

## Secure e-mail transaction guidelines for external users with Commission personnel.

This document describes in general the basic requirements to set up secure (encrypted) e-mail communication between external users and the European Commission with the S/MIME protocol.

**Disclaimer:** The content of this document is for information only and it must not be taken as a Commission recommendation or endorsement of any kind.  
The screenshots of the e-mail client software, the products name or entities names are used as examples only and must just be considered general guidance. The information given should be applicable to any S/MIME compatible e-mail client, with the suitable adaptations.

*In case you already have a S/MIME secure e-mail infrastructure setup in your organisation, chapters 2 & 3 are informational only.*

### 1. S/MIME protocol

Secure Email at the Commission uses the S/MIME V3 (Secure Multipurpose Internet Mail Extensions) protocol standard. To read S/MIME packaged Email messages, your Email client must understand the S/MIME standard, otherwise secure messages appear as mails with attachment *smime.p7m*.

External partners must use:

- S/MIME compatible Email clients;  
e.g.: Outlook, Outlook Express, Lotus Notes, Mozilla Thunderbird, Evolution, KMail or any other S/MIME compatible Email client. Two possible modes are normally possible; they can be used in native mode or with an add-in. This document only describes the native mode.
- Non-S/MIME clients (e.g. Eudora or OWA) in combination with an add-in or applet (not discussed in this document).

## 2. Obtain a Certificate

### 2.1. Choose a Certification Authority

Choose a Certificate Service Provider (CSP) to issue your certificate, e.g. VeriSign (<http://www.verisign.com>), GlobalSign (<http://www.globalSign.com>), Thawte (<http://www.thawte.com>), Ascertia (<http://www.ascertia.com>) or any other CSP that deliver certificates to the public. Check the web site to find out what kind of certificates is available and in particular the level of security you need; frequently free certificates can be obtained. To generate and install the certificates follow the CSP/CA instructions. A standard installation of Internet Explorer, Thunderbird and Netscape contains the root certificates of some Certification Authorities:

#### Internet Explorer

Tools - Internet Options

→ Content Tab

→ Certificates

→ Trusted root CA

#### Thunderbird

Tools - Options

→ Advanced

→ Certificates

→ View Certificates

→ Authorities

#### Netscape

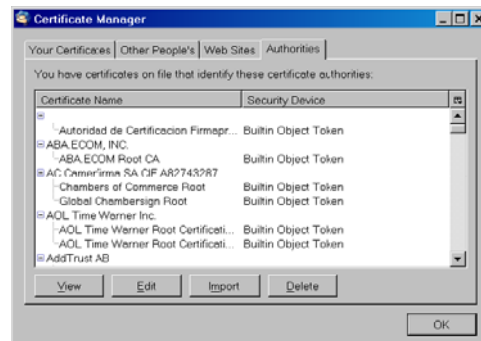
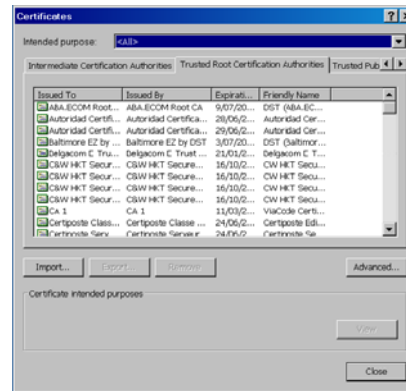
Edit - Preferences

→ Privacy & Security

→ Certificates

→ Manage Certificates

→ Authorities



## ***2.2 Get your personal digital ID***

The Certification procedure depends on the CA you choose and the level of security you need. This is an example of the procedure you might expect to obtain a demonstration certificate by means of a Web-CA.

In this case, the same certificate is used for signing and encryption.

- (a) Start the certificate request on the CA web site
- (b) The procedure verifies if the CA root certificates are present in your browser and imports them if missing.
- (c) Enter requested personal information, incl. a correct Email address and a password
- (d) Wait for a message sent to the specified Email address
- (e) Open the message when it arrives and go to the URL indicated in the message
- (f) Enter the password from the previous step for authentication
- (g) Private and public key are now generated locally on your workstation and the public key is certified by the CA.
- (h) Enter a new password that will protect your private key file
- (i) The certificate (with private key) is stored on your PC:
- (j) You are informed if the personal certificate has been imported
- (k) When the process is terminated, check if your personal certificate has been loaded

Note that the certificates (yours and CA) are only created on the PC where you performed the certificate generation procedure. If you want to use your digital ID on other systems, you must export/import your personal and CA certificates manually.

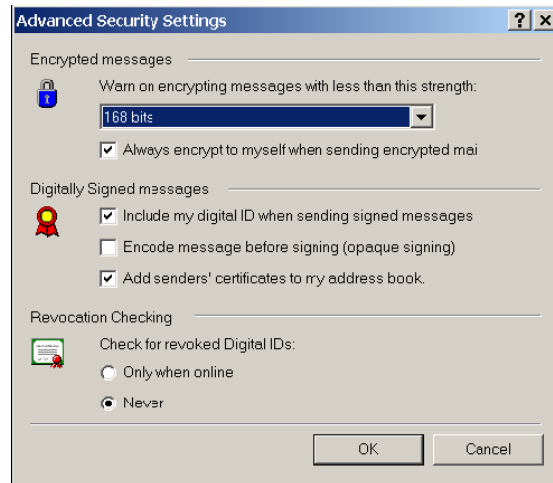
### 3 Configure security for Email clients

We will briefly explain the configuration of four Email clients.

#### 3.1. Outlook Express

After importing your personal certificates in Internet Explorer, set up Outlook Express security:

a) Go to: *Tools* → *Options* → *Security* → *Advanced*



b) *Encrypted messages* section:

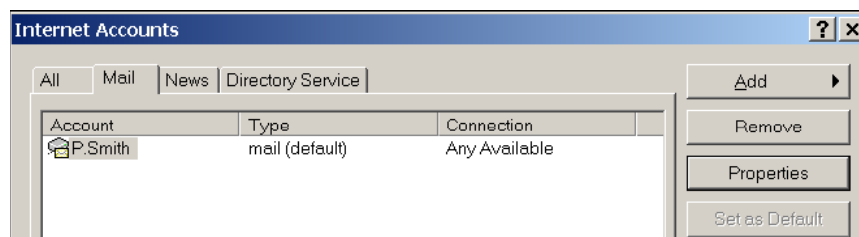
- Warn on encrypting messages with less than this strength: select **168 bits!**

c) *Digitally Signed messages* section:

- Select *Include my digital ID when sending signed messages*
- Select *Add sender's certificates to my address book*
- Select *Encode message before signing (opaque signing)* only if you're sure that these recipients use SMIME compatible Email clients. Commission users can verify opaque signed messages

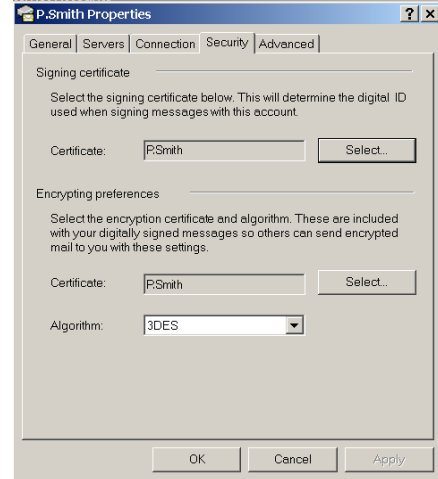
a) Set default signing and encryption certificate

Go to: *Tools* → *Accounts*



Select the account, click the *Properties* button and then click the *Security* tab

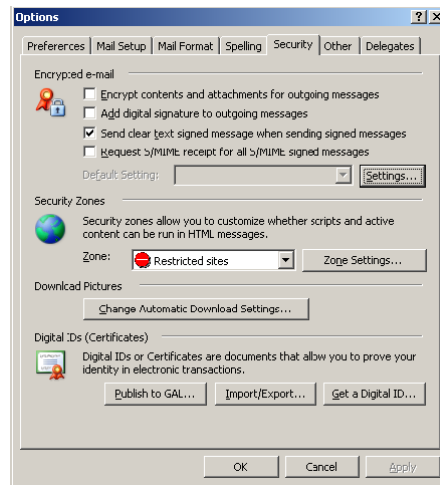
Outlook Express looks for signing and encryption certificates that correspond to your Email address and sets the first one it finds as default. If you have only one signing and one encryption certificate, no further action is required, otherwise, click the *Select* button for *signing certificate* and *encryption certificate* and select the correct certificate.



### 3.2. Outlook

After importing your personal certificates in Internet Explorer, set up Outlook security:

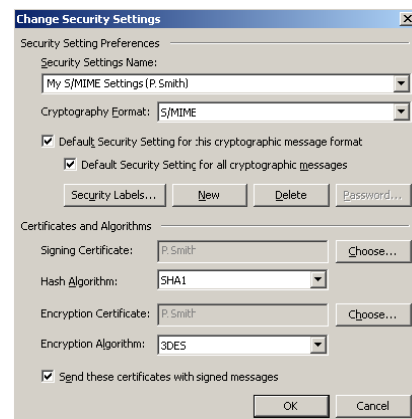
a) Go to: *Tools* → *Options* → *Security*



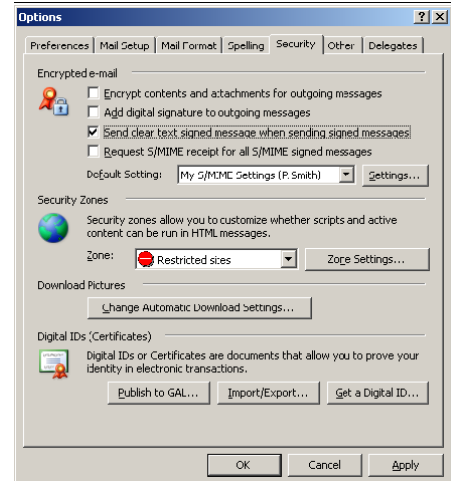
b) Click the *Settings* button.

c) Enter any name in the first field or keep default.

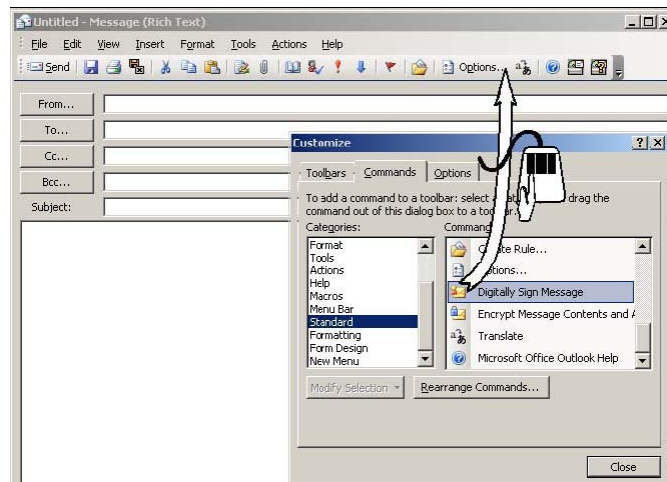
d) Outlook looks for signing and encryption certificates that correspond to your Email address and sets the first one it finds as default. If you have only one signing and one encryption certificate, no further action is required, otherwise, click the *Choose* button for signing certificate and encryption certificate and select the correct certificate.



e) Click the OK button to terminate.



f) Create a new message. In the Tools → Customize menu, click the Commands Tab.



g) Select Standard in the Categories box and locate in the Commands box the icons Digitally Sign Message and Encrypt Message Contents and Attachments. For each button icon, select it and while pressing the left mouse button, drag the icon to the position in the toolbar where you want the button to appear.

h) Close the message without sending or saving it

### 3.3. Thunderbird and Netscape

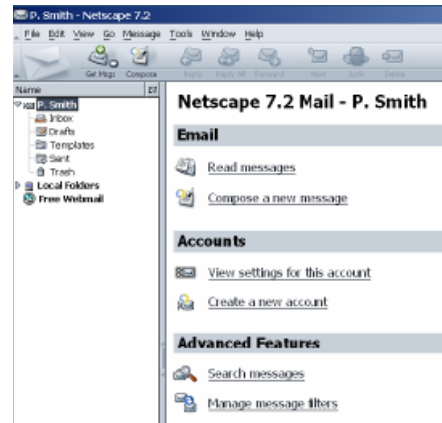
After importing your personal certificates, you need to set your default signing and encryption certificate. Most settings are identical for Thunderbird and Netscape.

a) Go to the main page

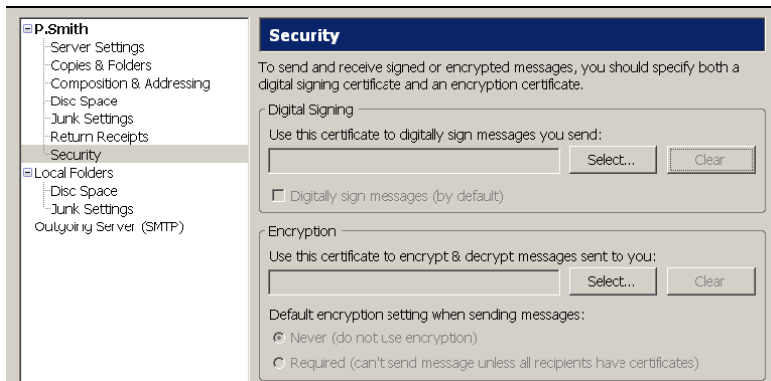
## Thunderbird



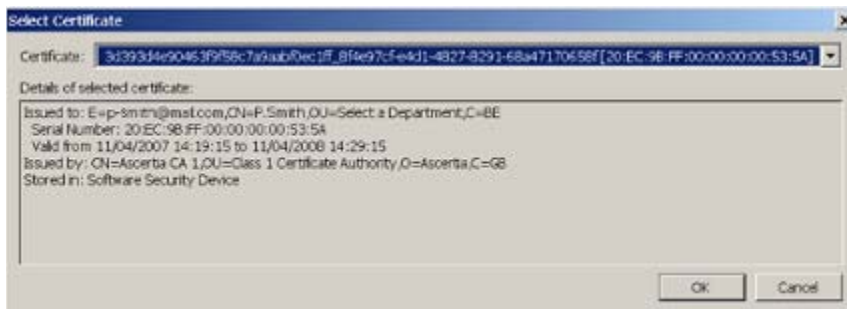
## Netscape



b) Click View Settings for this account and select Security

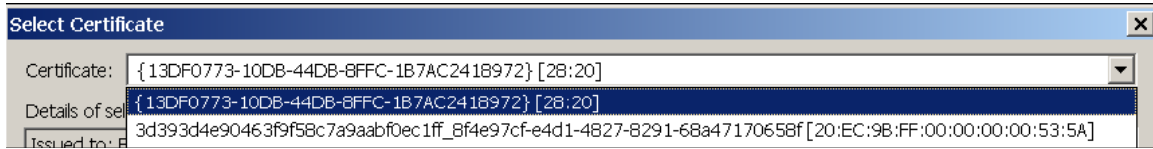


c) Click the *Select* button in *Digital Signing* section

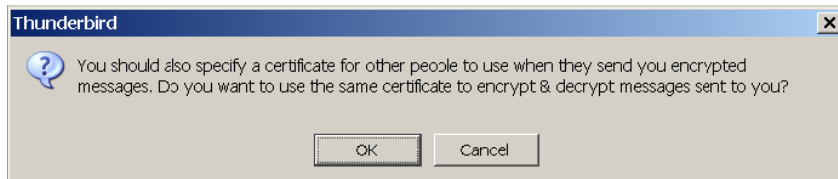


At the top of this screen you see the certificate's friendly name and serial number between brackets. The lower part shows the certificate details. Very often, the friendly name is a long (hexadecimal) code. In that case you should look at the details section for more information about the certificate.

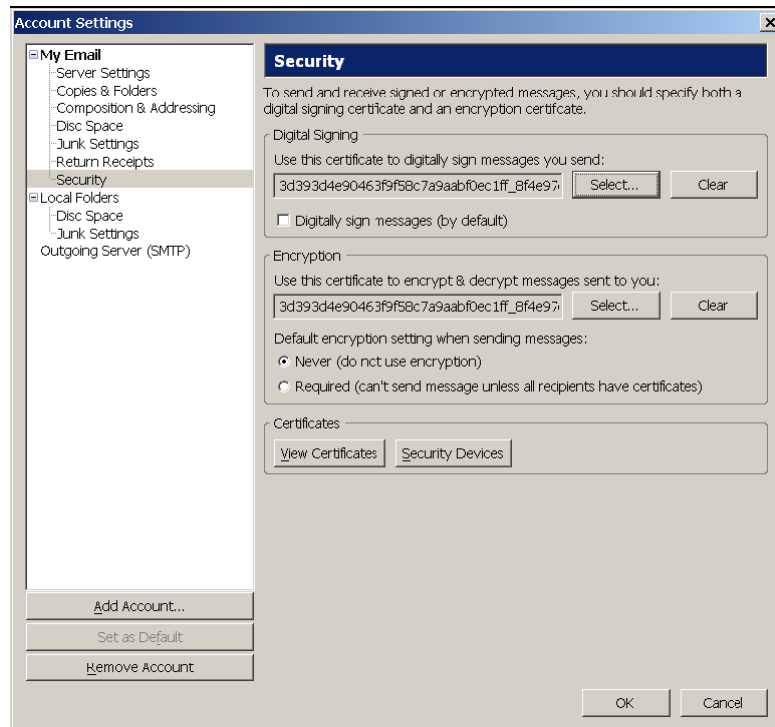
Note: If you have multiple certificates, the first one is selected and you can choose another by clicking the arrow at the right ▾



d) Click the OK button to select the certificate



e) If you want to use the same certificate for encryption click the *OK* button, otherwise click the *Cancel* button and then the *Select* button in the *Encryption* session.



f) Click the *OK* button to terminate

## 4 Install recipients Certificates

### 4.1. Introduction

To verify a digital signature, the receiver must trust the sender's certificate by trusting his CA. Once the CA is trusted, all certificates issued by this organisation will be trusted automatically.

To be able to send encrypted messages, the sender must have the recipient's certificate.

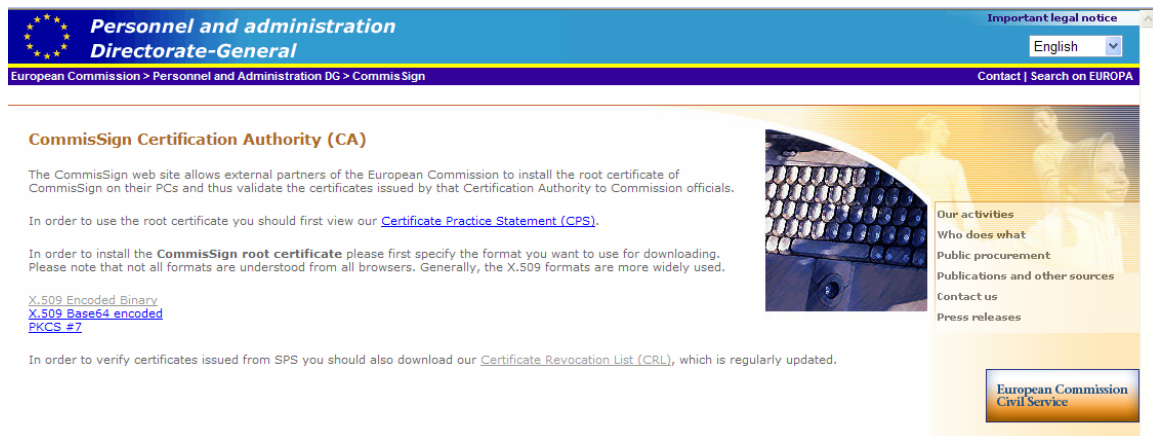
- To trust each other's certificates, users must exchange their CA certificate(s).
- To encrypt messages, users must exchange their personal certificate.

The easiest way to exchange personal certificates is by sending a signed-only message.

### 4.2. Import the European Commission root certificate

Before you can use secure e-mail communication with Commission partners, you must trust the European Commission root CA certificate. This trust is done by importing the Commission CA root certificate into Internet Explorer, Thunderbird, Netscape, etc.

The root certificate can be downloaded on the Commission Europa website:  
[http://ec.europa.eu/dgs/personnel\\_administration/commissign/index\\_en.htm](http://ec.europa.eu/dgs/personnel_administration/commissign/index_en.htm)



**Personnel and administration  
Directorate-General**

European Commission > Personnel and Administration DG > CommisSign

Important legal notice  
English

Contact | Search on EUROPA

### CommisSign Certification Authority (CA)

The CommisSign web site allows external partners of the European Commission to install the root certificate of CommisSign on their PCs and thus validate the certificates issued by that Certification Authority to Commission officials.

In order to use the root certificate you should first view our [Certificate Practice Statement \(CPS\)](#).

In order to install the **CommisSign root certificate** please first specify the format you want to use for downloading. Please note that not all formats are understood from all browsers. Generally, the X.509 formats are more widely used.

[X.509 Encoded Binary](#)  
[X.509 Base64 encoded](#)  
[PKCS #7](#)

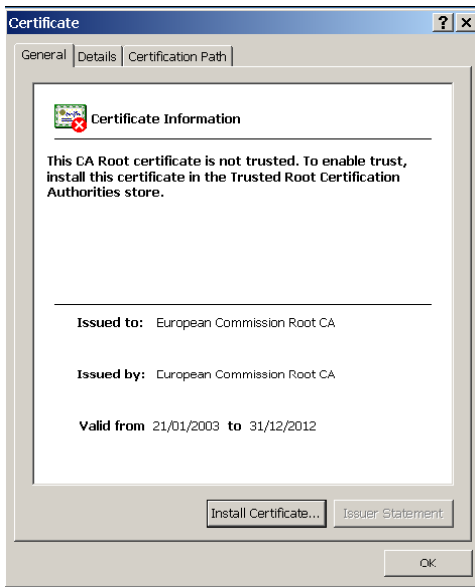
In order to verify certificates issued from SPS you should also download our [Certificate Revocation List \(CRL\)](#), which is regularly updated.

Our activities  
Who does what  
Public procurement  
Publications and other sources  
Contact us  
Press releases

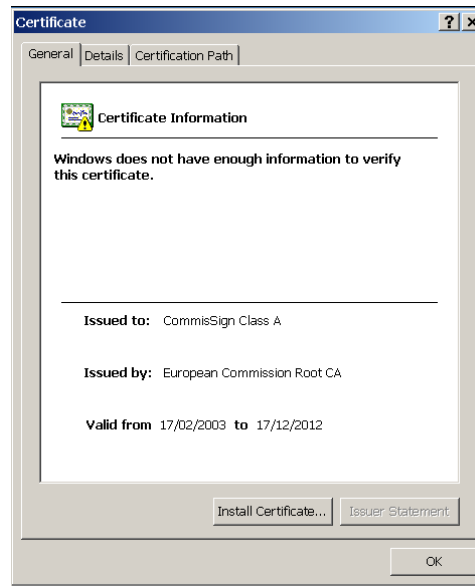
European Commission  
Civil Service

Click the *X509 encoded binary* or *X509 base64 encoded* link. The download of the certificate file *csselfder.cer* should start automatically.

The intermediate certificate *CommisSign Class A* should be obtained from a Commission user as a *.cer* file or by requesting a *signed* e-mail which is needed anyway for encrypted communication.



***CommisSign Root CA***

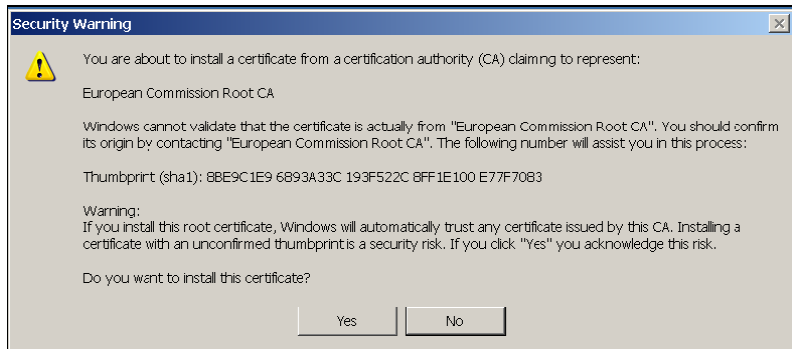


***CommisSign Class A***

#### ***4.2.1. Systems with Internet Explorer***

To import the CA certificates use following procedure:

- a) Copy the *Root* certificate file anywhere on your PC
- b) Double click the Root CA file
- c) Click the *Install Certificate* button to enter the Certificate Manager Import Wizard.
- d) Always click the *Next* button and keep the default values.
- e) After clicking the *Finish* button, confirm that you want to add and trust the *CA* root certificate.



- g) Verify in Internet Explorer via *Tools* → *Internet Options* → *Content* → *Certificates* if the root certificate has been loaded:  
*European Commission Root CA* → *Trusted Root Certification Authorities*

## 4.2.2 Systems with Thunderbird and Netscape

To import the CA use following procedure:

a) Start *Certificate Manager*

### Thunderbird

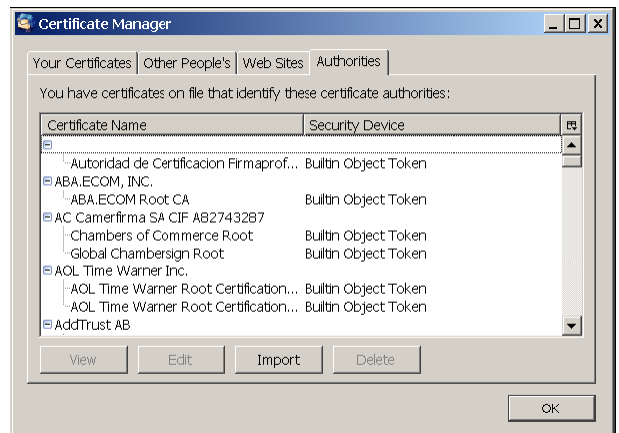
*Tools* → *Options* → *Advanced* → *Certificates* → *View Certificates*

### Netscape

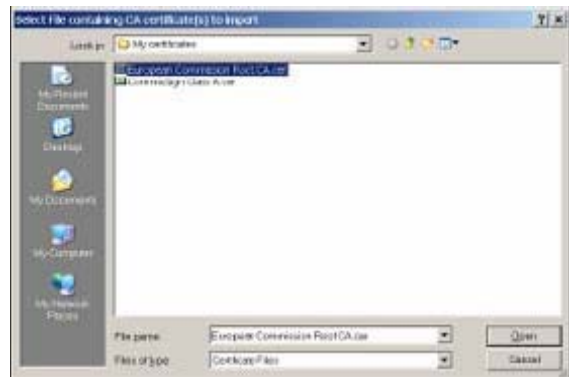
*Edit* → *Preferences* → *Privacy & Security* → *Certificates* → *Manage Certificates*

b) Click the *Authorities* tab

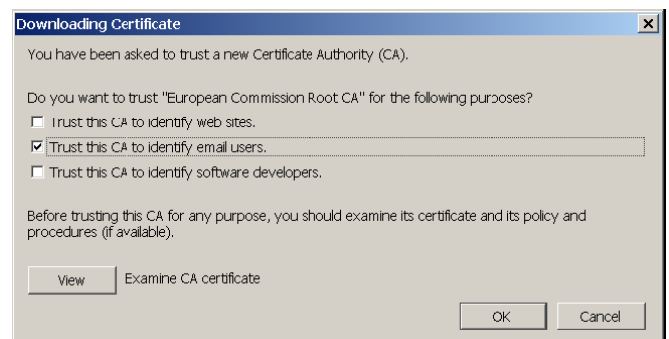
c) Click the *Import* button



d) Select the *CommisSign Root CA* certificate file and click the *Open* button

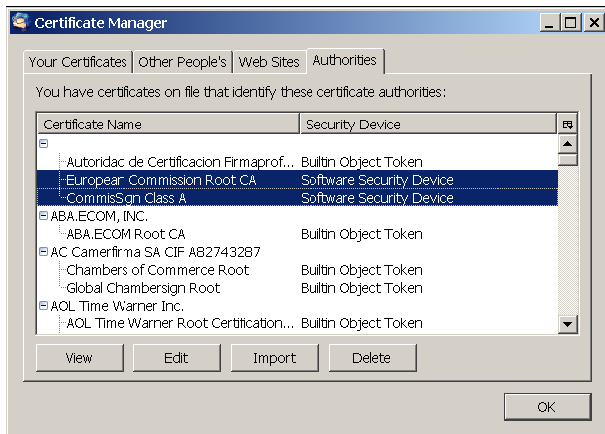


e) Select "*Trust this CA to identify Email users*" and click the *OK* button.



f) Repeat this procedure for *CommisSign Class A*

g) Return to the *Authorities* certificate store and check if the certificate is present



### 4.3. Import the User certificates

Ask the Commission user to send you a signed-only message.

#### 4.3.1. Outlook Express

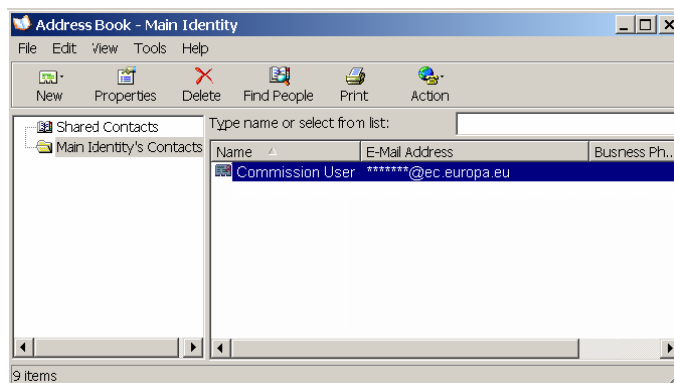
Outlook Express will automatically assign a certificate to a contact with the Email address from the certificate.

a) Go to *Tools* → *Options* → *Security* → *Advanced* and check if the option *Add sender certificates to my address book* is set.

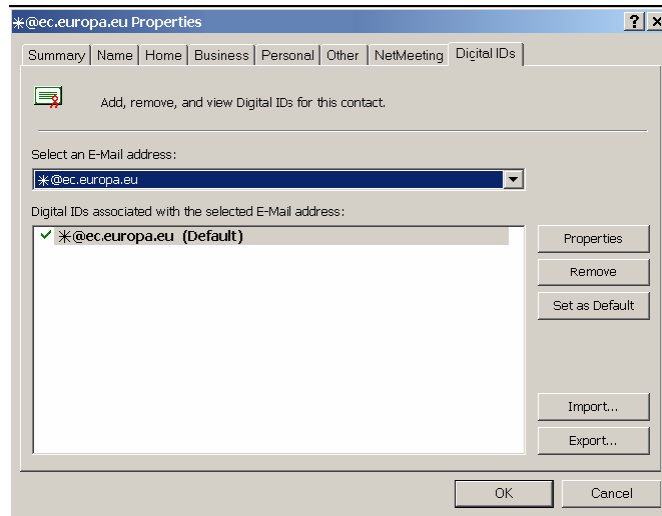
b) Open the signed mail from the Commission and close the message again.

c) The recipient will be created in the contacts (if not exists) or updated with the right certificate when he already exists.

d) Check the contacts: the recipient should now be represented by a red certificate sign.



e) Open the contact and select the *Digital IDs* Tab to verify the certificate.

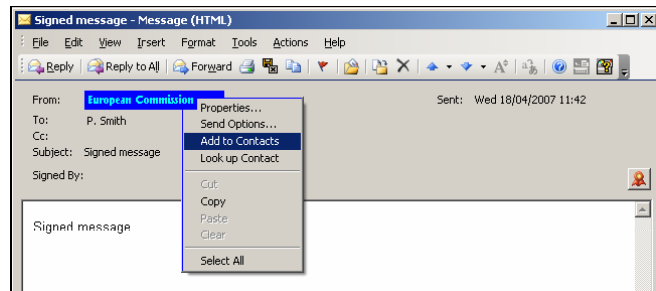


Note that you can always import a user certificate manually at this point via a file by clicking the *Import* button. It is also possible to import more than one certificate for a contact and define a default one.

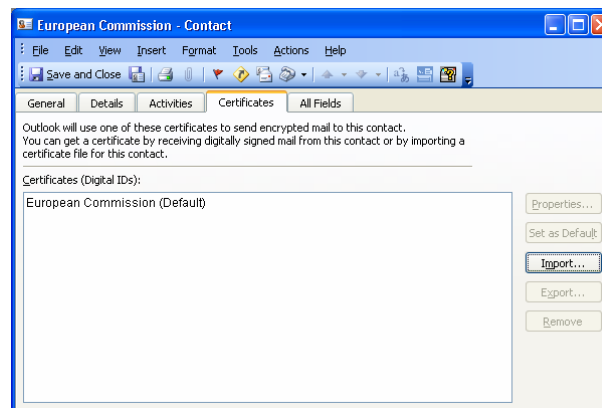
### 4.3.2. Outlook

a) Open the signed message from the Commission

b) Right click the sender (after the *From:* field) and select *Add to Contacts*. This will add the sender's address with certificate to your contacts. If the contact already exists, it will be updated



c) To check if the certificate was imported correctly, open the contact and select the *Certificates* Tab.

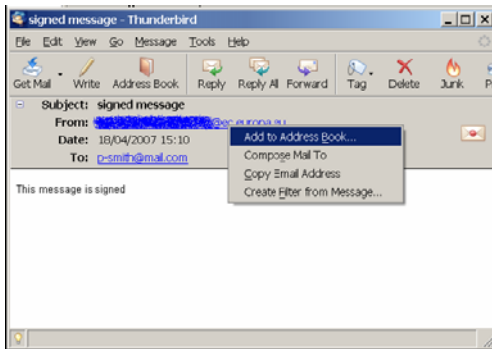


Note that you can always import a user certificate manually at this point via a (.cer) file by clicking the *Import* button. It is also possible to import more than one certificate for a contact and define a default one.

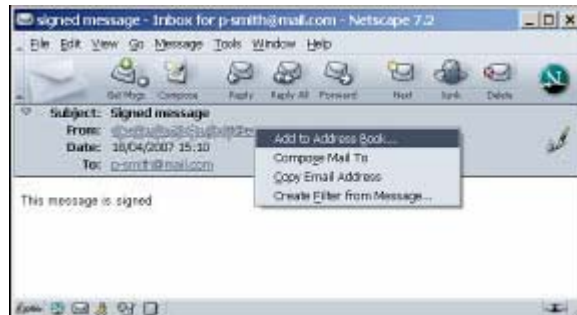
### 4.3.3. Thunderbird and Netscape

a) Open the signed message from the Commission

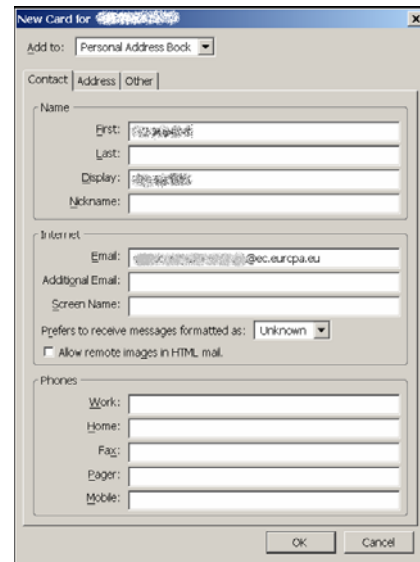
#### Thunderbird



#### Netscape



b) Right click the sender (after the *From:* field) and select *Add to Address Book*



c) Fill in the user information

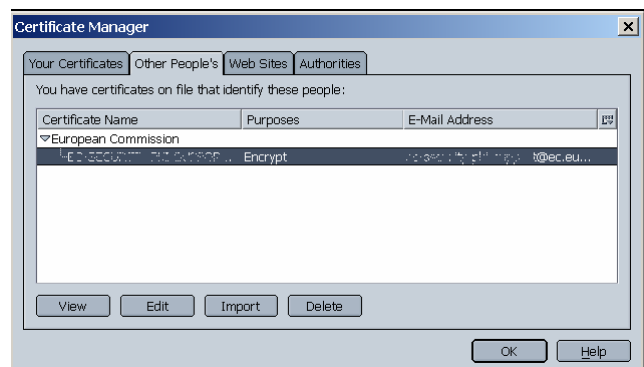
d) Check if the certificate has been added

#### Thunderbird

*Tools* → *Options* → *Advanced* → *View Certificates* → *Other People's*

#### Netscape

*Edit* → *Preferences* → *Privacy & Security* → *Certificates* → *Manage Certificates* → *Other People's*



## 5. Send encrypted messages

You can only send encrypted messages if you have the certificates if your recipients (obtained via a signed-only e-mail see chapter 4.3.).

### 5.1. Outlook Express

a) Create a new message

b) Click the *Sign* button to digitally sign the message (1)

c) Click the *Encrypt* button to encrypt the message (1)

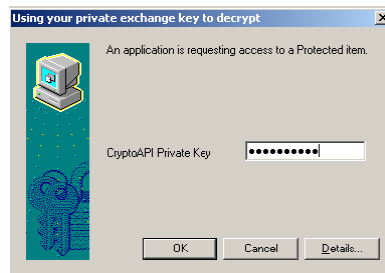
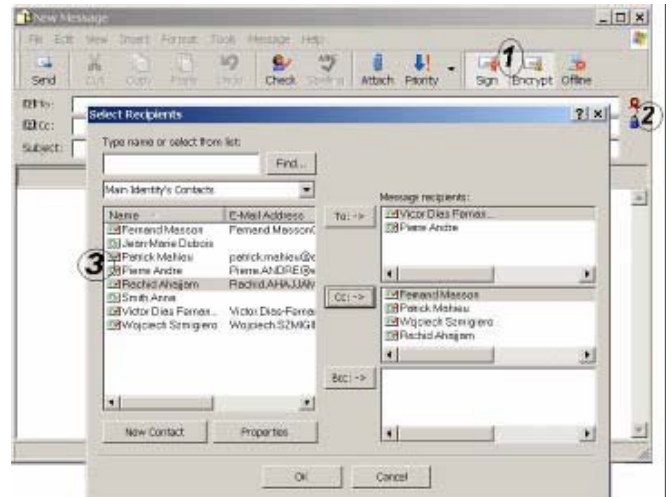
The (red) certificate icon indicates the message will be signed, the (blue) padlock icon indicates the message will be encrypted (2)

d) Select your recipients. To encrypt the message, you need the recipients' certificate installed (indicated by the red certificate sign icon in the contacts). (3)

e) Compose your message as you would do for a normal message

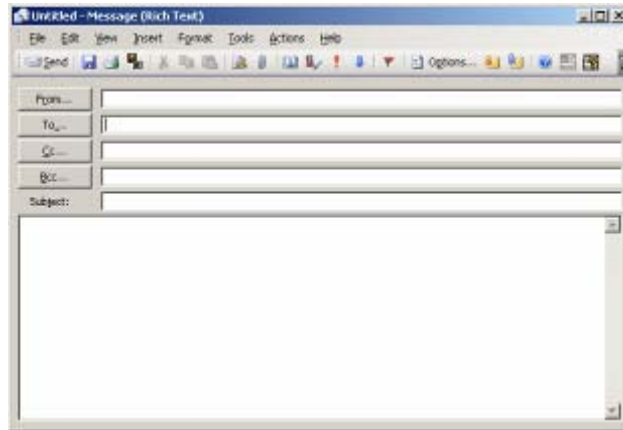
f) Click the *Send* button.


g) Enter your private key password (if configured)




## 5.2. Outlook

a) Create a new message



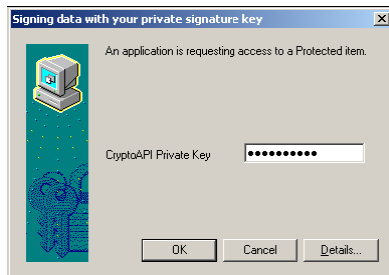
b) Click the  button to digitally sign the message

c) Click the  button to encrypt the message

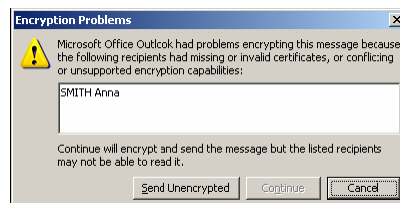
d) Compose your message, as you would do for a normal message.

e) Click the *Send* button to send the message

f) If you want to sign the message, you must enter your private key password (if configured)



Note that you can only encrypt the message if all recipients have a certificate. If the certificate of a recipient is missing, you'll see the following message:



If none of the recipients has a certificate, the *Continue* button is greyed out, if at least one of the recipients has a certificate, the *Continue* button can be clicked. In that case, the message is sent encrypted to all recipients, but only those with a certificate can read it.

### 5.3. Thunderbird and Netscape

a) Create a new message

#### Thunderbird

Click the *Write* button 

#### Netscape

Click the *Compose* button 

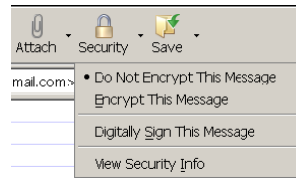
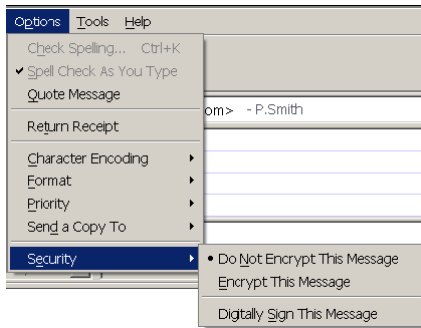
b) Digital signature and encryption can be selected in 2 ways:

*Options* → *Security*

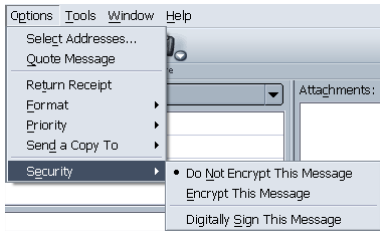
or

Click arrow at the right of *Security* icon

#### Thunderbird



#### Netscape



- To sign a message, click *Digitally Sign This Message*

- To encrypt a message, click *Encrypt This Message*

Note that only one option can be selected at the time

c) Compose your message as you would do for a normal message and click the *Send* button.

d) If you sign the message, enter the *Software Security Device* password

