MailID S/Mime Setup Guide

Trademarks
ID Control Authentication Server, MailID, HandyID, KeystrokeID, MessageID, RiskID, ID Control OTP Key are trademarks of ID Control BV. All other brand names and product names are trademarks or registered trademarks of their respective owners.

Licence Conditions
Please read your licence agreement with ID Control carefully and make sure you understand the exact terms of usage.

Disclaimer
This document is provided "as is" without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the document. ID Control BV may make improvements of and/or changes to the product described in this document at any time.

Contact
If you wish to obtain further information on this product or any other ID Control BV products, you are always welcome to contact us.

ID Control BV
Van Diemenstraat 202
2518 VH DEN HAAG
The Netherlands

Tel: +31-888-SECURE (732873)
www.idcontrol.com
support@idcontrol.com

Table of Contents

Introduction

This guide briefly explains how to setup you S/MIME infrastructure using MailID email encryption gateway. This guide only gives a brief explanation of S/MIME. For an introduction of MailID's S/MIME support and for more information on administrating MailID see the administration guide.

S/MIME is a widely supported email encryption standard[1]. S/MIME is natively supported by most common email clients like Outlook, Outlook express, Windows Mail, Lotus Notes, Thunderbird, Evolution, Apple Mail, Blackberry etc.

S/MIME supports public key encryption using X.509 certificates. The receiver of a S/MIME message needs a public certificate and an associated private key to be able to receive encrypted email. The sender of an encrypted message uses the public certificate of the recipient to encrypt a message. The recipient needs the private key associated with the public certificate to decrypt the message. Without the correct private key it is not possible to decrypt the message. For digitally signing a message the sender uses his own private key. The recipient can check the signature using the public certificate of the sender. Only certificates that are trusted are used when encrypting a message. Some certificates are implicitly trusted because they have been issued by a trusted root authority. A trusted root authority is a CA issuer that is ultimately trusted. A trusted root can issue intermediate CA certificates. The intermediate certificate again can issue other certificates. This forms a chain of trusted certificates until and end-user certificate is reached. Certificates issued by a trusted root are trusted if the complete certificate chain is trusted (I.e. no certificate in the chain is revoked, expired etc.). A signed message includes the certificate of the signer. The recipient extracts the certificate from the signed message and stores it in the certificate store. The recipient can now reply encrypted because there is a certificate available for the recipient.

MailID has support for S/MIME email encryption and digital signatures. Because the sender and receiver both require a certificate and private key MailID has a built-in CA server that can be used to issue certificates and keys to internal and external users. Once they have acquired a certificate external users can use any S/MIME capable email client to start sending en receiving encrypted email. External and internal users don't need to use the build-in CA. If an external recipient already has a S/MIME certificate, for example a free Thawte certificate, or if they don't want the MailID server to store a backup-copy of the private key, they can use their own existing certificate or get a certificate from another CA. A big advantage of using MailID's built-in CA server, as opposed to getting your own certificate, is that it's much easier for an external recipient to install the pfx file containing the private key than it is to request a certificate from a third-party CA. Another advantage is that MailID functions as a "key escrow". If an external recipient looses the certificate and private key because of a system crash and forgot to create a backup the recipient can no longer decrypt incoming email. Because a backup of the certificate and key is stored on the MailID server the system administrator can securely sent a new copy to the recipient.

Sometimes you no longer want to use a certificate. For example when a private key has been leaked or

1 See http://www.ietf.org/html.charters/smime-charter.html for an overview of S/MIME related standards.

when a recipient no longer has access to an email address. A blacklist of certificates you no longer should use is called a certificate revocation list (CRL). A CRL is a list of certificate serial numbers that have been revoked by the issuer of the CRL. Some certificates contain a URL that point to the location from which an updated CRL can be downloaded from. This is known as a “CRL distribution point”. MailID periodically scans all the certificates from the certificate stores and downloads all the CRLs it can find. MailID’s built-in CA allows you to create a CRL for your CA certificates. This allows you to revoke certificates issued by your CA which you no longer trust or no longer use.

Quick setup

We will provide a short guide on how to setup MailID for S/MIME. We assume that you have read the administration guide and have already setup MailID to sent and receive email. If you would like the private key password to be sent by SMS Text message you should make sure that the SMS gateway is setup correctly.

Create a CA

You need to create a new CA which will be used for issuing new certificates (skip this if you already have setup a CA).

Open the create CA page by clicking “CA → Create new CA”. This should open the following page (Figure 1: Create new CA).

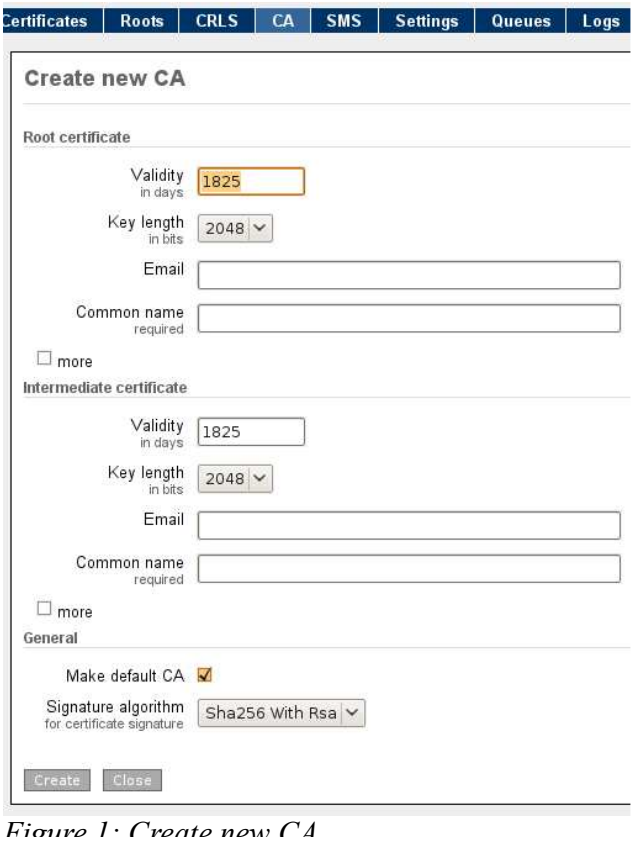


Figure 1: Create new CA

Fill in the form:

1. Set validity at 1825 days (5 years) and key length at 2048[2].
2. Skip email field (i.e. leave it empty).
3. Set a common name that uniquely identifies your CA. The root common name must be different from the intermediate common name.
4. Alternatively you can set the organization, first name and last name (select the more checkbox).
5. Make sure that "make default CA" is selected.
6. Set signature algorithm to "SHA256 With RSA".

Click the "Create" button to create the new CA.

Add certificates for internal users

For every internal user that needs to send S/MIME encrypted email you need to create a certificate[3]. You first have to make sure that the domains for which you receive email are internal domains and allow encrypted S/MIME messages to be sent.

For each domain for which you receive email

1. Add the domain.
2. Set "Encrypt mode" to "Allow"[4].
3. Set the "Locality" property to "Internal".
4. Select the S/MIME "Allow" property.

For each internal user:

1. Create a user.
2. Create a new end-user certificate by clicking CA*.

*instead of clicking CA you can click on the certificate icon 
for the user on the users page and then click on "create new certificate". This way the email address is already filled-in.

The following "Create new end-user certificate" page should be opened (see Figure 2: Create new end-user certificate).

2 Unless you have different requirements it's best to leave the default values.
3 Even though it's possible to sent encrypted email without the sender having a certificate it's better to create a certificate for every sender because otherwise the external recipient won't be able to reply encrypted.
4 Alternatively you can set it to "No encryption" and enable the subject trigger.

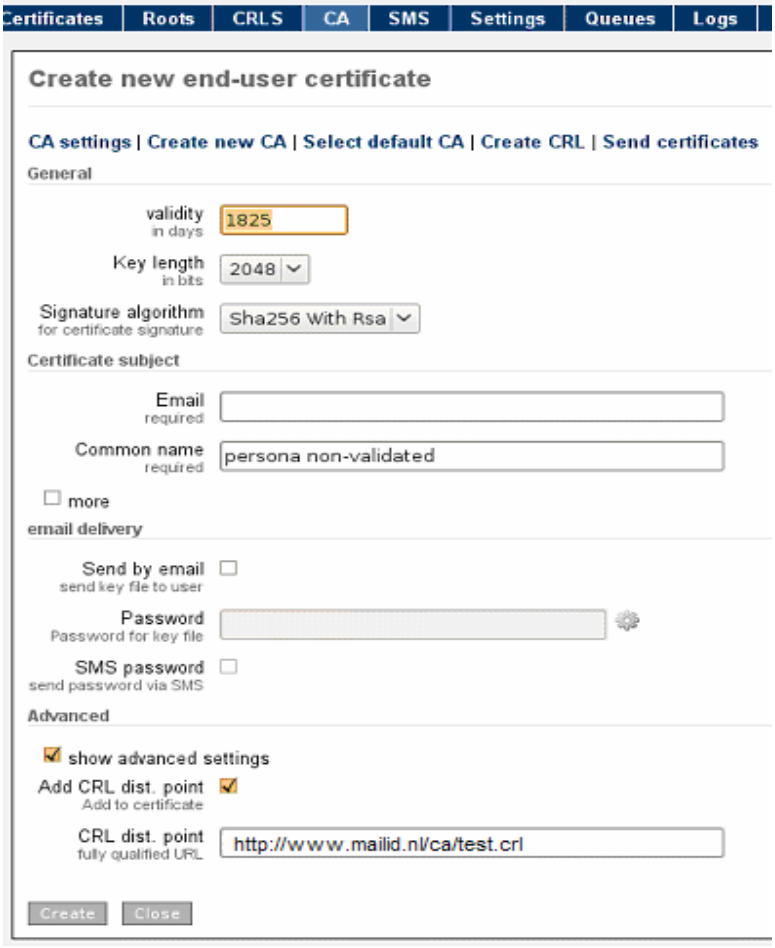


Figure 2: Create new end-user certificate

1. Set validity at 1825 days (5 years) and key length at 2048[5].
2. Set signature algorithm to "SHA256 With RSA".
3. Email should be set to the email address of the user.
4. Leave the common name as-is (or set it to a identifier that identifies the user).
5. Alternatively you can set the organization, first name and last name (select the more checkbox).
6. Add a CRL distribution point if required. See Appendix A for more info on adding a CRL distribution point.

Because the certificate is for an internal user you don't need to sent the certificate by email because the gateway will encrypt and decrypt messages for the internal user.

Click "Create" to create the certificate and private key. The certificate and private key will be added to the certificates store.

5 Unless you have different requirements it's best to leave the default values.

Add certificates for external recipients

External recipients need to have a certificate and private key to start sending and receiving S/MIME encrypted email. The external recipient can request a certificate from an external CA, like for example Thawte, or get a certificate from the built-in MailID CA. As it is much easier for an external recipient to install a certificate from a pfx file we will explain how to create a certificate for an external recipient. For every external recipient that needs to receive S/MIME encrypted email you need to create a certificate.

For each external user:

1. Create a user.
2. Make sure that S/MIME "Allow" property is set.
3. Create a new end-user certificate by clicking CA*.

*instead of clicking CA you can click on the certificate icon
for the user on the users page and then click on "create new certificate". This way the email address is already filled-in.

The "Create new end-user certificate" page should be opened (see Figure 2: Create new end-user certificate).

1. Set validity at 1825 days (5 years) and key length at 2048[6].
2. Set signature algorithm to "SHA256 With RSA".
3. Email should be set to the email address of the external recipient.
4. Leave the common name as-is (or set it to a identifier that identifies the recipient).
5. Alternatively you can set the organization, first name and last name (select the more checkbox).
6. If you want to send the certificate and private key using a password encrypted pfx file you should select "Send by email" and create a secure password (the 'gear' icon generates a secure random password).
7. If the recipient should receive the password via SMS Text message you should select "SMS password" and make sure that the recipients telephone number is set for the user.
8. Add a CRL distribution point if required. See Appendix A for more info on adding a CRL distribution point.

Click "Create" to create the certificate and private key. The certificate and private key will be added to the certificates store. If "Send by email" was selected the certificate and private key will be stored inside a password encrypted pfx file and sent to the recipient. If the "SMS password" was selected the password will be sent to the recipient via a SMS Text message. If the password was not sent via a SMS Text message you should use an alternative way to let the recipient know what the password is[7].

The recipient receives a message with the password protected pfx file attached. The pfx file with the

6 Unless you have different requirements it's best to leave the default values.

7 You should use a different means of sending the password than email because you need be sure that password and pfx file are not sent using the same communication channel.

certificate and private key should be installed into the recipients email client. The pfx installation procedure if different for every mail client.

Email client setups

The next chapters will explain how to install the pfx, sent by email to the external recipients, for the most popular email clients.

Outlook

The Outlook recipient receives the following message[8] containing an attached password encrypted pfx:

Figure 3: Outlook pfx email

Importing the pfx

The recipient should take the following steps:

1. Double-click the key.pfx file and start the “certificate import wizard”.
2. Step through the “certificate import wizard” using all default values.
3. If asked for the private key password, fill-in the password provided to you.
4. Press Next for all pages.
5. The final page asks you to accept the trusted root certificate. You must select “Yes”.

The above steps will now be explained in more detail.

Double-click the attached pfx file (or alternatively you can save the pfx file and open it from the Explorer by double-clicking it). A warning will be shown asking you if you want to open the pfx file (see Figure 4: Outlook opening Mail Attachment). Click the “Open” button.

8 In this example the password was sent via a SMS Text message. The message is slightly different when the password was not sent via SMS.

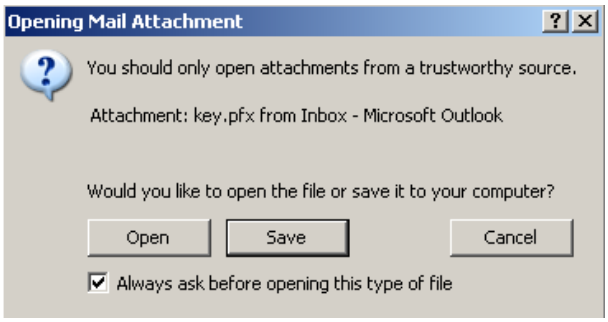


Figure 4: Outlook opening Mail Attachment

The “certificate import wizard” will be started which will import the password protected certificate and

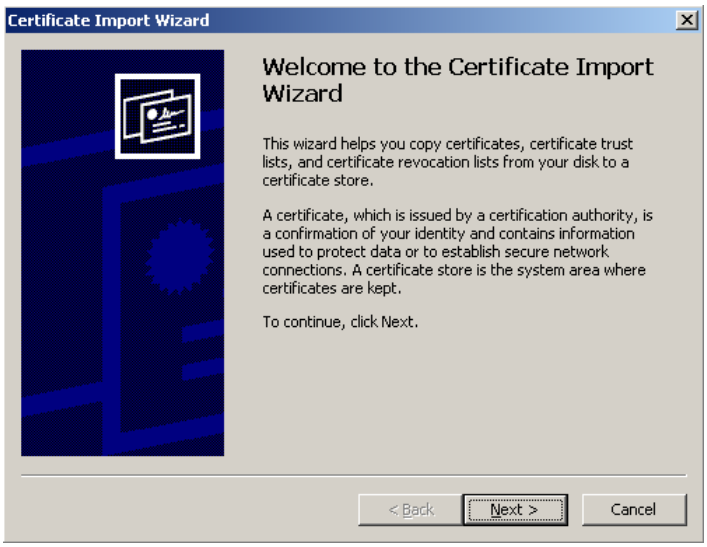


Figure 5: Outlook Certificate Import Wizard

private key.

Click the Next button until you come to password page

You should enter the password for the pfx file.

Optionally you can select the two following options: Enable strong private key protection

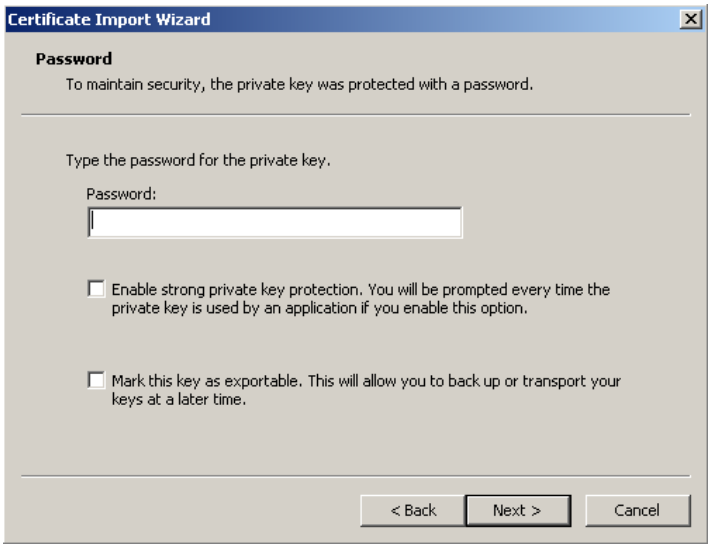


Figure 6: Outlook Certificate Import Wizard password

If this option is selected Windows will always ask for your permission when a program tries to access your private key. You are advised to leave it unselected.

Mark this key as exportable

If this option is selected you are able to export the private to a new pfx file. This allows you to create backups of your private keys. If you want to create backups of your private keys you should select this option.

Click the Next button and on the Next pages leave the defaults until you get to the "Completing the Certificate Import Wizard" page.

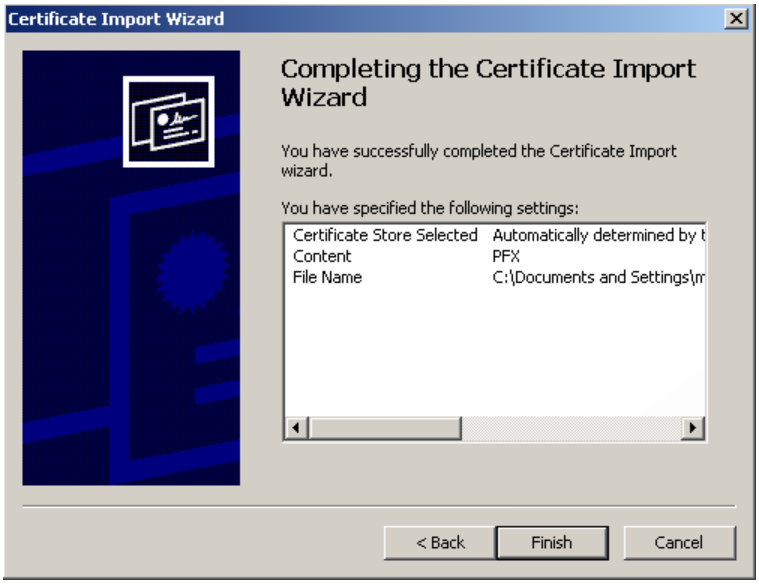


Figure 7: Outlook Certificate import wizard finish

On the final page you should click "Finish" to start importing the certificate and private key.

The pfx file not only contains the end-user certificate and private key but also the root and intermediate certificate. The import wizard will also try to import the root and intermediate certificate. Windows asks for permission when importing a root certificate (see Figure 8: Windows security warning).

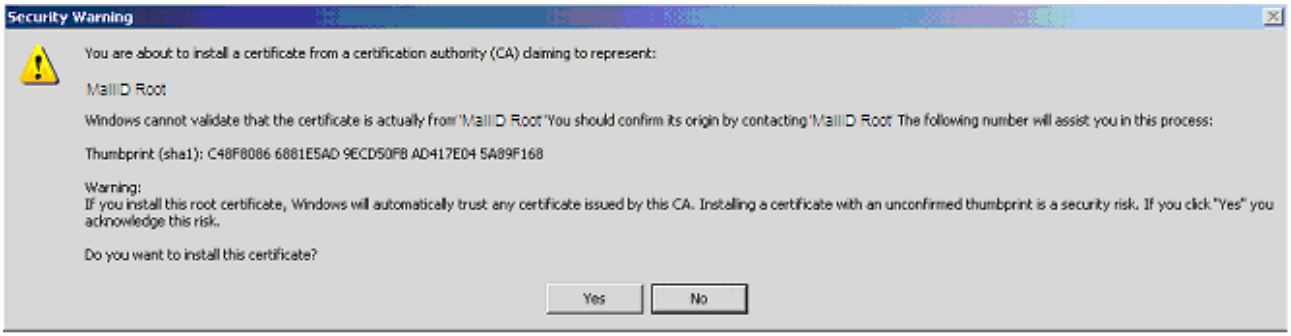


Figure 8: Windows security warning

Click "Yes" to accept the root certificate. The root certificate should be accepted otherwise it won't be possible to send encrypted email from Outlook (it's still possible to receive encrypted email even when you do not accept the root certificate).

Now that you have installed a certificate and private key you are able to receive encrypted email.

Receiving signed and encrypted email

A signed and encrypted message looks like:

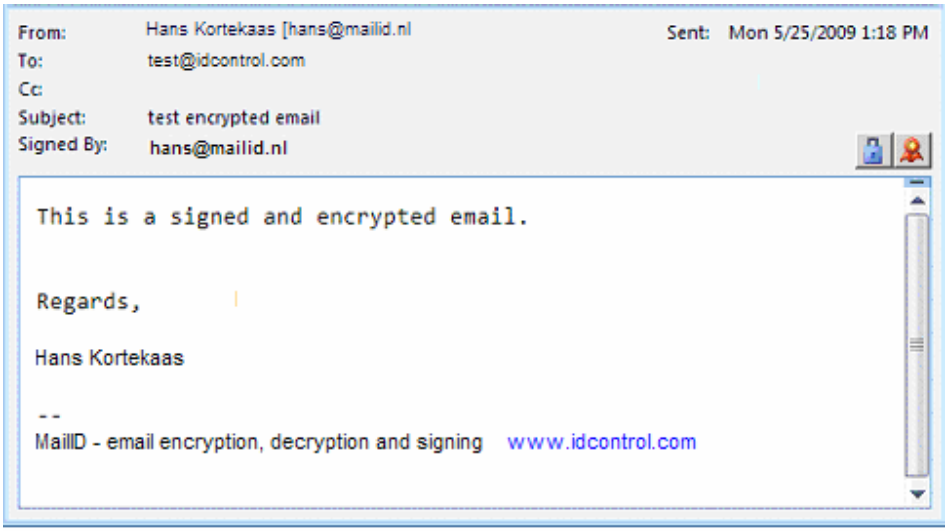


Figure 9: Outlook signed and encrypted

The 'padlock' shows that the message was encrypted and the 'ribbon' shows that the message was signed.

The signed and encrypted message contains the public certificate of the sender. To make it possible to reply to the message you should associate the public certificate with the sender. This can be done by clicking on the senders email address (the from header), right-click and select "Add to Outlook Contacts" (see Figure 10: Add to Outlook Contacts).

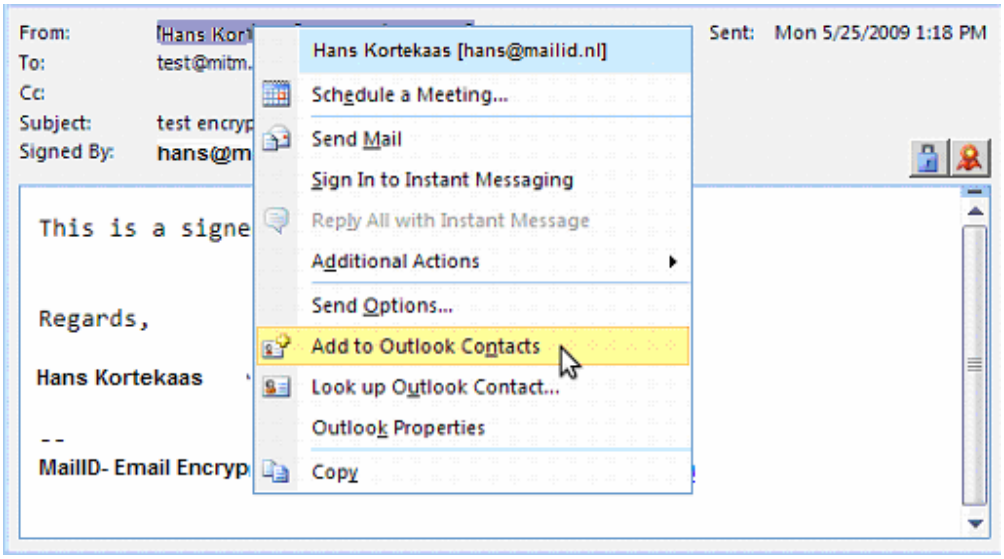


Figure 10: Add to Outlook Contacts

Save the newly added Outlook contact. If the contact is already part of your contacts you will receive a "Duplicate Contact Detected" warning.

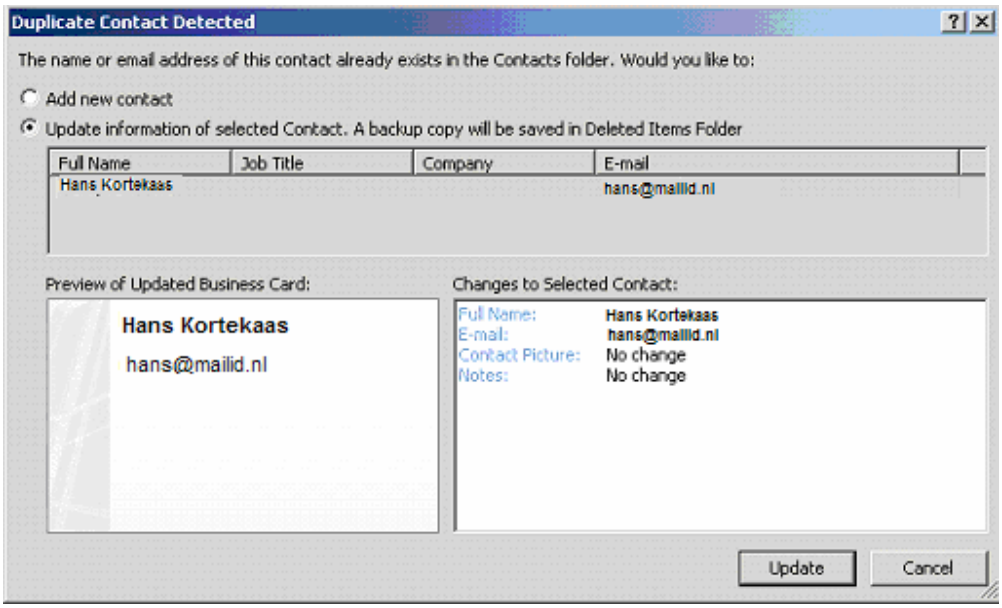


Figure 11: Outlook Duplicate Contact Detected

Click "Update" to add the certificate to the contact.

Note: You will only need to associate the certificate with the sender contact the first time you receive a signed and encrypted email.

Sending signed and encrypted email

Sending a signed and encrypted email is similar to sending a normal email. You only need to select the sign and encrypt options. Outlook 2007 adds these icons to the tool-bar (see Figure 12: Outlook sign and encrypt).

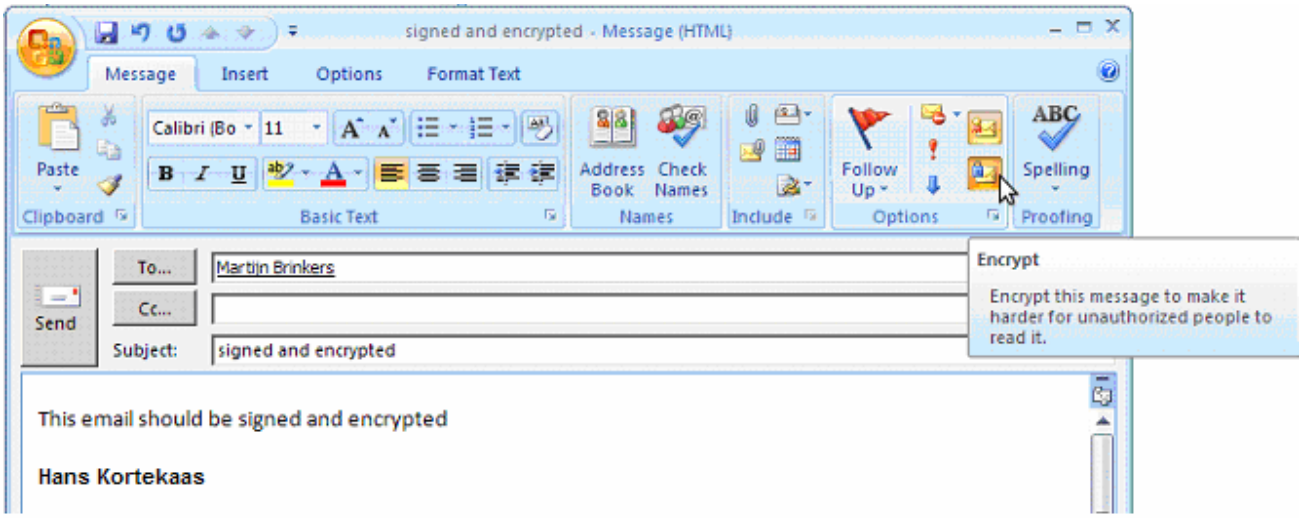


Figure 12: Outlook sign and encrypt

With older Outlook versions you either have to add the sign and encrypt icons manually to the tool-bar or you can enable sign and encrypt by opening the message options and selecting the "Security Settings..." (see Figure 13: Outlook Security Properties).

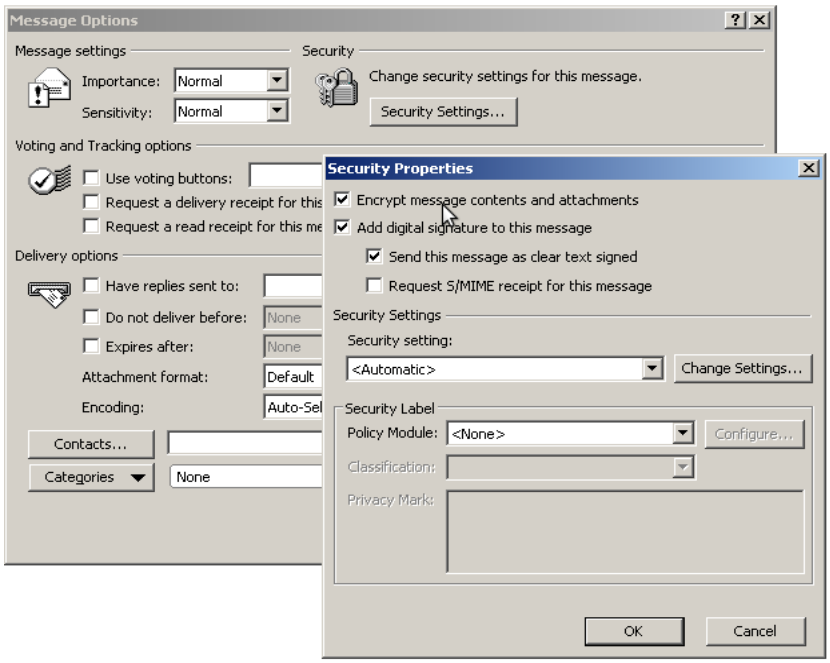


Figure 13: Outlook Security Properties

For encryption the certificate of the recipient need to be available. If Outlook cannot find a certificate for one of the recipients the following warning will be shown:

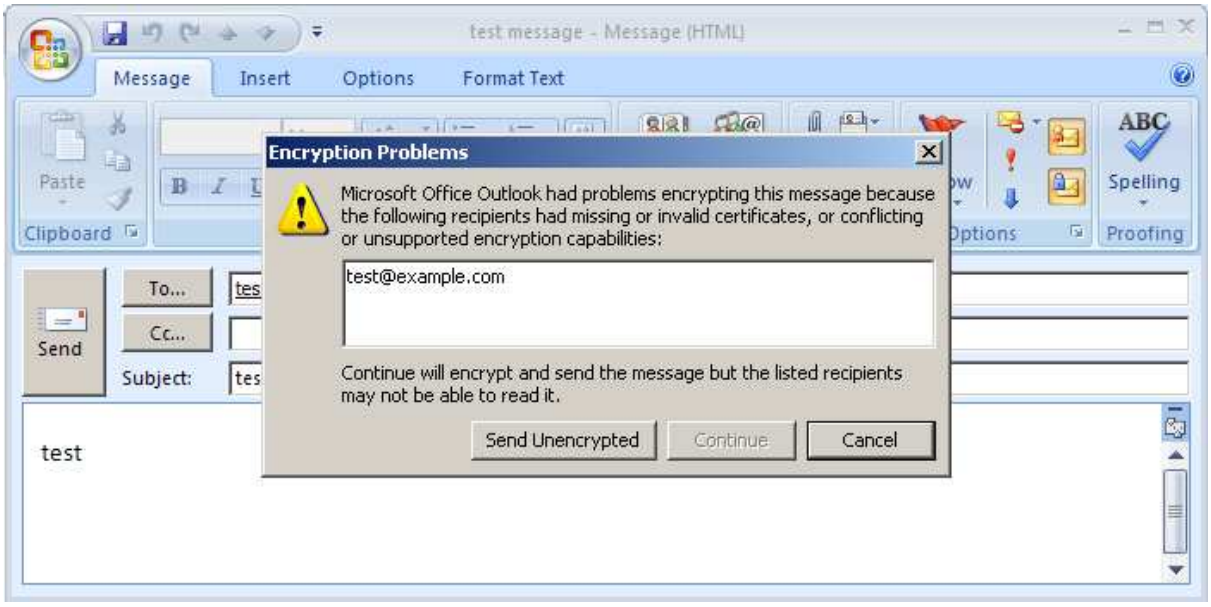


Figure 14: Outlook encryption problems

You will get this warning when the recipient does not have a certificate associated with the contact. If you have a copy of the recipients certificate you can directly import it into the contacts certificate list. Open the contact and select the "Certificates" for the contact[9] and import the certificate file (.cer or .p7b).

9 In Outlook 2003 you should open the "Certificates" tab.

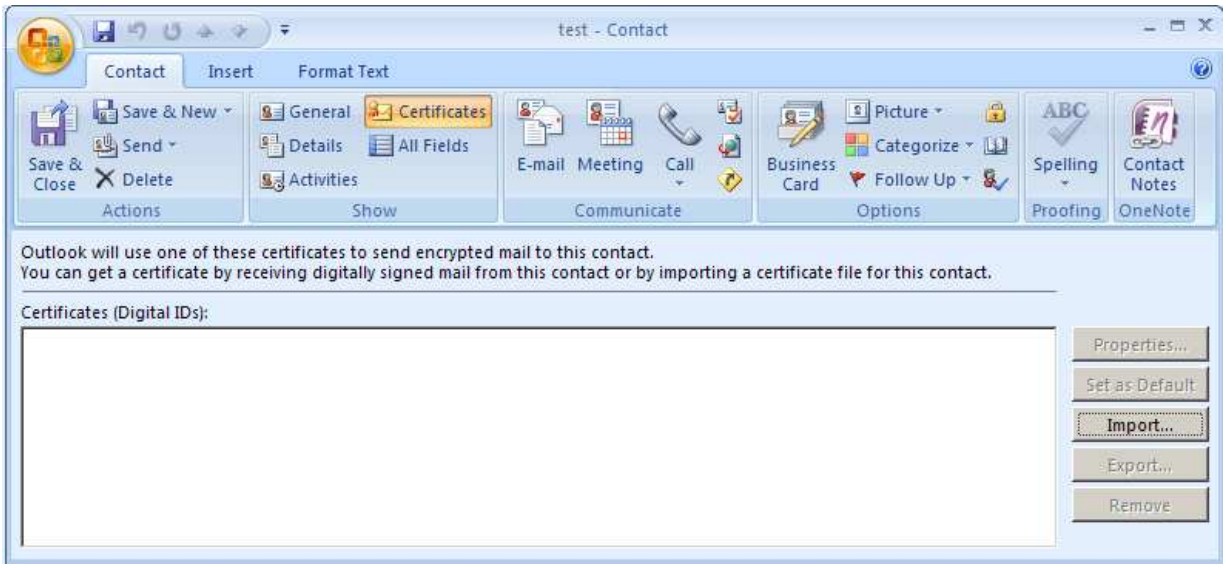


Figure 15: Outlook contact certificates

Outlook express

The Outlook express recipient receives the following message[10] containing an attached password encrypted pfx:

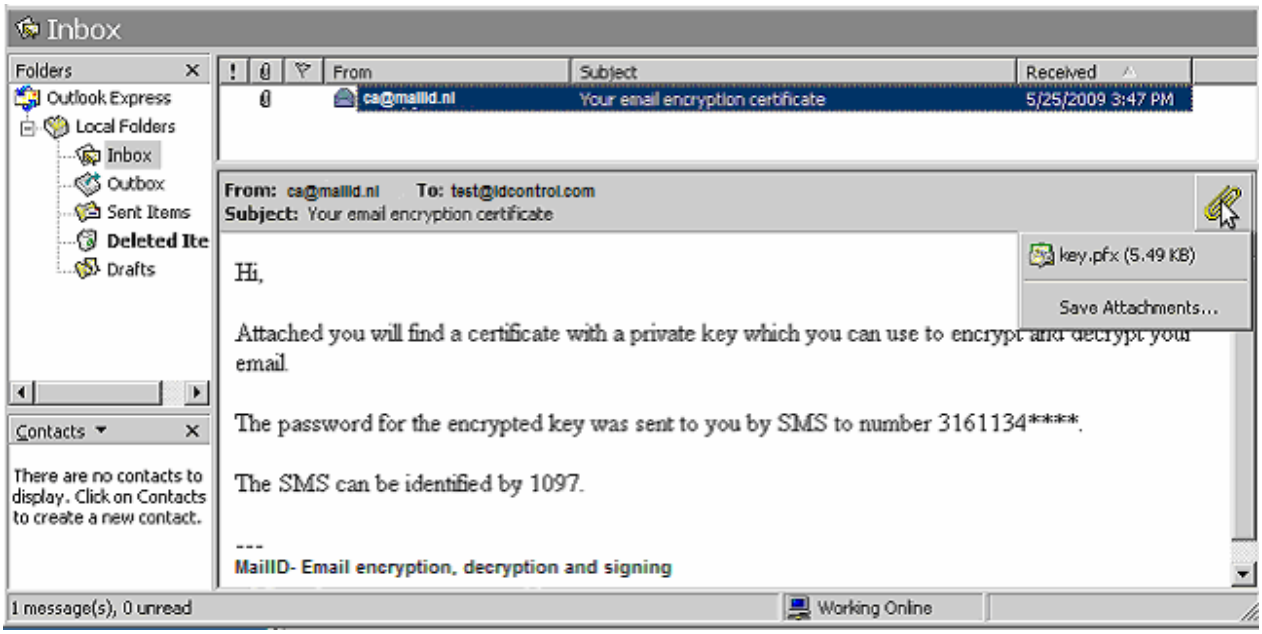


Figure 16: Outlook express PFX email

Importing the pfx

Importing the pfx from Outlook express into windows is similar to importing it from Outlook so we refer to section Importing the pfx from the Outlook chapter.

Receiving signed and encrypted email

A signed and encrypted message in Outlook express is automatically decrypted. The 'ribbon' shows that the message is signed and the 'padlock' shows that the message is encrypted (see Figure 17: Outlook express signed and encrypted)

10 In this example the password was sent via a SMS Text message. The message is slightly different when the password was not sent via SMS.

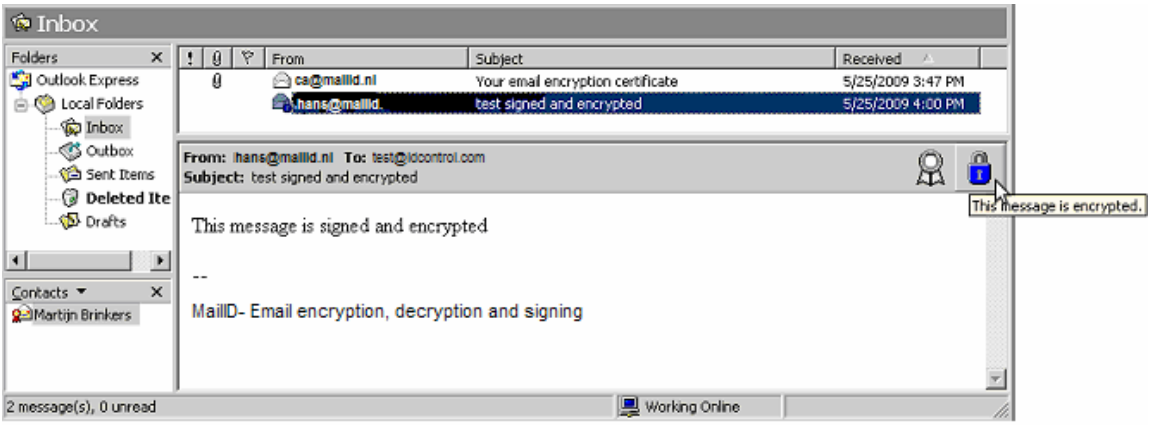


Figure 17: Outlook express signed and encrypted

Outlook automatically associates the certificate of the sender with the senders contact (see the contact on the left-hand corner with the red 'ribbon').

Sending signed and encrypted email

Sending a signed and encrypted email is similar to sending a normal email. You only need to select the sign and encrypt options (see Figure 18: Outlook express sign and encrypt).

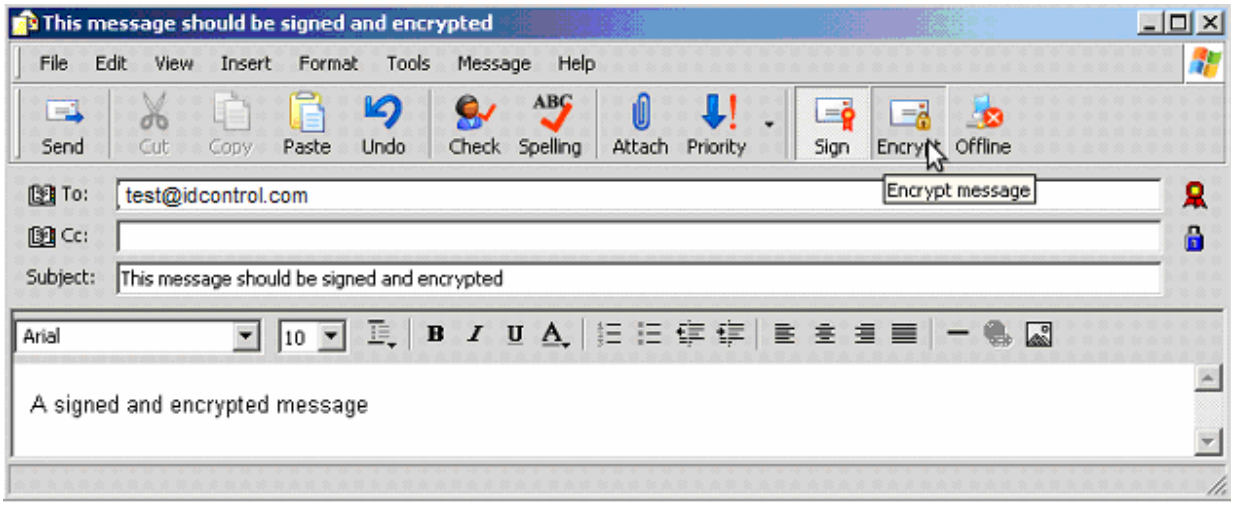


Figure 18: Outlook express sign and encrypt

Thunderbird

The Thunderbird recipient receives the following message[11] containing an attached password encrypted pfx:

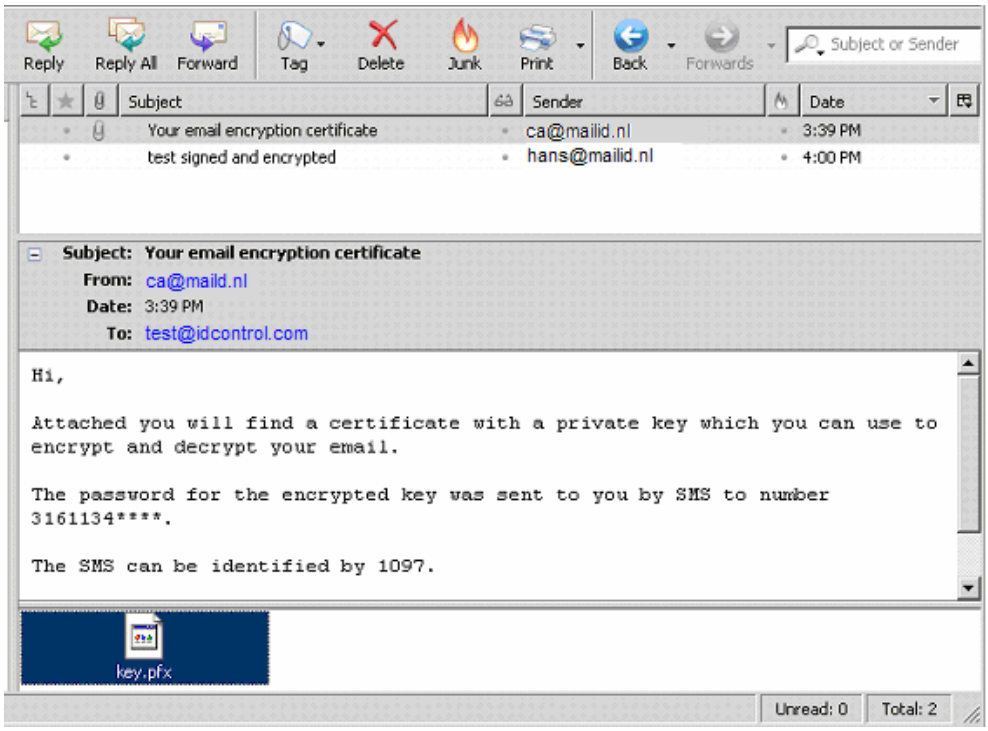


Figure 19: Thunderbird PFX email

Importing the pfx

You first need to save the pfx attachment before you can import it into Thunderbird. Save the key.pfx file on the desktop (or on any other location you normally use for your attachments).

Now open the certificates options from the tools menu Tools → options, select the Advanced settings and open the Certificates tab (see Figure 20: Thunderbird certificates options).

11 In this example the password was sent via a SMS Text message. The message is slightly different when the password was not sent via SMS.

Figure 20: Thunderbird certificates options

Now click the "View Certificates" button. This opens the "Certificate Manager" (see Figure 21: Thunderbird Certificate Manager).

Figure 21: Thunderbird Certificate Manager

Now click the "Import" button and select the pfx file you have previously saved.

The first time you add a certificate you are asked to set a "Master Password" (see Figure 22: Thunderbird change master password). The master password is used to protect the private keys stored in Thunderbird. The private keys are encrypted with the master password to ensure that only you can access the private keys. You only have to set the master password once.

Note: this is NOT the password for the pfx file that has been handed out to you! The master password should be chosen by you.

Figure 22: Thunderbird change master password

Now that you have set the master password you are now asked for the password of the password protected pfx file. This is the password that was given to you via SMS Text message or in some other way.

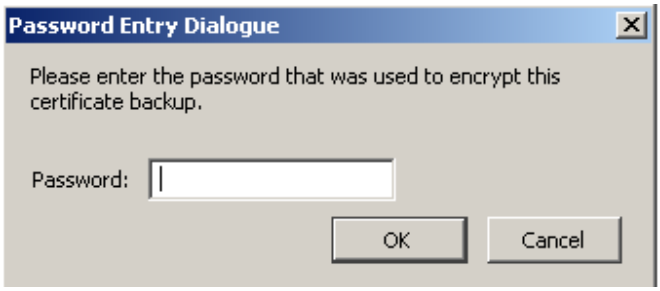


Figure 23: Thunderbird Password Entry Dialog

Enter the pfx password and press “OK”. If the certificate and private key from the pfx were installed correctly the following dialog should be shown:

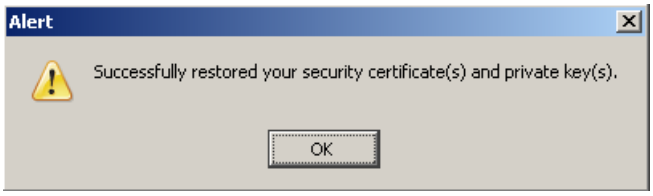


Figure 24: Thunderbird certificate restored

The certificate with the private key and the root and intermediate certificates have now been installed. You should now manually trust the root certificate because it is not automatically trusted. You first need to find out which root you need to trust. First select your newly installed certificate (see Figure 25: Thunderbird select personal certificate)

Double-click the certificate you just installed. The certificate details dialog should pop-up (see Figure

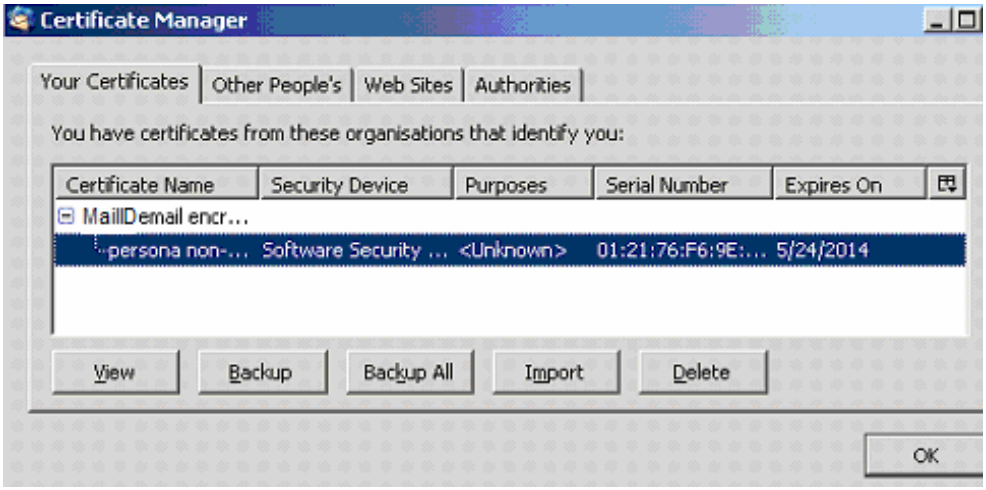


Figure 25: Thunderbird select personal certificate

26: Thunderbird certificate viewer). The first entry in the "Certificate Hierarchy" is the root certificate. You should remember the name because you need it in the next steps.

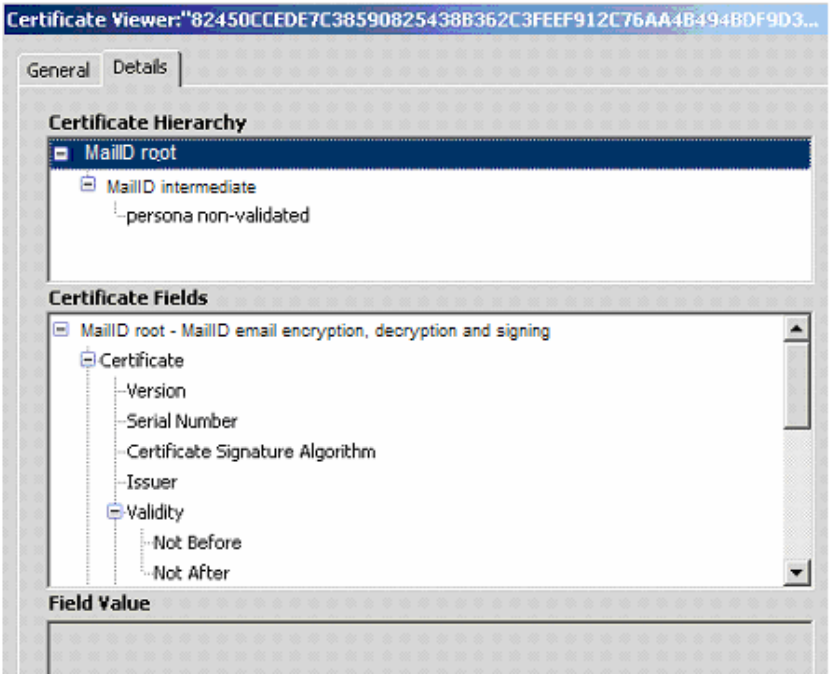


Figure 26: Thunderbird certificate viewer

Now open the “Authorities” tab on the “Certificate Manager” and select the correct root certificate (see Figure 27: Thunderbird authorities).

Figure 27: Thunderbird authorities

Select the correct root certificate and click the “Edit” button. In the following dialog you must select “This certificate can identify mail users.” (see Figure 28: Thunderbird Edit CA certificate trust

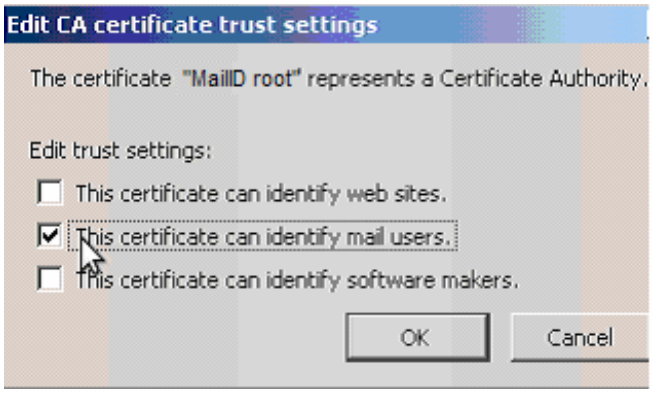


Figure 28: Thunderbird Edit CA certificate trust settings

settings).

Now close all dialogs. We now need to associate the certificate with your account.

Open tools → Account settings... and select “security” options of your email account (see Figure 29: Thunderbird account settings).

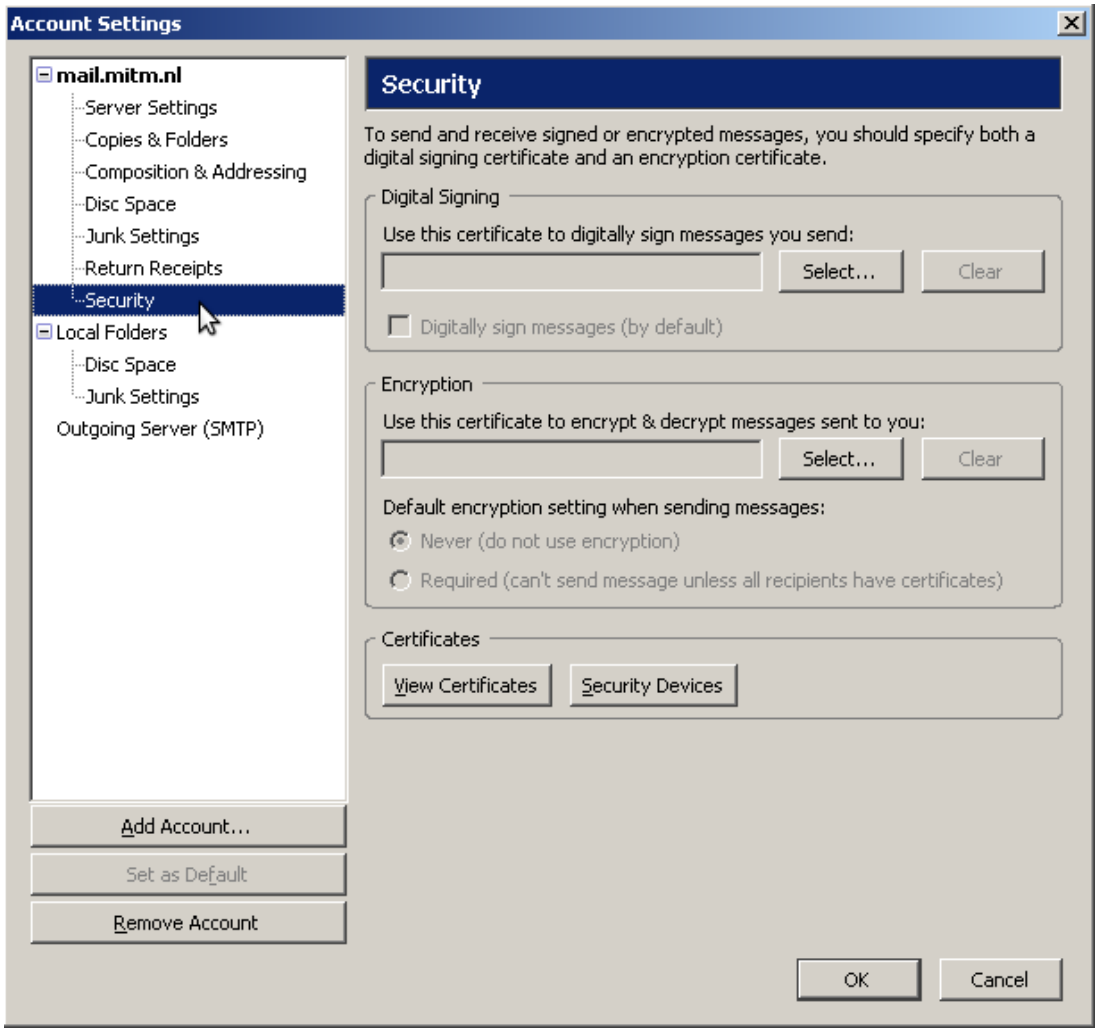


Figure 29: Thunderbird account settings

Now click the “Select...” button for “Digital Signing” and “Encryption” and select the newly added certificate. Leave all other settings to default and close the account settings.

Thunderbird is now setup to start sending and receiving signed and encrypted email.

Receiving signed and encrypted email

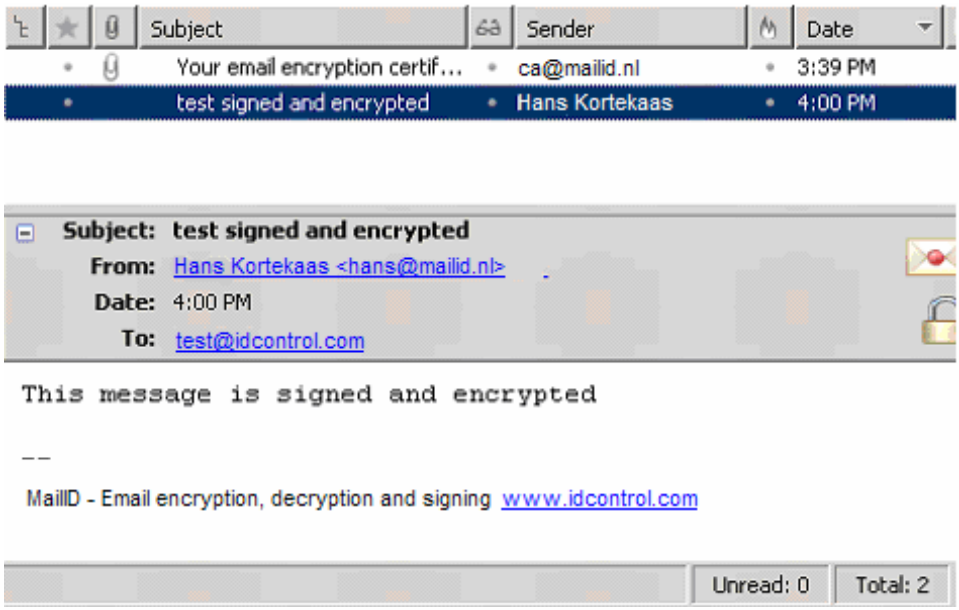


Figure 30: Thunderbird signed and encrypted email

A signed and encrypted email in Thunderbird looks as follows: Shows that the message has been signed and shows that the message has been encrypted.

Sending signed and encrypted email

You should enable “Encrypt This Message” and “Digitally Sign This Message” from the security pull-down menu.

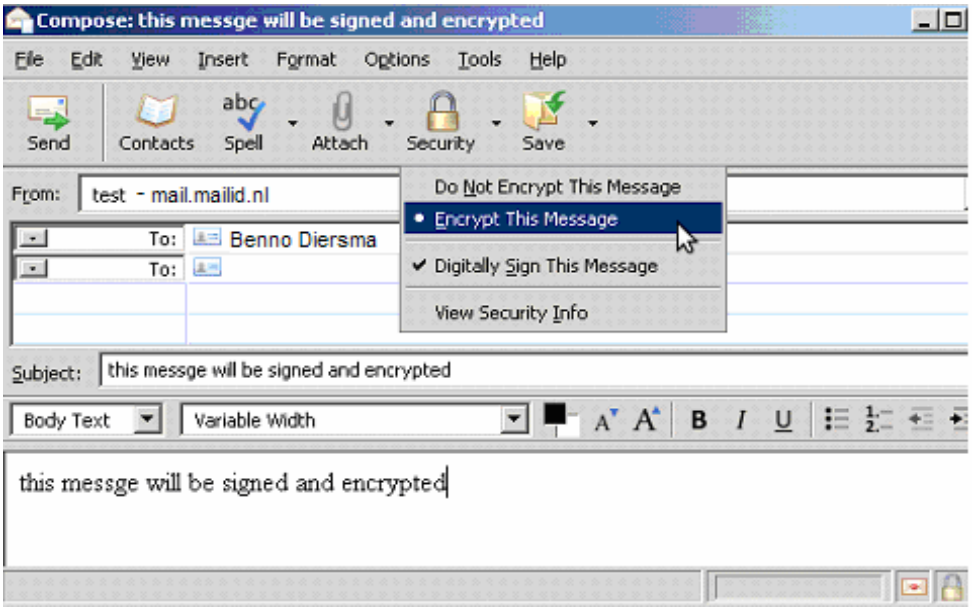


Figure 31: Thunderbird sign and encrypt

Apple Mail

Importing the pfx

Double-click the pfx file. This will open the Keychain Access application which will try to import the certificate and private key. If the Keychain Access application is not opened, drag the pfx file onto the Keychain Access application icon (/Applications/Utilities).

You are now asked for the password of the password protected pfx file. This is the password that was given to you via SMS Text message or in some other way.

The pfx file not only contains the end-user certificate and private key but also the root and intermediate certificate. The Keychain Access will also try to import the root and intermediate certificate and permission is asked when importing a root certificate (see Figure 32: Mac Mail Keychain Access[12]). You should select “Always trust”.

Figure 32: Mac Mail Keychain Access

After installing the private key you should restart Mail. Apple Mail is now setup for sending and receiving signed and encrypted email.

When Apple Mail needs decrypt a message it has to access the private key. Apple Mail will ask for permission for accessing the ‘PrivateKey’.

12 This example is in Dutch but it should look similar in any other language.

Receiving signed and encrypted email

A signed and encrypted email in Mail looks as follows:

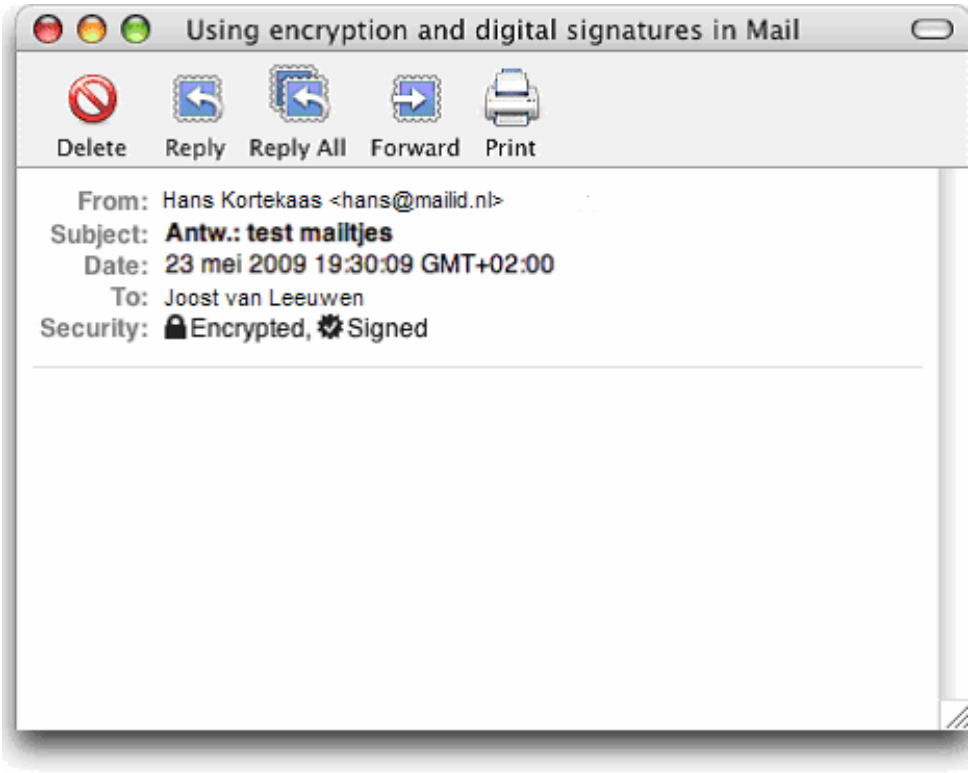


Figure 33: Apple Mail signed and encrypted

shows that the message was encrypted and shows that the message was signed.

Sending signed and encrypted email

You can sign and encrypt a message in the compose window by selecting the sign and encrypt options:

Encrypt: Sign:

Gmail

If you access Gmail with pop3 or imap you are using normal email client (like Outlook) and should use the guide for your email client. If you access Gmail using the Gmail web interface you will need a special add-in for reading and sending S/MIME messages because Gmail does not natively support S/MIME. There is a cross-platform add-in available for Firefox that allows you to read and send S/MIME encrypted email directly from Gmail's web interface.

Installing the add-in

Requirements: Firefox

The Gmail add-in can be downloaded from https://addons.mozilla.org/en-US/firefox/addon/592. Just install the add-in by clicking the "Add to Firefox" button.

Importing the pfx

The email with the password protected pfx file containing your certificate and private key will look similar to:

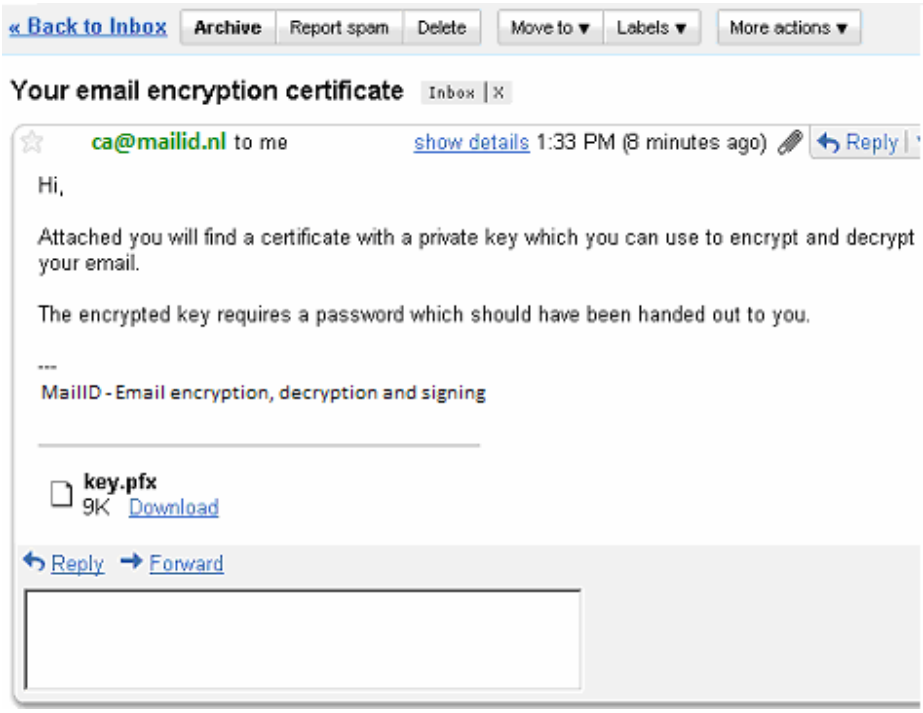


Figure 34: Gmail PFX email

Because the Gmail add-in works from Firefox you will need to import the certificate and private key into Firefox. This requires first that you save the attached pfx file onto your local file system by downloading the pfx file.

Now open the Firefox encryption settings using tools → options... and then open the “Advanced” options (see Figure 35: Firefox Advanced settings).

Figure 35: Firefox Advanced settings

Now open the the Certificate Manager by clicking the “View Certificates” button. In the Certificate Manager select the “Your Certificates” tab (see Figure 36: Firefox Certificate Manager).

Figure 36: Firefox Certificate Manager

Now click the “Import” button.

The first time you add a certificate you are asked to set a “Master Password”. The master password is used to protect the private keys stored in Firefox. The private keys are encrypted with the master password to ensure that only you can access the private keys. You only have to set the master password once.

Note: this is NOT the password for the pfx file that has been handed out to you! The master password should be chosen by you.

Figure 37: Firefox master password

Now select the pfx file you have previously saved. A dialog pop-up asks for the pfx password (see Figure 39: Firefox pfx installed). This is the password that was given to you via SMS Text message or in some other way.

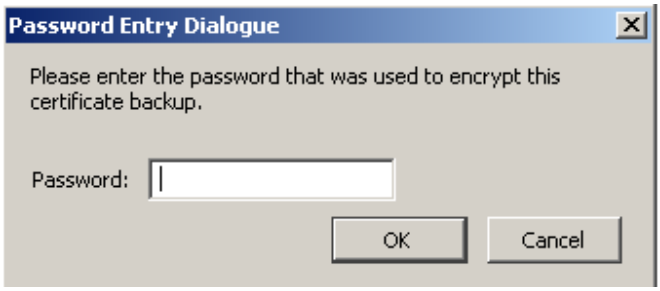


Figure 38: Thunderbird Password Entry Dialog

Enter the pfx password and press “OK”. If the certificate and private key from the pfx were installed correctly the following dialog should be shown:

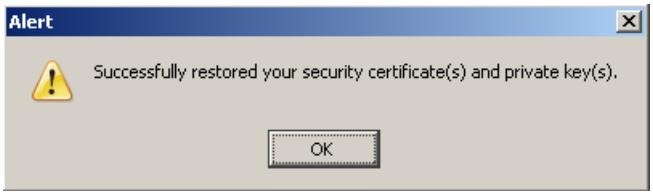


Figure 39: Firefox pfx installed

The certificate with the private key and the root and intermediate certificates have now been installed.

You can now send and receive encrypted email. If you also would like to send signed email you must trust the root certificate you just installed[13]. You should now manually trust the root certificate because it is not automatically trusted. You first need to find out which root you need to trust. First select your newly installed certificate (see Figure 40: Firefox Your Certificates).

Double-click the certificate you just installed. The certificate details should now be shown (see Figure

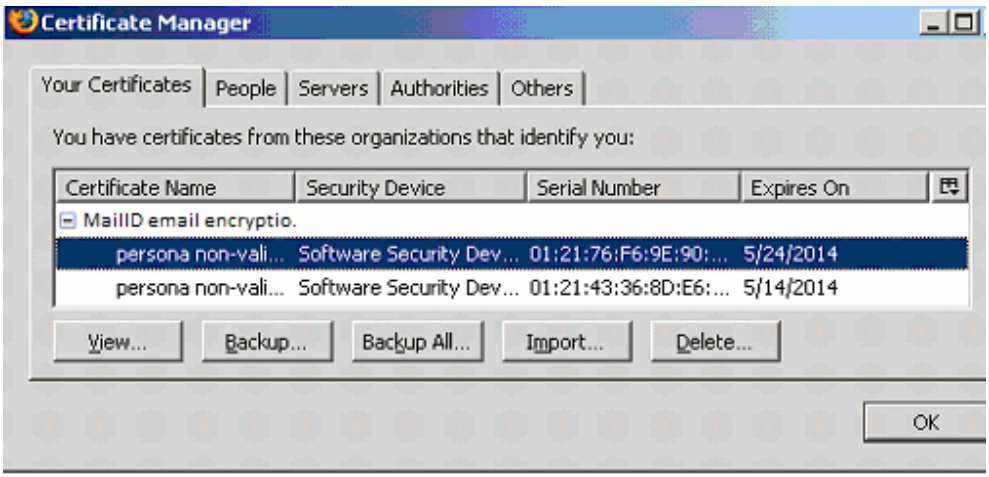


Figure 40: Firefox Your Certificates

41: Firefox Certificate Viewer). The first entry in the “Certificate Hierarchy” is the root certificate. You should remember the name because you will need it in the next step.

13 If you sign with a non trusted certificate the Gmail add-in reports an internal error.

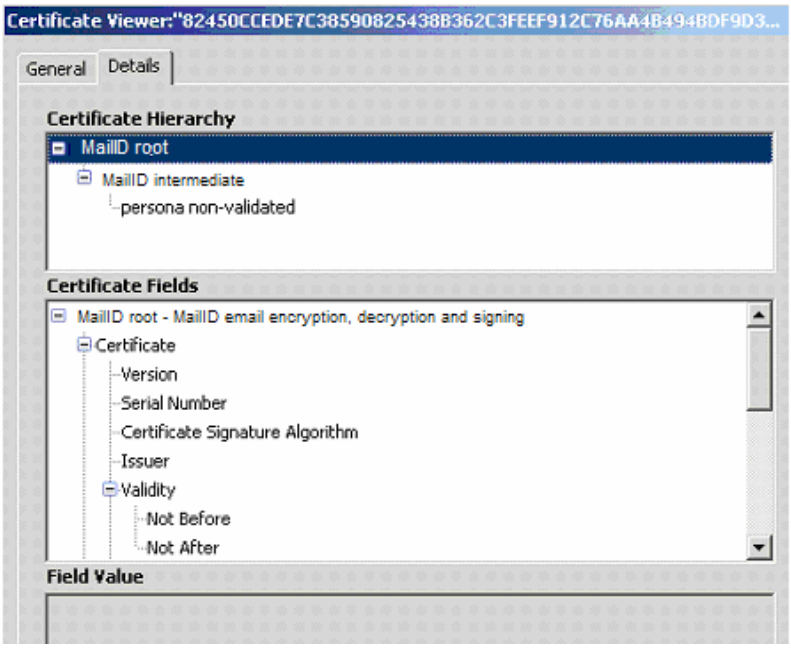


Figure 41: Firefox Certificate Viewer

Now open the "Authorities" tab on the "Certificate Manager" and select the correct root certificate (see Figure 42: Firefox Authorities).

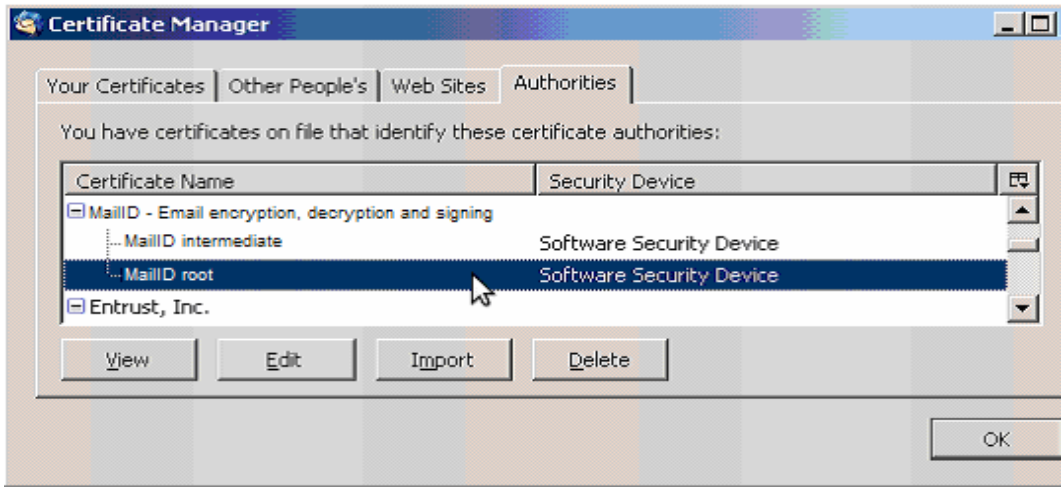


Figure 42: Firefox Authorities

Select the correct root certificate and click the "Edit" button. In the following dialog you must select "This certificate can identify mail users." (see Figure 43: Firefox CA certificate trust settings).

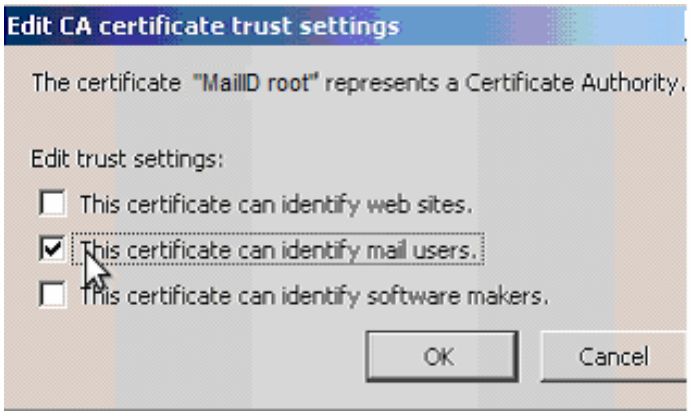


Figure 43: Firefox CA certificate trust settings

Now close all dialogs. Your can now start sending and receiving S/MIME signed and encrypted email from Gmail.

Receiving signed and encrypted email

A signed and encrypted email in Gmail looks like:

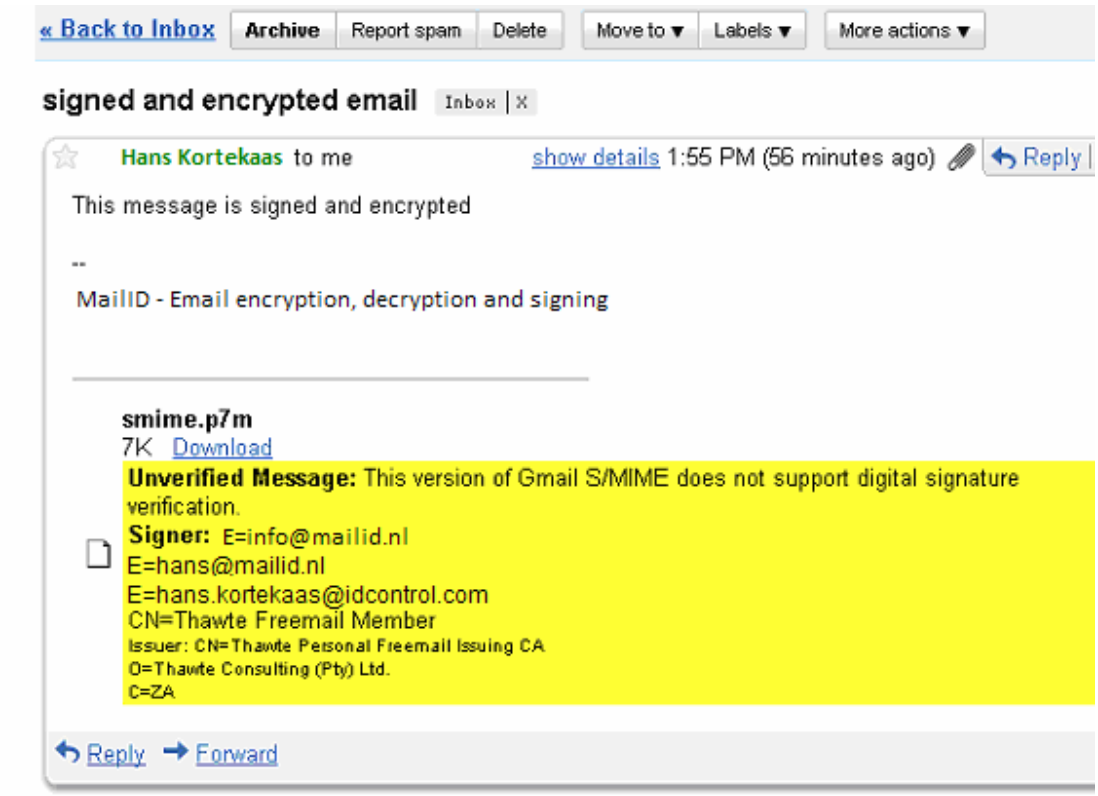


Figure 44: Firefox Gmail signed and encrypted

The current version of Gmail add-in does not verify digital signatures.

Sending signed and encrypted email

You can sign and encrypt your email by selecting the sign and encrypt option (see Figure 45: Gmail send signed and encrypted)

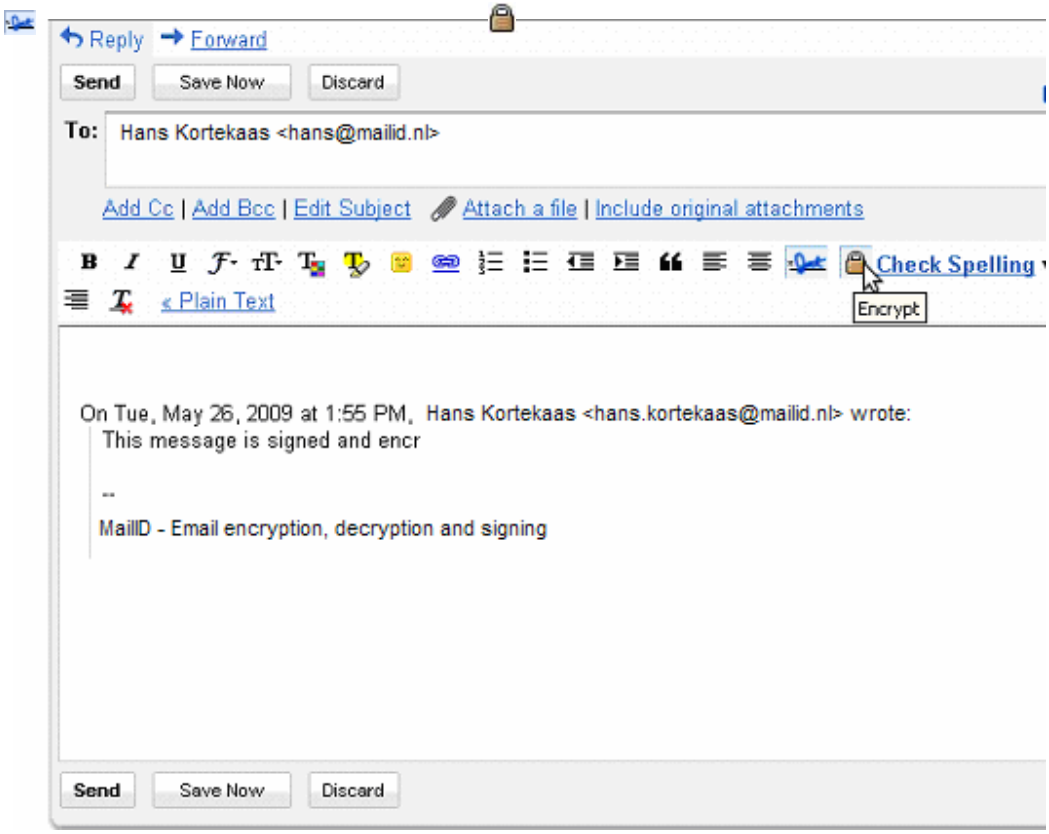
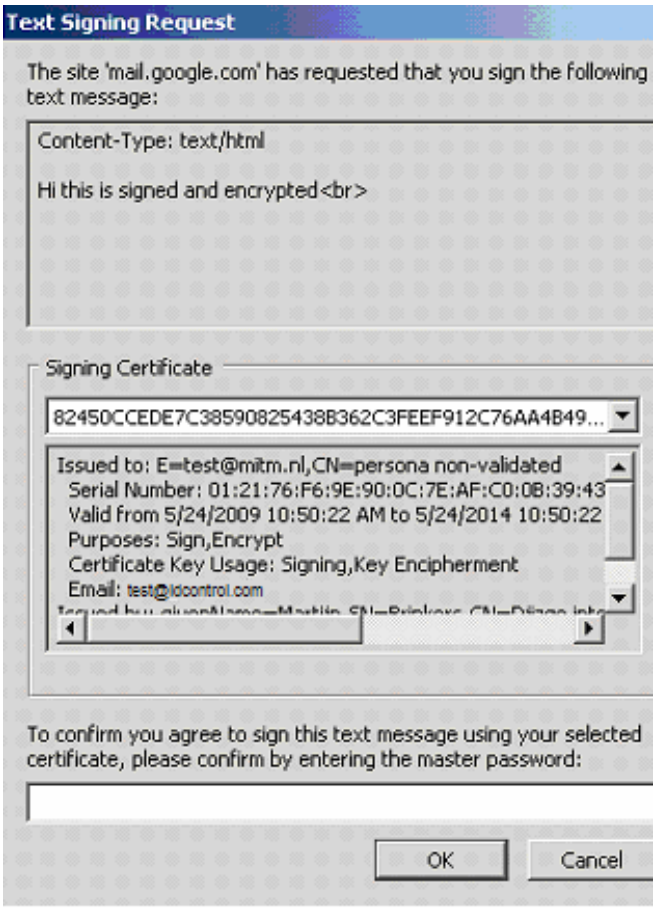


Figure 45: Gmail send signed and encrypted

Selecting will sign the message and selecting will encrypt the message

Click “Send” to sign, encrypt and send the message. When you sign a message a confirmation dialog will pop-up asking you to confirm the signing of the message (see Figure 46: Firefox Gmail confirm signing).



To confirm you need to enter Firefox's master password which was previously set by you.

After clicking the OK button a pop-up dialog asks for your Gmail password. The Gmail add-in sends the signed and encrypted message via the Gmail SMTP servers. Your Gmail password is required for sending the message with the Gmail SMTP server.

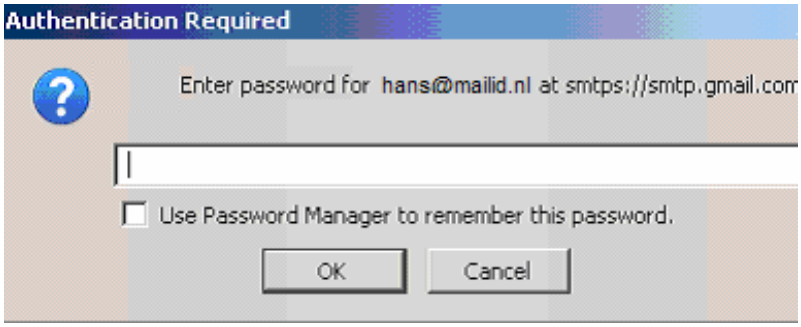


Figure 47: GMail authentication required

Entering your Gmail password and click the OK button. The message has now been sent.

Remarks

The Gmail S/MIME add-in has some shortcomings compared to S/MIME support in other mail clients that you should be aware of:

- Signatures are not verified.
- Drafts are not stored securely.

For more issues see http://richard.jones.name/google-hacks/gmail-smime/gmail-smime.html

Lotus Notes

The Lotus Notes recipient receives the following message[14] containing an attached password encrypted pfx:

Figure 48: Lotus Notes PFX email

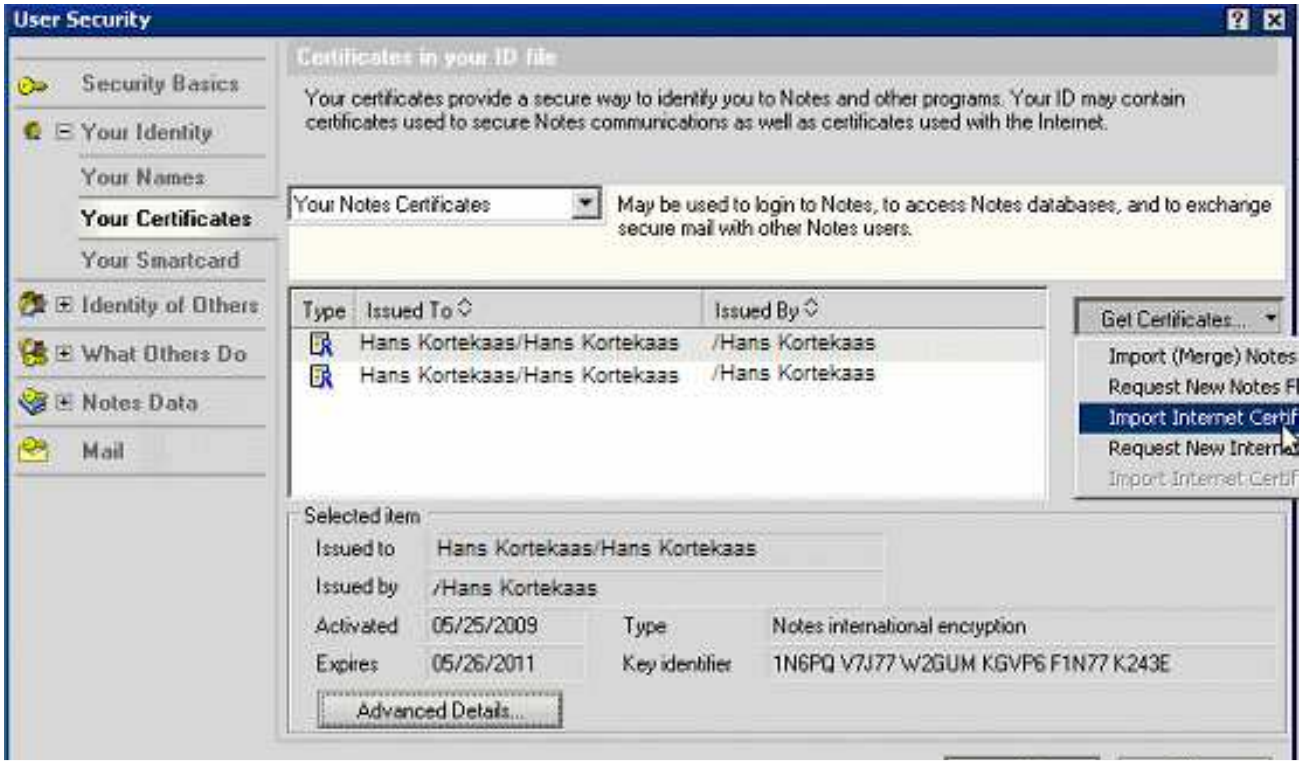
Importing the pfx

You first need to save the pfx attachment before you can import it into Lotus Notes. Save the pfx file on the desktop (or on any other location you normally use for your attachments).

Now open the User Security settings by selecting File → Security → User Security...

On the “User Security” dialog select Your Identity → Your Certificates. Now click the “Get Certificates” pull-down menu and select “Import Internet Certificates” (see Figure 49: Lotus Notes Import Internet Certificates)

14 This guide explains using Lotus Notes 8. For older versions of Lotus Notes it should however be similar.



Now select the pfx file you have just saved. A pop-up dialog opens asking you for the file format (see Figure 50: Lotus Notes Select Import File Format)

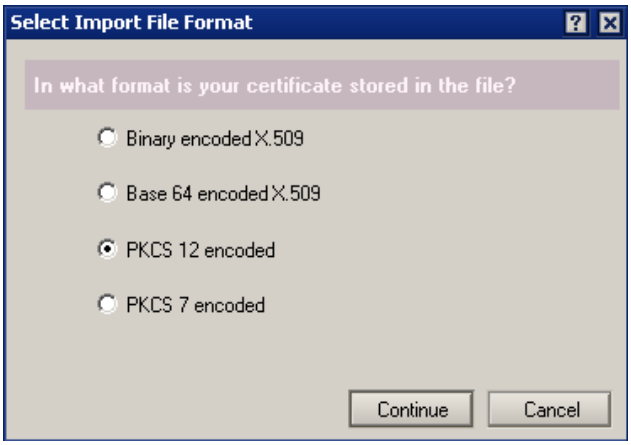
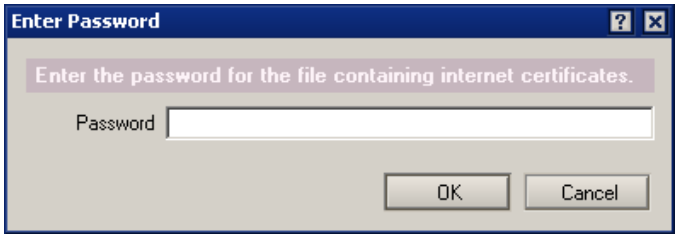


Figure 50: Lotus Notes Select Import File Format

Select “PKCS 12 encoded” and click “Continue”. You are now asked for the pfx password:



Enter the password that was given to you via SMS Text message or in some other way. Enter the password and click “OK”. The import wizard pops-up (see Figure 51: Lotus Notes Import Internet Certificates).

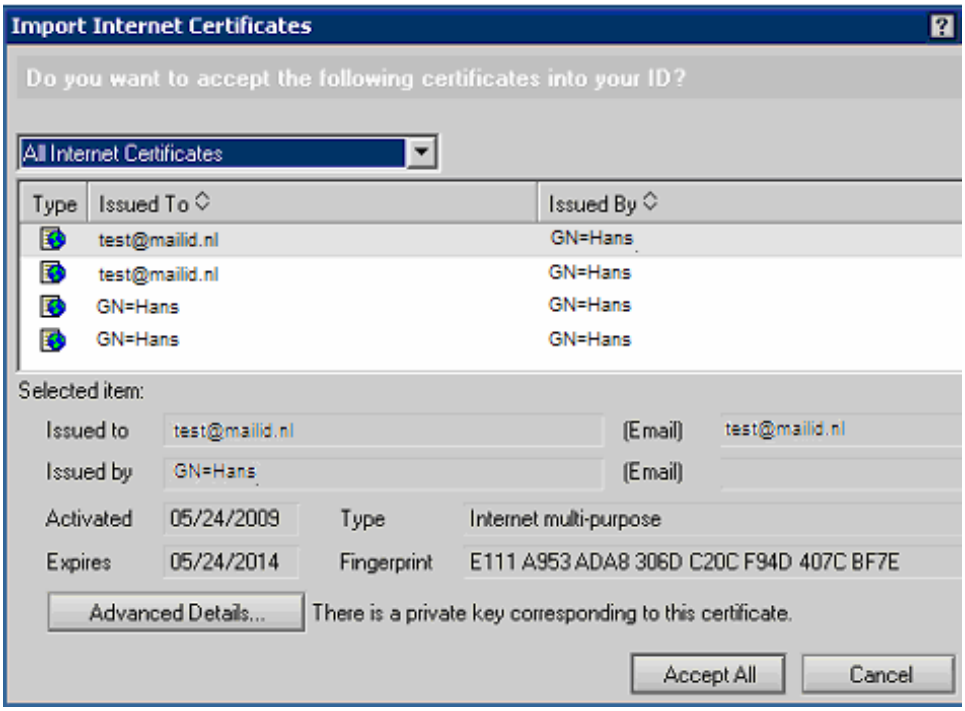


Figure 51: Lotus Notes Import Internet Certificates

Click the “Accept All” button to import all the certificates and keys.

Receiving signed and encrypted email

The first time you receive a signed and encrypted message Lotus Notes asks you to “Cross certify” the signer certificate. Click “Cross certify” to approve the certificate (see Figure 52: Lotus Notes Cross

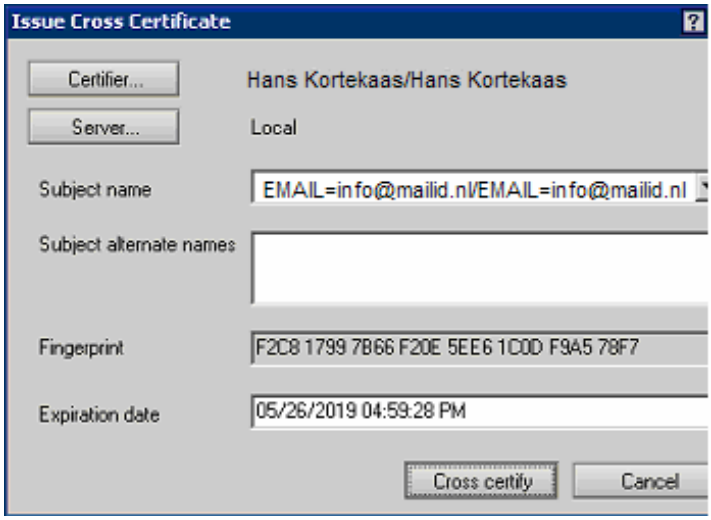


Figure 52: Lotus Notes Cross certify

certify).

You only need to cross certify the first time a new signer certificate is used.

You can check if a message is signed or encrypted using the signature/encryption pop-up menu  (see Figure 53: Lotus Notes signed and encrypted)

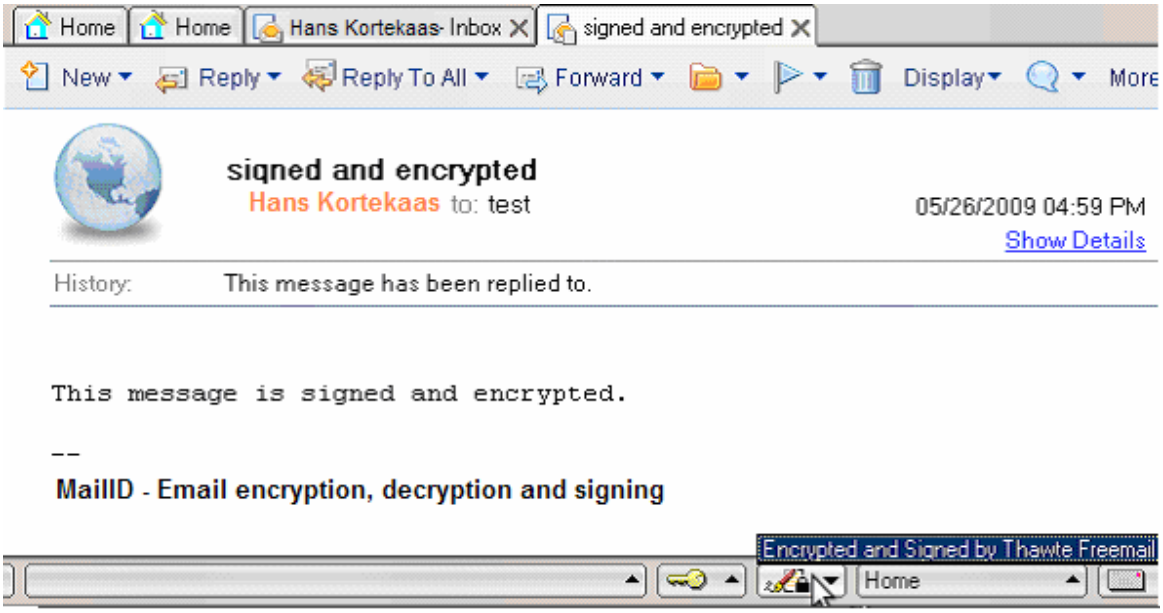


Figure 53: Lotus Notes signed and encrypted

Sending signed and encrypted email

If you want to send a message signed and/or encrypted you have to open the “Delivery Options” from the message composer. On the delivery options dialog select the Sign and Encrypt checkboxes (see Figure 54: Lotus Notes Delivery Options). The message will now be signed and encrypted when it is sent.

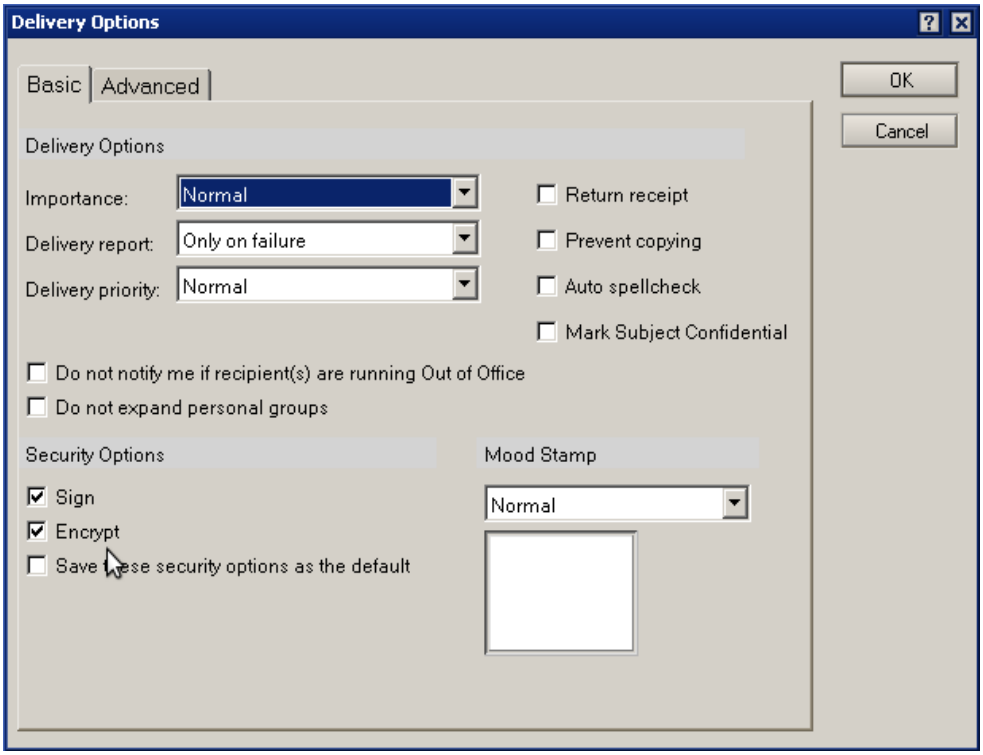


Figure 54: Lotus Notes Delivery Options

Appendix A: adding a CRL distribution point.

If you decide to add a CRL distribution point to your CA you should make sure that the CRL is available and accessible for external recipients. This is required because the S/MIME clients of the external recipients periodically tries to download the CRL. The CRL distribution point should be a fully qualified URL. The HTTP(S) and LDAP protocols are supported but we advise you to use HTTP protocol. Once the end-user certificate is created you cannot change the CRL distribution point of the created certificate so you should make sure that the URL is the correct URL.

Create CRL

You can create a CRL by clicking CA → Create CRL. This opens the page where you need to select the CA for which you want to create a CRL. Select the CA (there is probably just one). The following page will be shown:

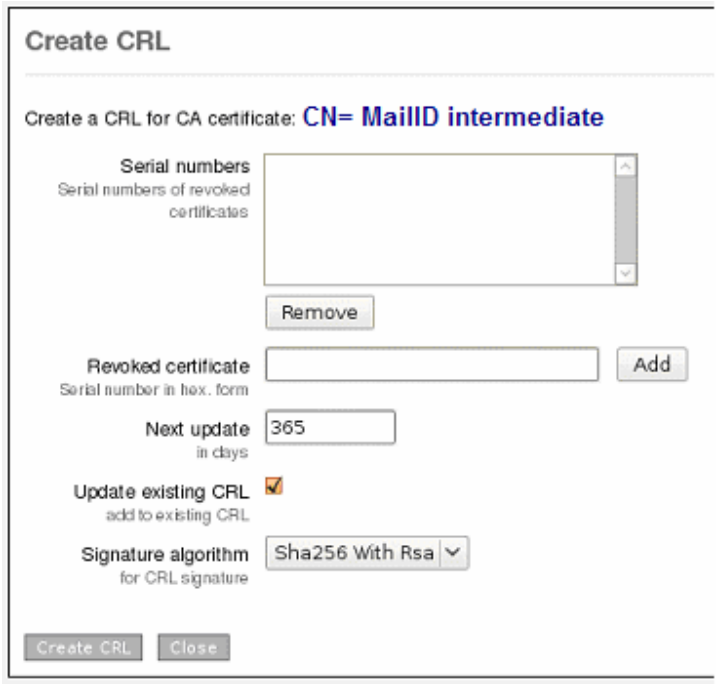


Figure 55: Create CRL

If you do not yet have any CRLs to revoke leave all settings to default values and press the "Create CRL" button. The CRL is now created.

Publishing the CRL

After you created a new CRL you should upload the new CRL to the URL from which the new CRL will be downloaded by the external clients. You should first download the new CRL from the CRL store and then upload it to the server where you host the CRL.

Appendix B: MailID S/MIME headers

When an incoming email is handled by MailID, special headers about the properties of the email are automatically added to the email. For example an encrypted message sent to an internal users is decrypted by MailID. Because the message, after being handled by MailID, is no longer encrypted the internal recipient of the message cannot check whether the message was initially encrypted. MailID therefore adds some security related headers that can be used to check if the message was secured or not.

The following headers are added:

```
X-MailID-Info-Signer-ID -*
X-MailID-Info-Signer-Verified-*
X-MailID-Info-Signer-Trusted -*
X-MailID-Info-Signer-Trusted-Info-*
X-MailID-Info-Encryption-Algorithm -*
X-MailID-Info-Encryption-Recipient -*
```

The * is build-up as follows [INDEX-]LEVEL

where INDEX and LEVEL are integer numbers starting at 0. INDEX is not used for all headers.

Example:

```
X-MailID-Info-Signer-ID-0-0
```

LEVEL denotes the S/MIME level the values applies to. A S/MIME message supports multiple nested levels of protection (CMS layers). For example a message can first be signed and then encrypted. LEVEL 0 is the first level encountered by the S/MIME handler. Within one level there can be multiple items. For example a message can be encrypted for multiple recipients. INDEX is the index of an item within a level.

Example headers:

```
X-MailID-Info-Encryption-Algorithm-0: AES128, Key size: 128 X-MailID-Info-
Encryption-Recipient-0-0: CN=Thawte Personal Freemail Issuing CA, O=Thawte
Consulting (Pty) Ltd.,
C=ZA/6B55D312FF5F9D5DAD9866FF827FFEB5//1.2.840.113549.1.1.1 X-MailID-Info-
Encryption-Recipient-1-0: EMAILADDRESS=support@cacert.org, CN=CA Cert
Signing Authority, OU=http://www.cacert.org, O=Root
CA/6683C//1.2.840.113549.1.1.1
```

```
X-MailID-Info-Signer-ID-0-1: CN=UTN-USERFirst-Client Authentication and
Email, OU=http://www.usertrust.com, O=The USERTRUST Network, L=Salt Lake
City, ST=UT, C=US/88F9874A02A53042E0228D78CBD55795/ X-MailID-Info-Signer-
Verified-0-1: True
X-MailID-Info-Signer-Trusted-0-1: True
```

The example headers shows that the message was first signed and then encrypted. The encryption algorithm was AES128. The message was encrypted with two certificates:

`X-MailID-Info-Encryption-Recipient-0-0` and `X-MailID-Info-Encryption-Recipient-1-0`

One certificate was issued by Thawte and the other was issued by CACert[15]. The message was signed by one signer with a certificate issued by Usertrust.

`X-MailID-Info-Signer-Verified` tells whether the message content was signed by the signer and that it has not been changed (tampered).

`X-MailID-Info-Signer-Trusted` tells whether the signing certificate was trusted (signed by root etc.) by the gateway. If the signing certificate was not trusted the reason for not trusting is given in the `X-MailID-Info-Signer-Trusted` header.

When email is received by MailID it will remove all `X-MailID-*` headers to make sure that an external sender cannot fake any MailID specific headers.

15 The certificate serial number, subjectKeyIdentifier and encryption algorithm is also added to the header.

Appendix C: links

Outlook

Using S/MIME in Microsoft Outlook

http://searchexchange.techtarget.com/generic/0,,sid43_gci1252311,00.html

Installing and using your certificate in Microsoft Outlook 2003
http://www.globalsign.com/support/personal-certificate/per_outlook03.html

Overview of certificates and cryptographic e-mail messaging in Outlook
http://office.microsoft.com/en-us/outlook/HP012305341033.aspx?pid=CH100622191033

Configuring S/MIME Security with Outlook Web Access 2003
http://www.msexchange.org/tutorials/Configuring-SMIME-Security-Outlook-Web-Access-2003.html

Implementing Outlook Web Access with the S/MIME Control http://technet.microsoft.com/en-us/library/aa998939(EXCHG.65).aspx

Apple Mac

Mail – How to Use a Secure Email Signing Certificate (Digital ID)
http://support.apple.com/kb/TA22353?viewlocale=en_US

S/MIME for Apple Mail

http://joar.com/certificates/

Webmail

Gmail S/MIME

https://addons.mozilla.org/en-US/firefox/addon/592

http://richard.jones.name/google-hacks/gmail-smime/gmail-smime.html