

Adding Digital Signature and Encryption in Outlook

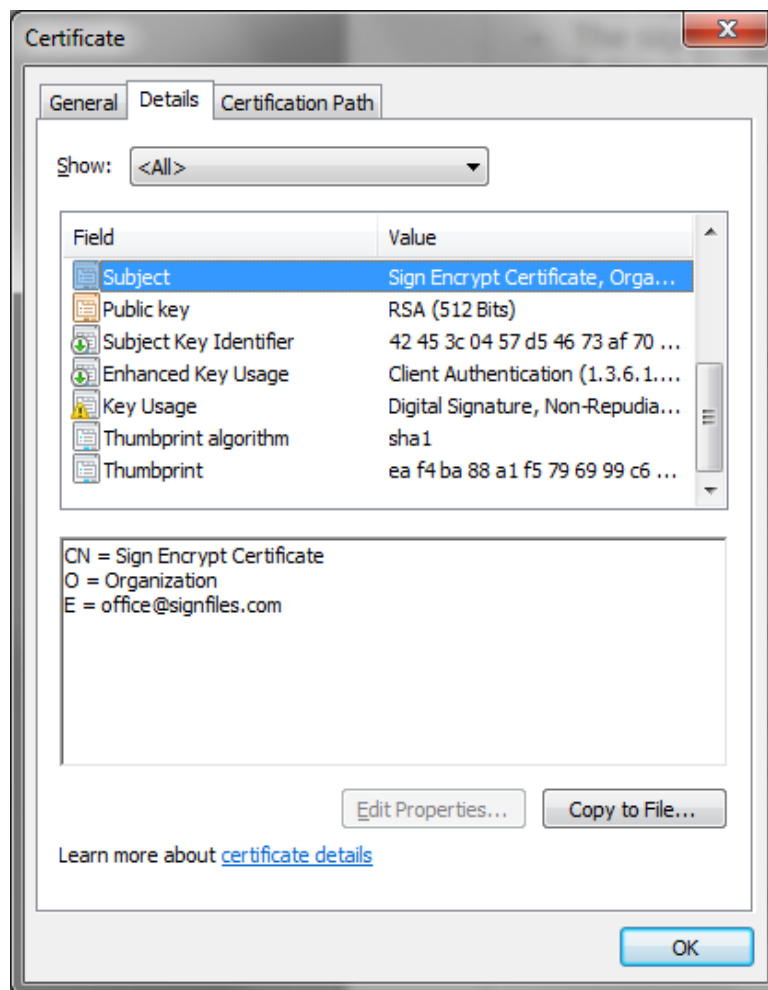
Using Outlook, the email messages can be signed and encrypted by a digital certificate.

To **digitally sign** a message in Outlook some conditions must be accomplished:

- The digital signature is created using your personal certificate.
- The signing certificate must have your email address on the certificate Subject (E=).
- The certificate is recommended to be issued by a CA and not to be a self signed certificate.

To **encrypt** an email message for a recipient in Outlook:

- The encryption is made using the encryption certificate of the recipient and not by your personal certificate.
- To encrypt a message for a recipient be sure that the recipient address exists in *Address Book* and it has a certificate.



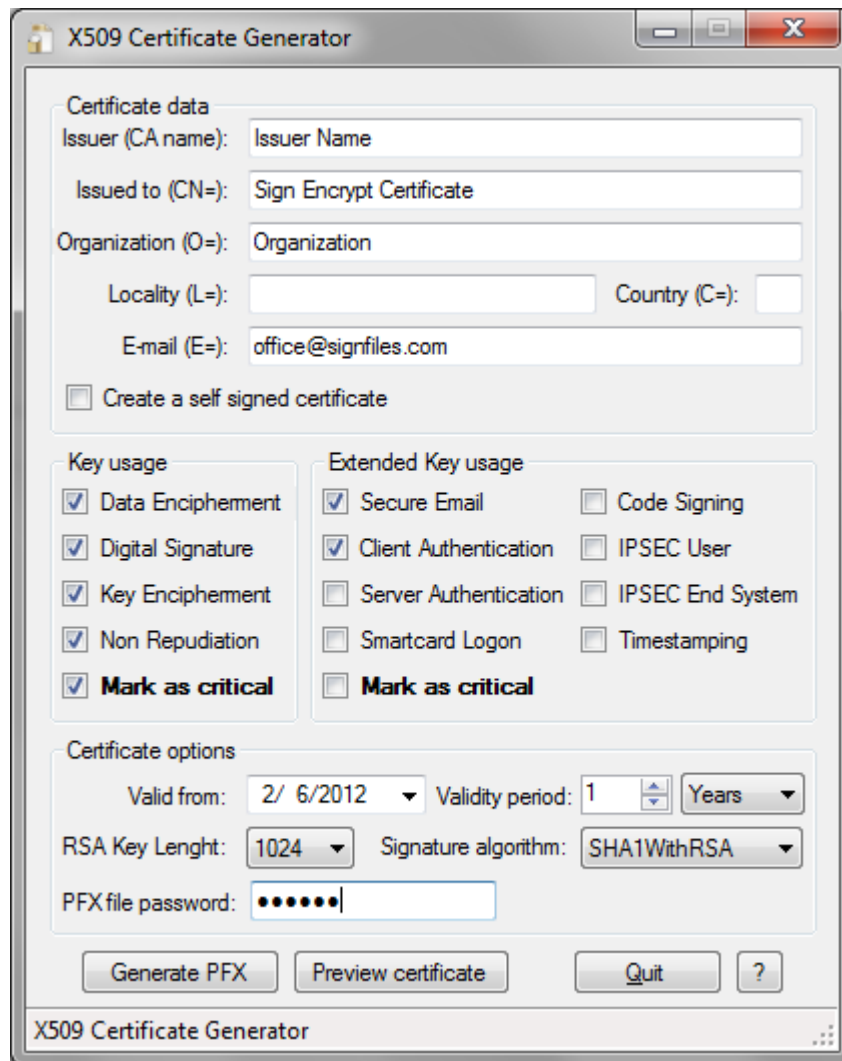
Obtain a certificate using X.509 Certificate Generator

The signing and encryption certificate must have these extensions:

Key Usage (marked as critical): Data Encipherment, Digital Signature, Key Encipherment, Non Repudiation

Extended Key Usage: Secure Email, Client Authentication

Also, be sure that your Outlook email address will be entered on the e-mail field.



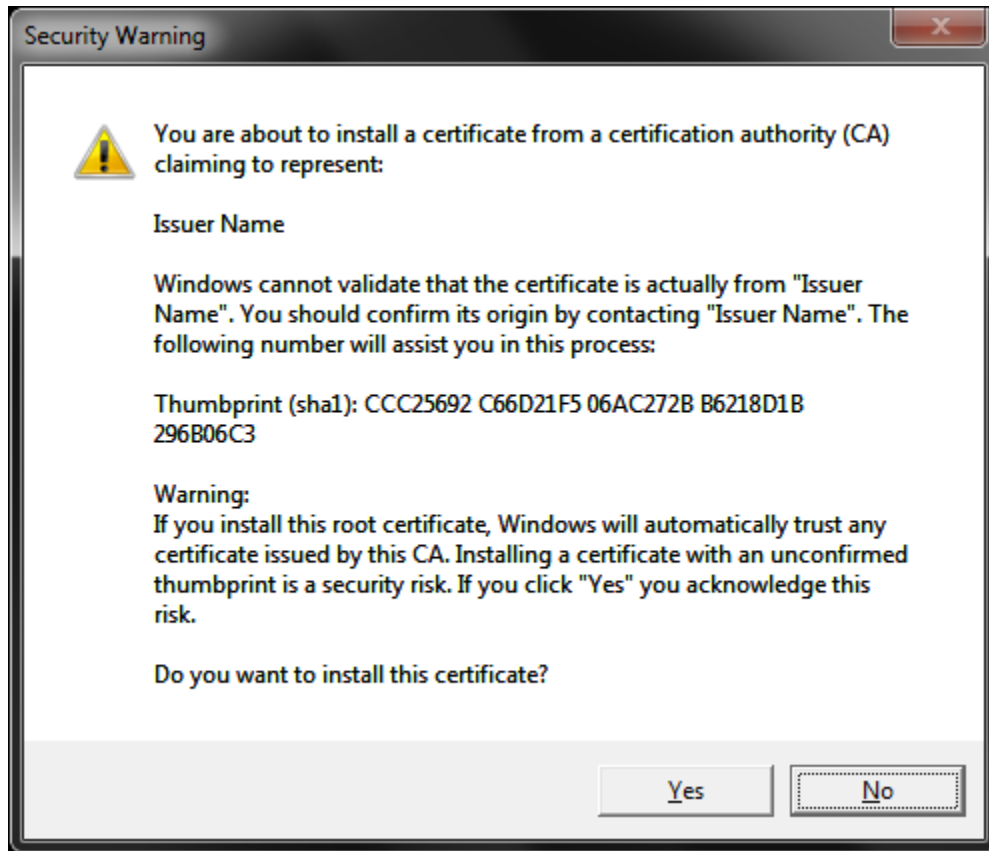
The screenshot shows the X509 Certificate Generator application window. The window title is "X509 Certificate Generator". The interface is divided into several sections:

- Certificate data:** Fields for Issuer (CA name): Issuer Name, Issued to (CN=): Sign Encrypt Certificate, Organization (O=): Organization, Locality (L=):, Country (C=):, and E-mail (E=): office@signfiles.com. There is a checkbox for "Create a self signed certificate" which is unchecked.
- Key usage:** A list of checkboxes: Data Encipherment, Digital Signature, Key Encipherment, Non Repudiation, and **Mark as critical** (checked).
- Extended Key usage:** A list of checkboxes: Secure Email, Client Authentication, Server Authentication, Smartcard Logon, Code Signing, IPSEC User, IPSEC End System, Timestamping, and **Mark as critical** (unchecked).
- Certificate options:** Fields for Valid from: 2/ 6/2012, Validity period: 1 Years, RSA Key Length: 1024, Signature algorithm: SHA1WithRSA, and PFX file password: [masked].

At the bottom, there are buttons for "Generate PFX", "Preview certificate", "Quit", and a help icon (?). The status bar at the bottom left says "X509 Certificate Generator".

Importing the certificate on your system

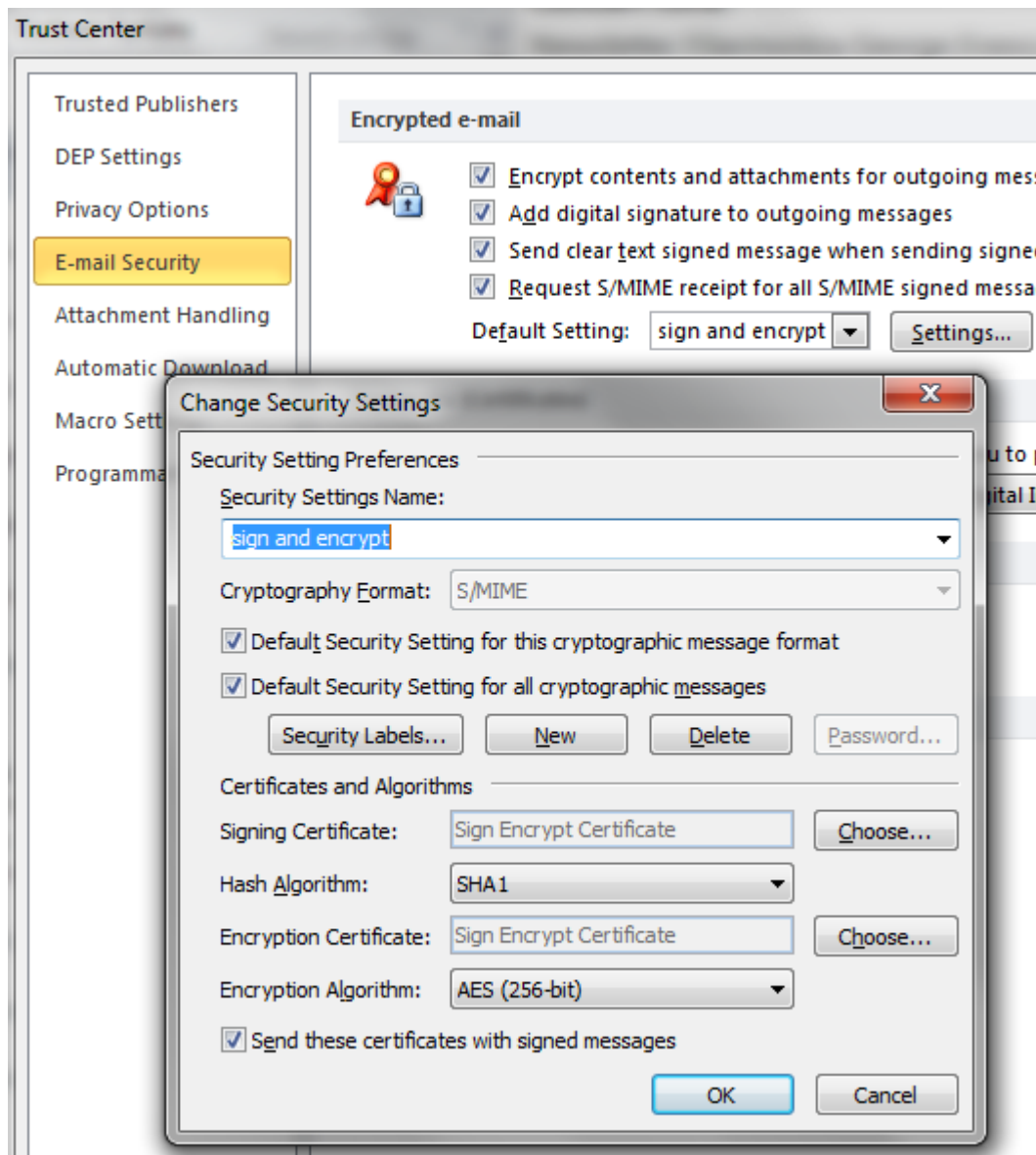
After the certificate is created it must be imported on your system. Double click on the generated .PFX certificate file and click Yes on the dialog box like below.



At this moment, your generated certificate is imported on *Microsoft Store* and it can be used for signing your emails.

Associate the certificate with your email account

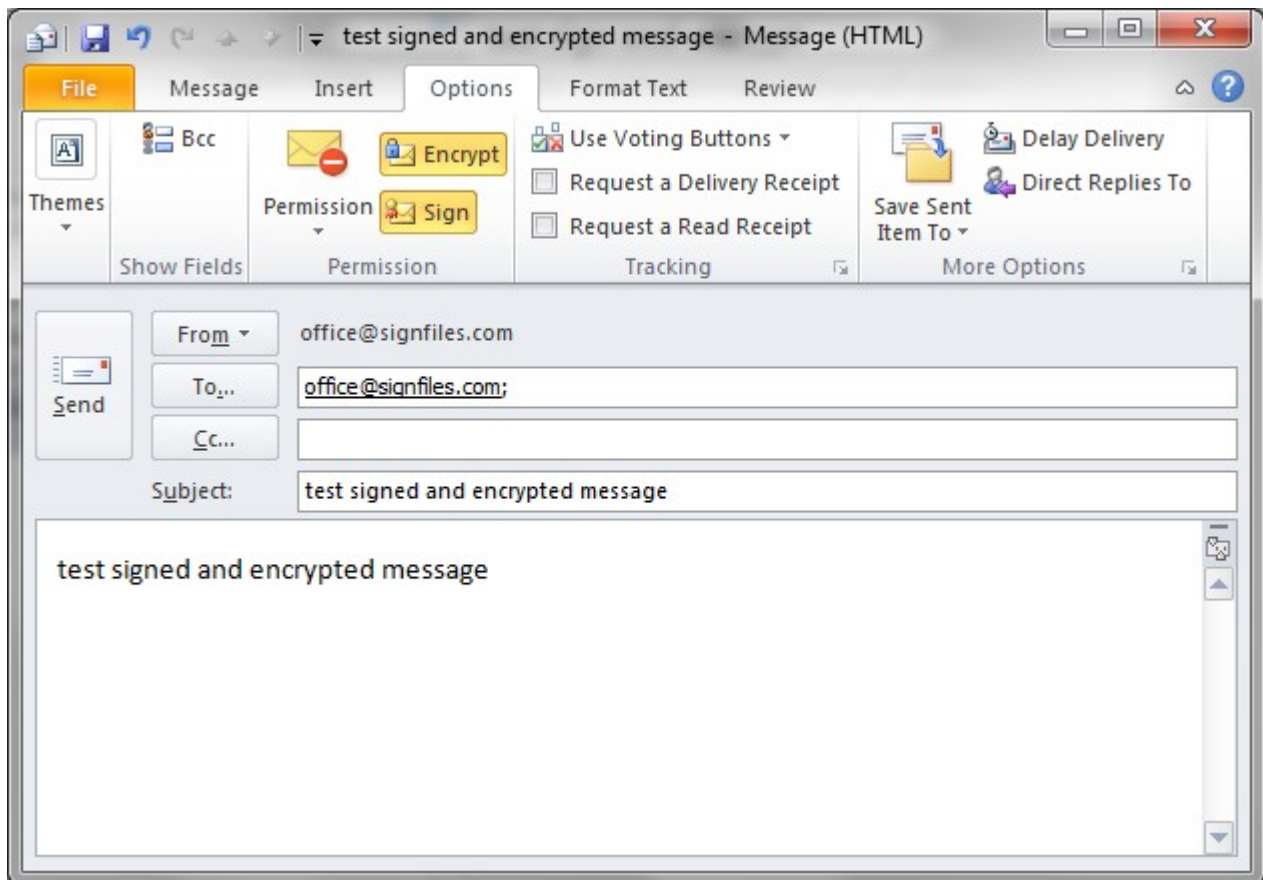
- On Outlook, go to *File – Options – Trust Center* – click on “*Trust Center Settings*” button – *Email Security* – click on the “*Settings*” button.
- Select your signing and encryption certificate by clicking “*Choose*” button.
- Click OK to save the settings.



At this moment, your certificate can be used for signing your email messages.

Create a test signed encrypted email message

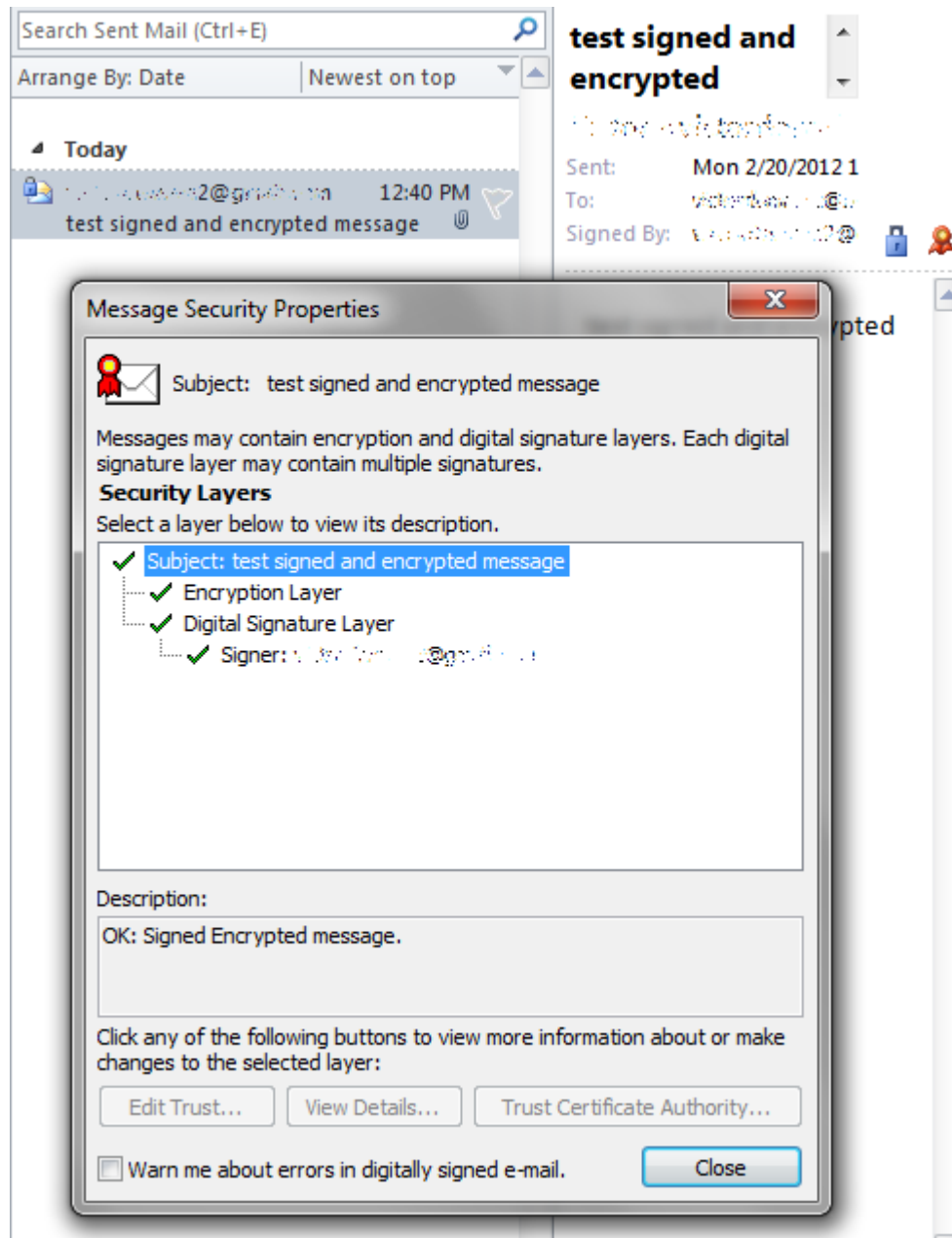
To digitally sign and encrypt an email message using your digital certificate, on *Message* window go to *Options* tab and select *Encrypt* and *Sign* like below.



To test the encryption, add your address to the *Address Book* and send a test signed and encrypted message to yourself.

Verify a signed and encrypted message

On the *Sent Items* folder, open the test message and check the digital signature and encryption like below.



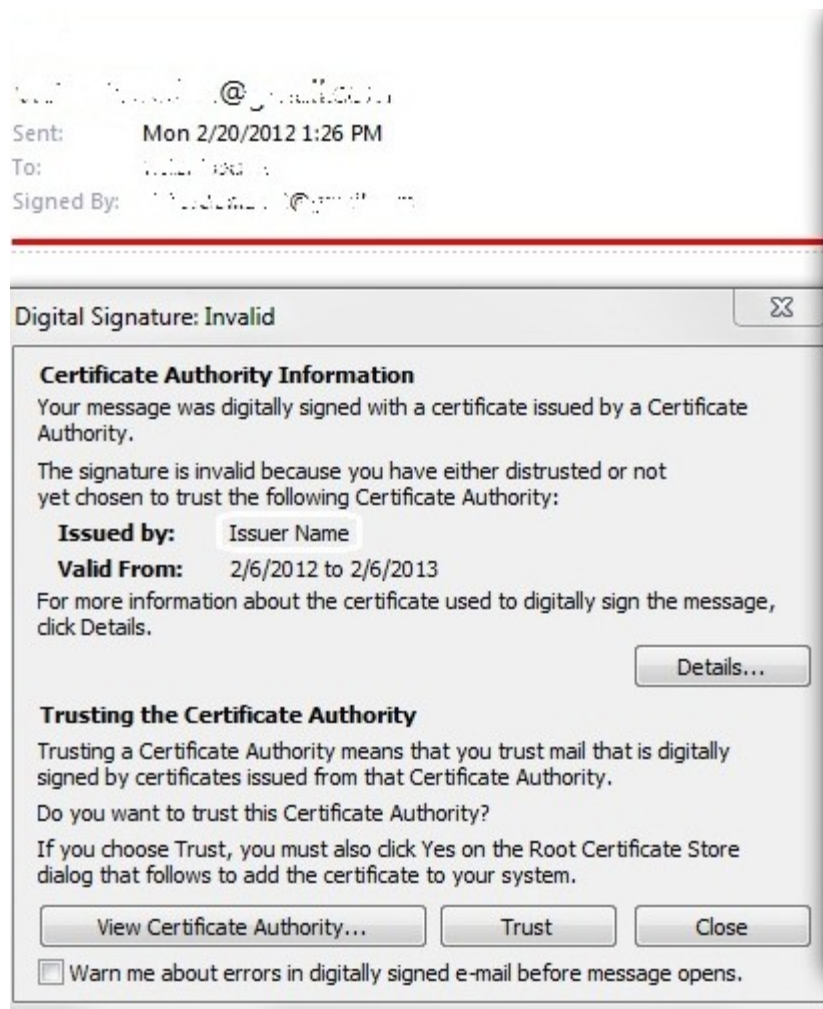
At this moment a test signed and encrypted message was created.

Validating signed email messages on other systems

The digital certificates used for signing email messages are issued by a Certification Authority.

Because this Certification Authority Certificate (Root Certificate) is installed only on your system, to validate the email digital signature on other systems the Root Certificate of the signing certificate must be installed on every system that will receive your signed message.

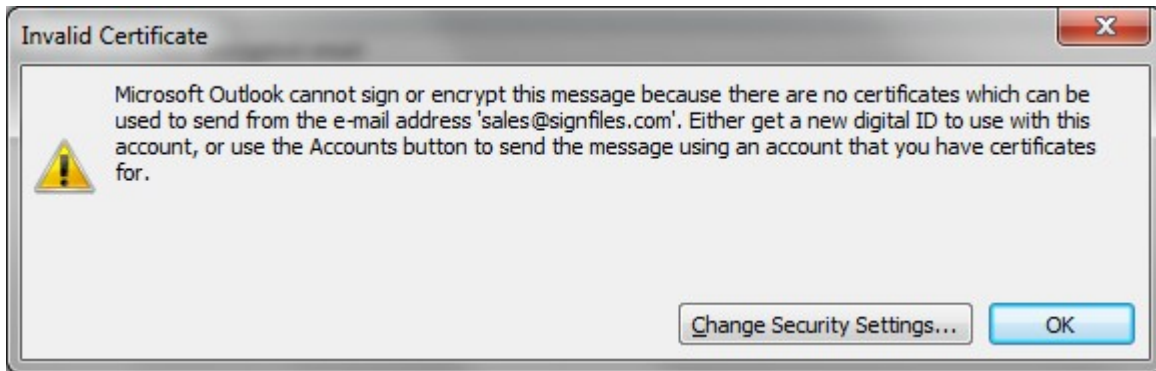
To trust the Root Certificate, click *Trust* button like below.



To validate Digital Certificates in Windows, see this document:
<http://www.signfiles.com/manuals/ValidatingDigitalCertificatesInWindows.pdf>

Error messages

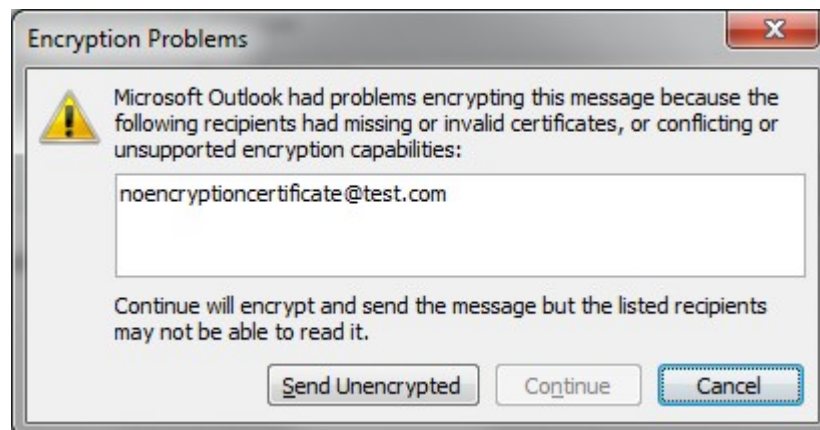
Invalid certificate: This error occurs when you try to send a signed email message but your account does not have any signed certificate associated with it.



Encryption problems: This error occurs when you try to send an encrypted email message to a recipient that is not in your *Address Book* and no certificate is associated with this email address.

To avoid this error, be sure that the recipient has a digital signature associated with his email address.

Usually, the recipient certificate can be obtained from a previous signed message by the recipient.



Open an encrypted message: This error occurs when a email message was encrypted for you but your certificate was deleted from the *Microsoft Store*. On this case, the encrypted email message cannot be recovered.

