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:

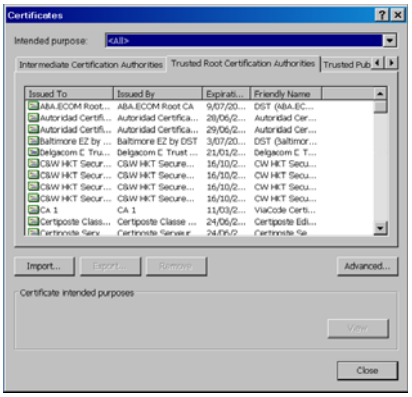
- S/MIME compatible Email clients;
  e.g.: Outlook, Outlook Express, Lotus Notes, Mozilla Thunderbird, Evolution, KMail or any other S/MIME compatible Email client. Two possible modes are normally possible; they can be used in native mode or with an add-in. This document only describes the native mode.

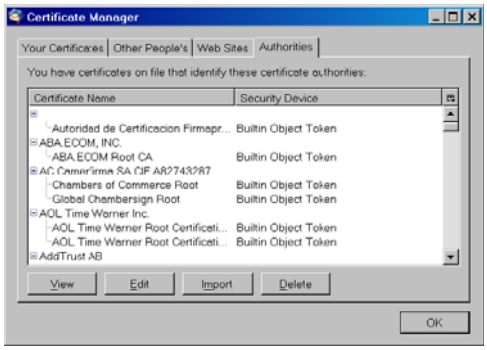
- Non-S/MIME clients (e.g. Eudora or OWA) in combination with an add-in or applet (not discussed in this document).

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://ww.globalSign.com), Thawte (http://ww.thawte.com), Ascertia (http://ww.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.

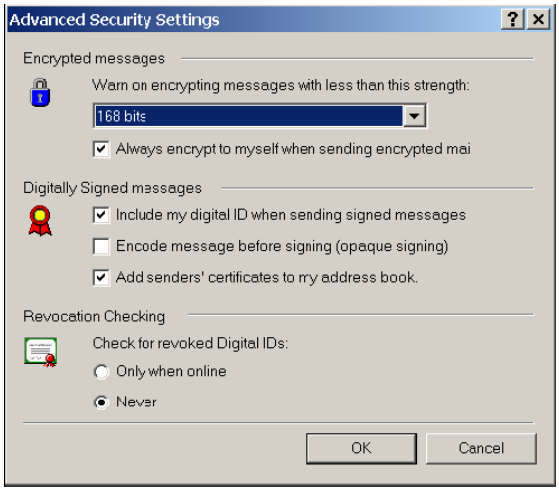
3 Configure security for Email clients

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*



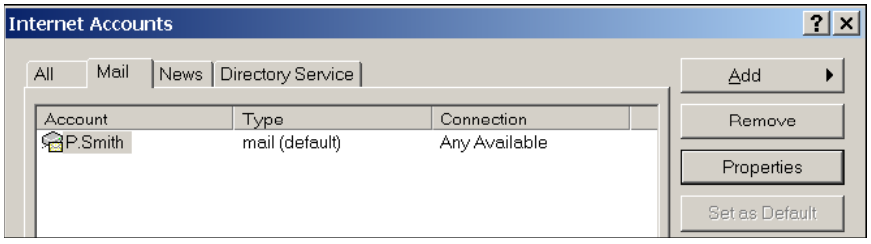
b) *Encrypted messages* section:

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

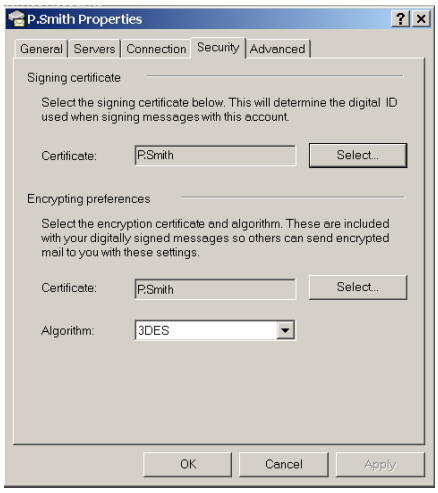
c) *Digitally Signed messages* section:

- 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

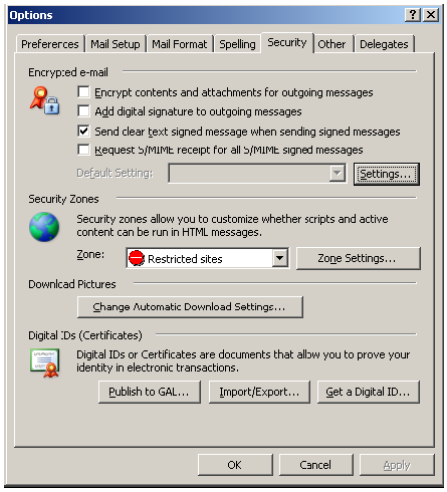


Outlook Express looks for signing and encryption certificates that correspond to your Email address and sets the first one it finds as default. If you have only one signing and one encryption certificate, no further action is required, otherwise, click the *Select* button for *signing certificate* and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