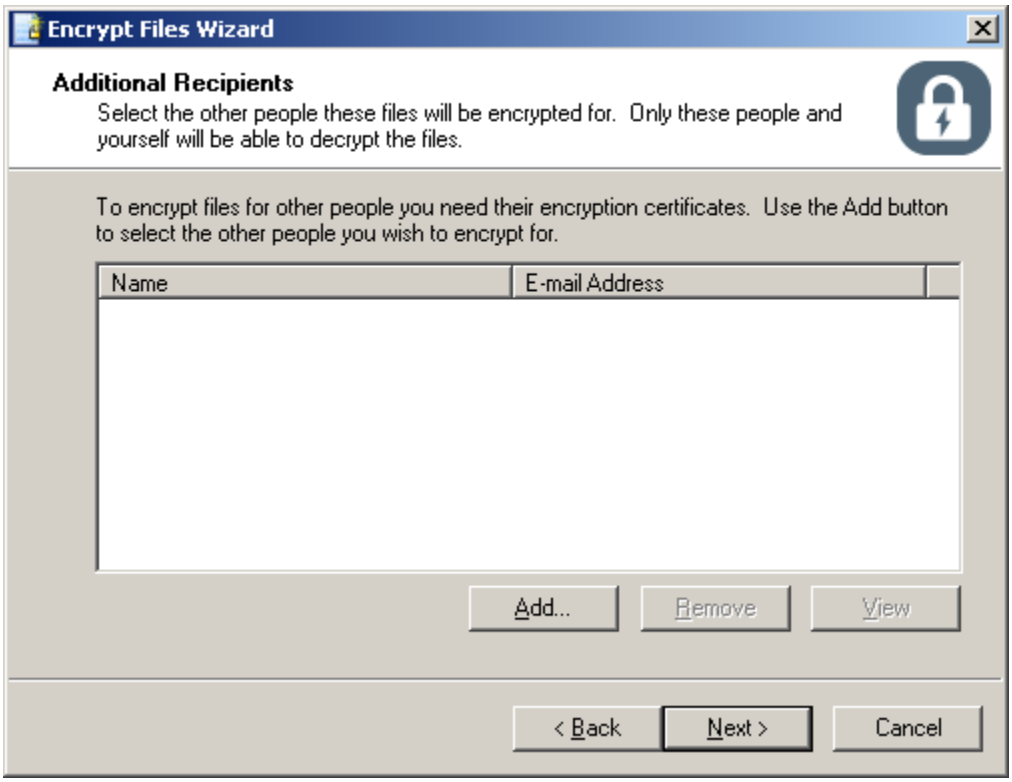
5. Your Encryption Certificate and Encryption Algorithm "3DES" will appear, then click “**Next**”


Encrypt Files Wizard
Encryption Options
Encrypted files are encrypted for yourself and optionally for other people.
Files are always encrypted for yourself.
Your Encryption Certificate:
pshankara@ncdc.gov.sa Key Usage: Ke
Choose...
Encryption Algorithm:
3DES
Encrypt the files for other people in addition to myself
< Back
Next >
Cancel

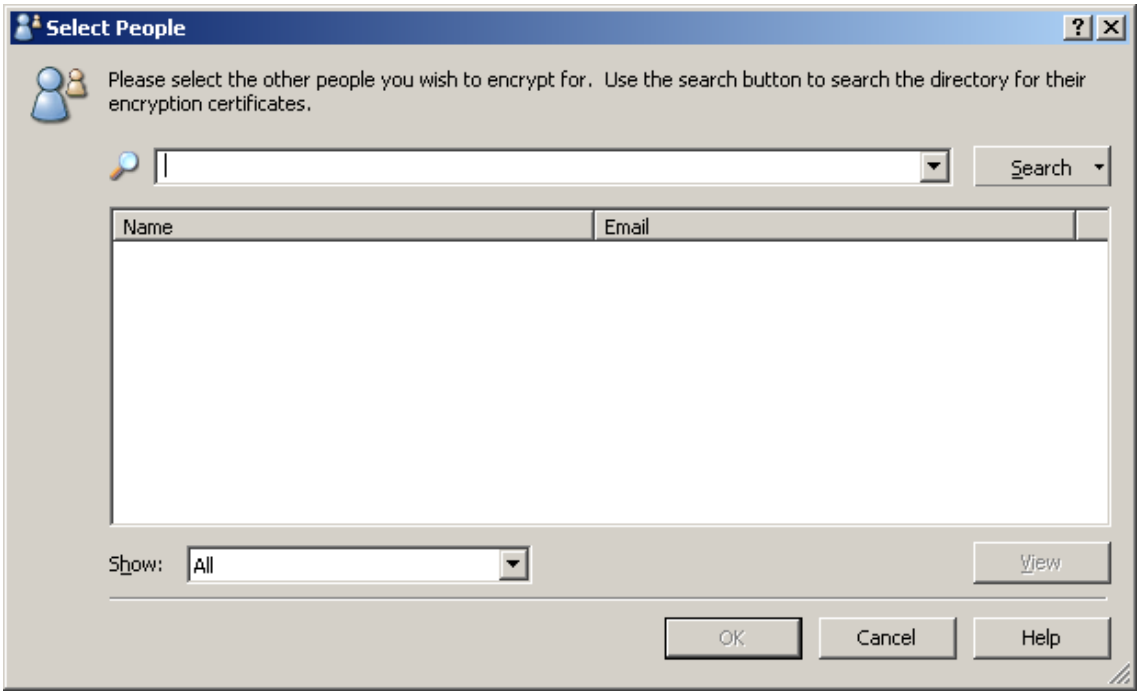
6. Tick the box in case you intend to encrypt the file for other people in addition to yourself



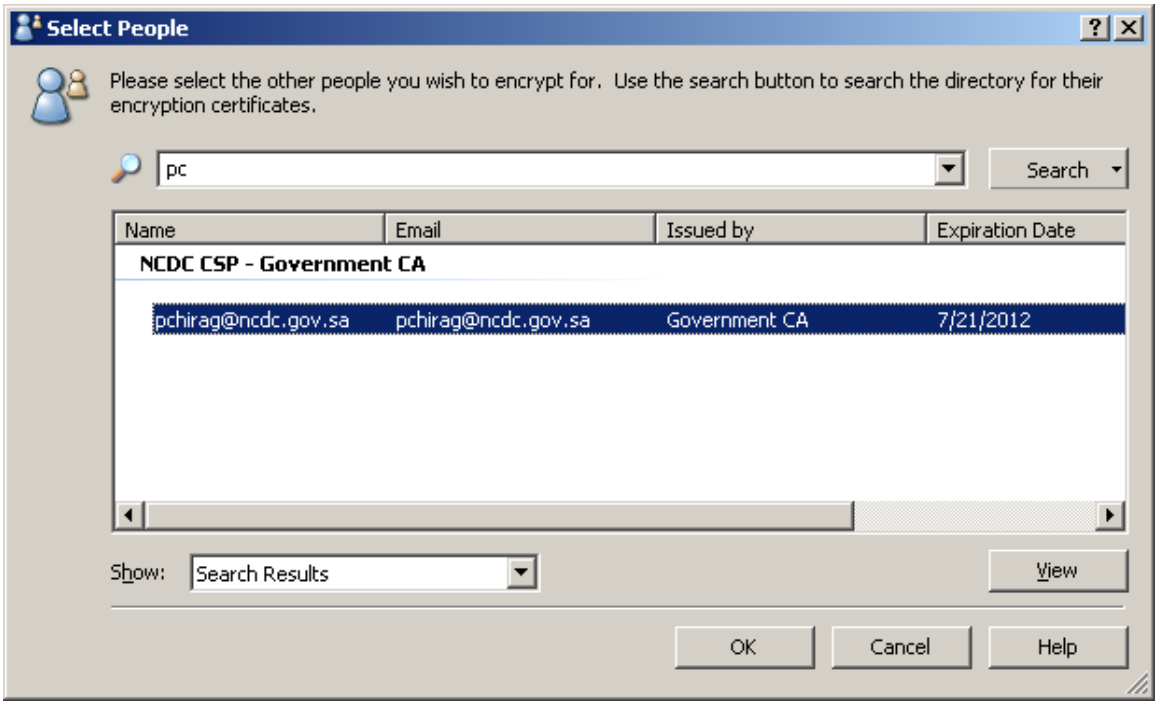
7. To encrypt files for other people you need their encryption certificate. Use the "**Add**" button to select the other people you wish to encrypt the file


Encrypt Files Wizard
Additional Recipients
Select the other people these files will be encrypted for. Only these people and yourself will be able to decrypt the files.
To encrypt files for other people you need their encryption certificates. Use the Add button to select the other people you wish to encrypt for.
Name
E-mail Address
Add...
Remove
View
< Back
Next >
Cancel

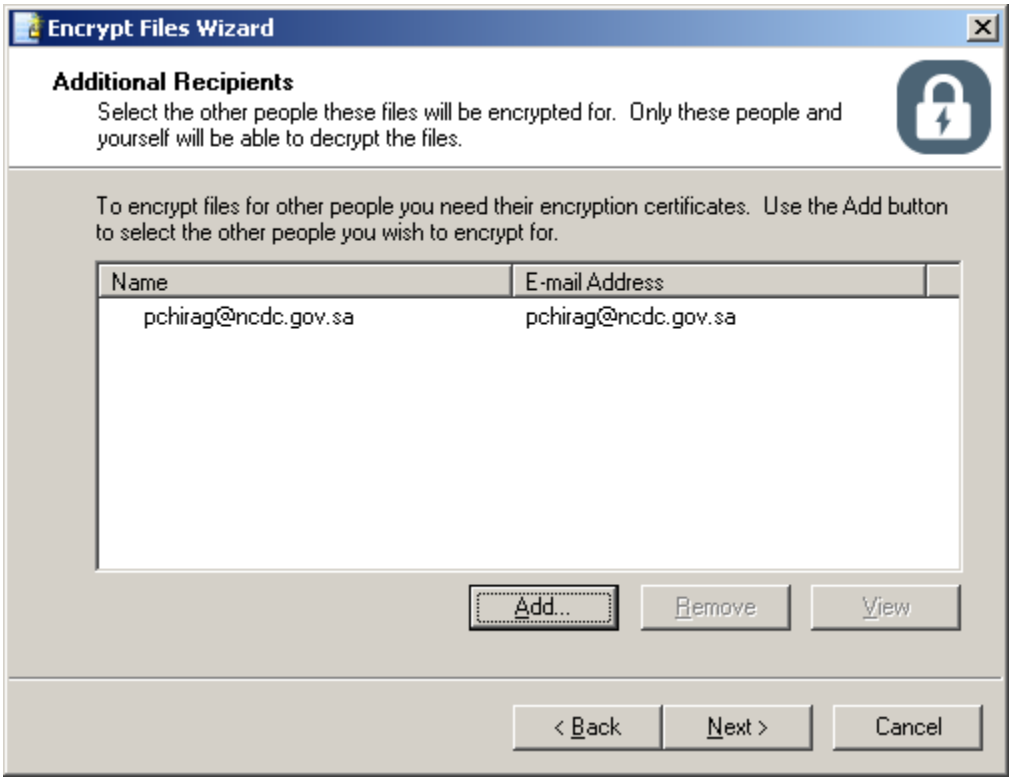
8. Type in name/email id of person to whom you wish to encrypt the file and use the "**search**" button to search the directory for their encryption certificates



9. Once the search results provides you with the details of the person to whom you wish to encrypt the file, select the persons certificate and click on "**OK**"

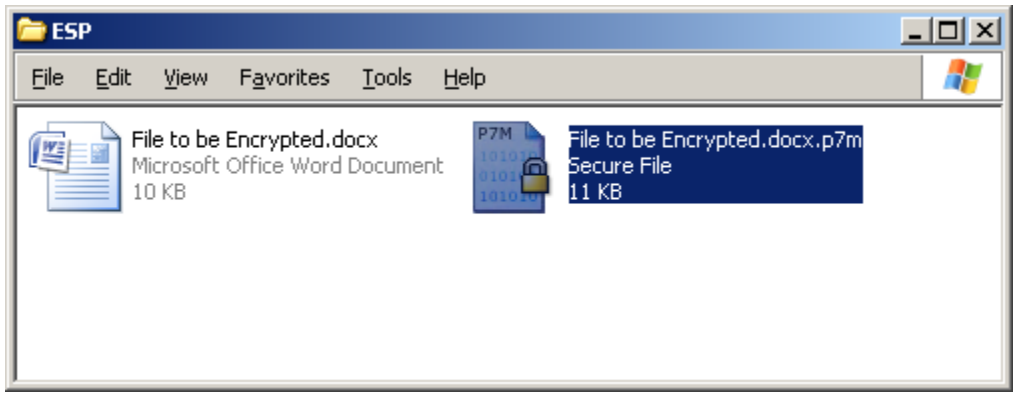


10. Once the details of the person to whom you wish to encrypt the file are added to the Encrypt file wizard click "**Next**"



11. Click on "**Finish**" to complete the Encrypting process.

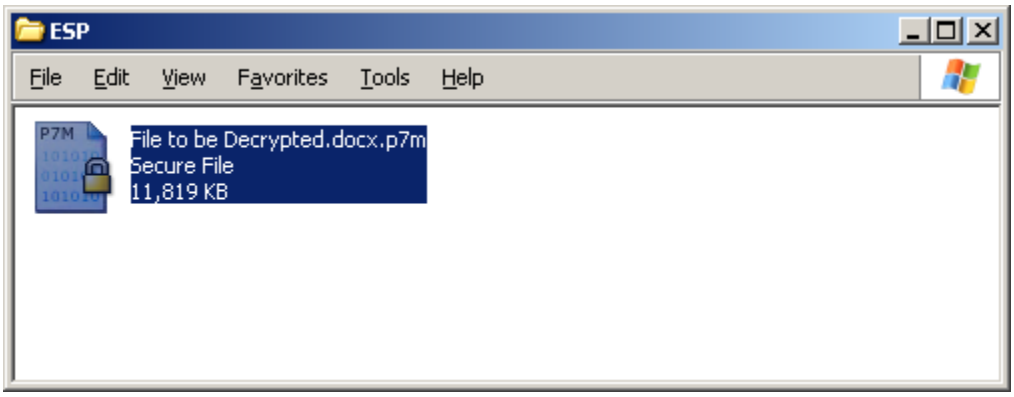
12. The output of the Encrypted file will be in a new format (.p7m). The encrypted file for other user may be sent using any medium such as flash memory, CD or by email.



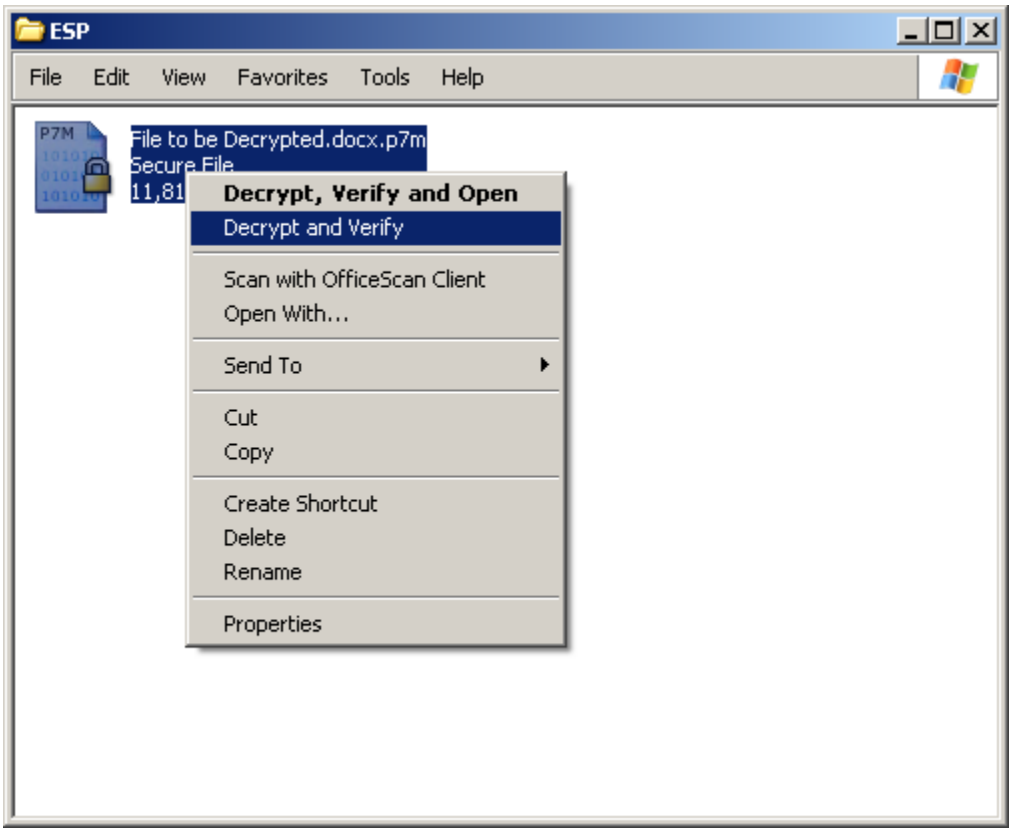
To Decrypt an Encrypted Document

The following steps will be invoked to execute this procedure:

1. Select an Encrypted file to decrypt

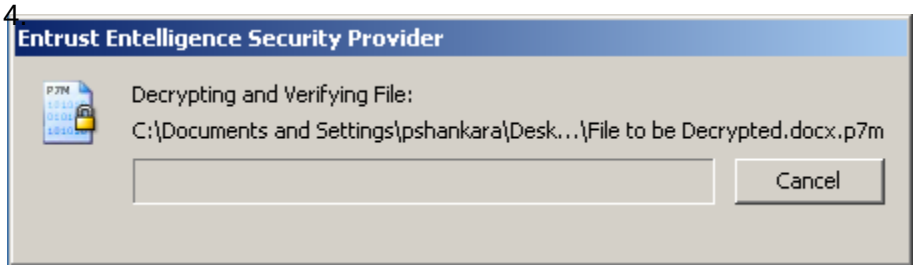


2. Right click on the encrypted file and Select the "**Decrypt and Verify**"

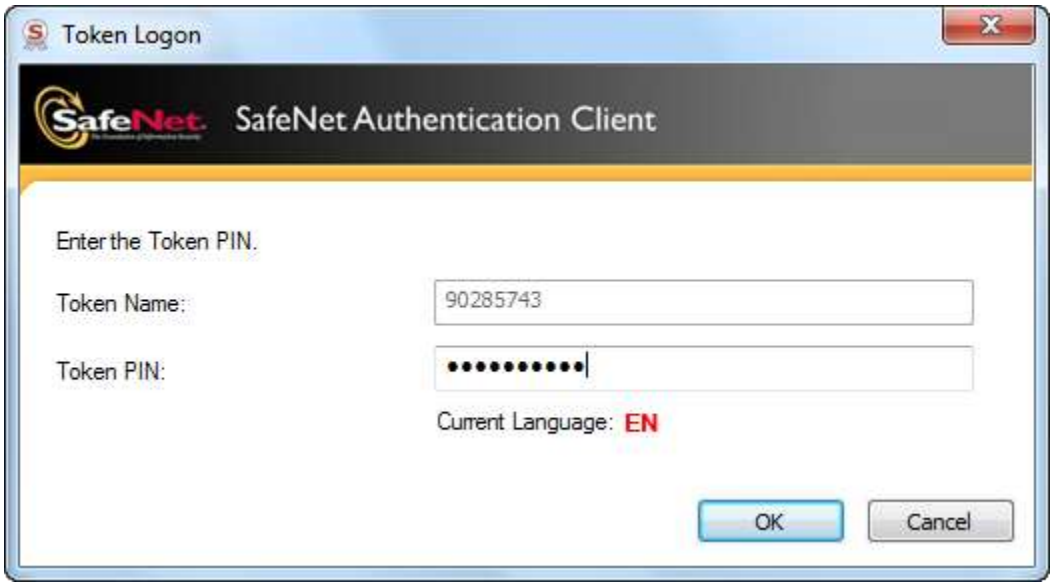


3. Entrust Entelligence Security Provider (ESP) will start the verification process

4.



4. The Wizard will prompt to provide the USB Token PIN after Providing the PIN, Click "**OK**"



5. The selected encrypted file will be decrypted and the output will be as follow