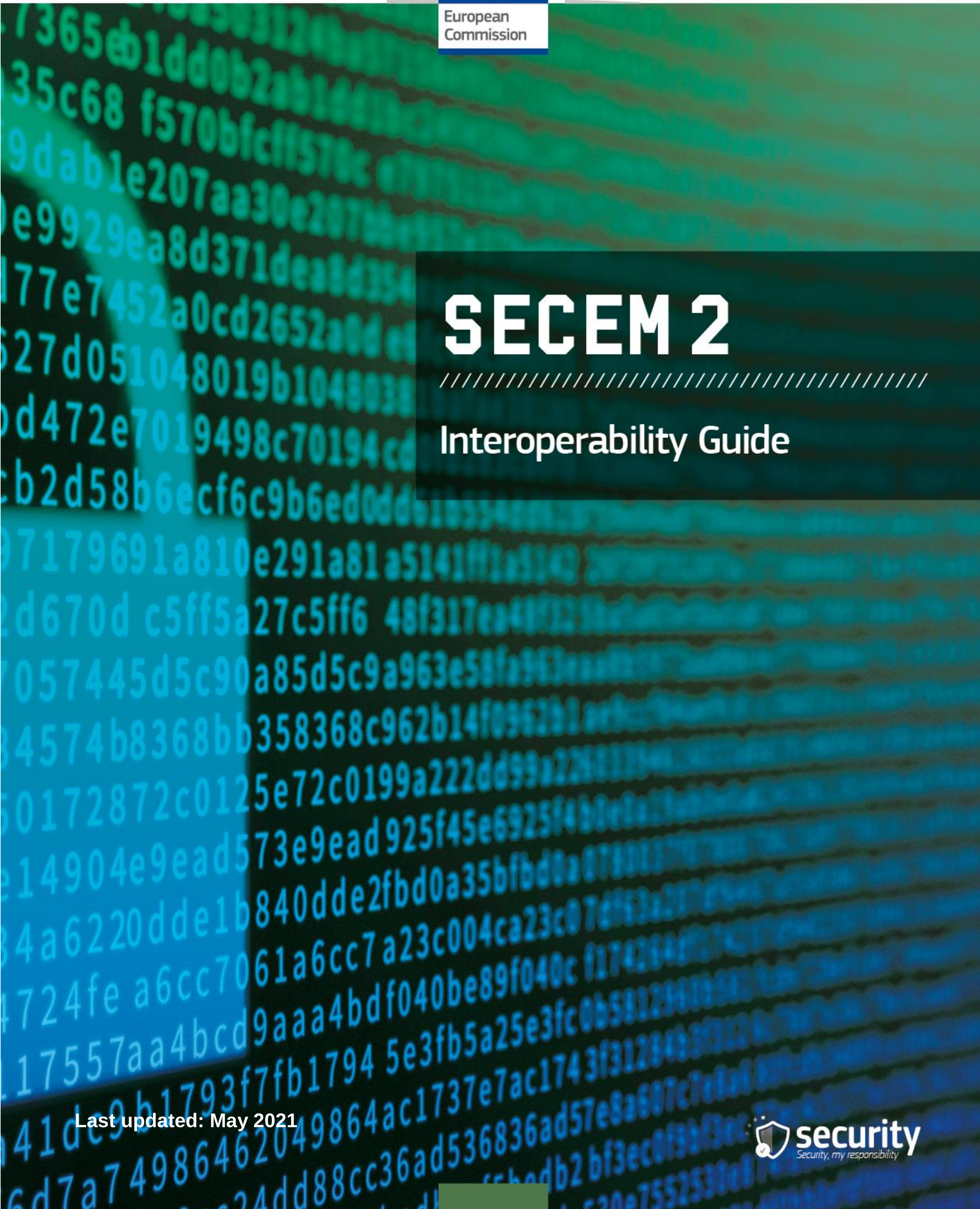


SECEM 2

Interoperability Guide

Last updated: May 2021

In this guide…

Introduction

Secure E-Mail (SECEM-2) is the Commission's in-house tool for encrypting e-mails. As laid down in the Security notice C(2019)1904 on marking and handling sensitive non-classified information, all **e-mails containing sensitive non-classified information** must be **encrypted with SECEM-2** or an equivalent application using AES-256.

This document explains how to configure e-mail clients to enable encrypted exchanges between Commission staff and external stakeholders.

Please note that the Commission has Service Level Agreements with a number of **European institutions, bodies and agencies** and might be able to provide S/MIME (SECEM-2) certificates to them. Contact the PKI team for information.

For any questions, please contact:

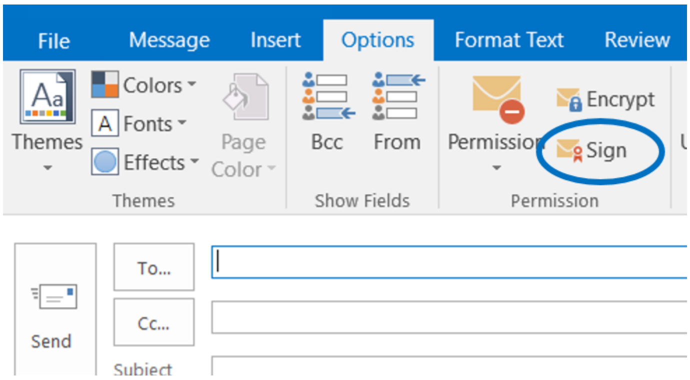
- HR-SECURITY-PKI-SUPPORT@ec.europa.eu – for Commission staff
- Your company's IT support – for external stakeholders

Disclaimer: *This document is for information only and it does not represent the Commission's endorsement of any particular e-mail client, software or Certificate Service Provider. The screenshots of the e-mail client software, as well as the product and entities names are referenced as examples only. The information provided below should be applicable to any S/MIME compatible e-mail client, with the suitable adaptations.*

1. How to exchange encrypted e-mails with external stakeholders

1.1. Ask the external stakeholder to send you a signed-only message

The external stakeholder must click on the **Sign button** before sending the e-mail.

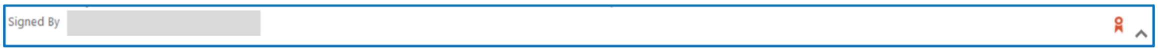


If the stakeholder does not have secure email, (s)he can install it himself/herself or through their company's IT support - see section 2.

1.2. Open the signed e-mail and verify that the user is trusted

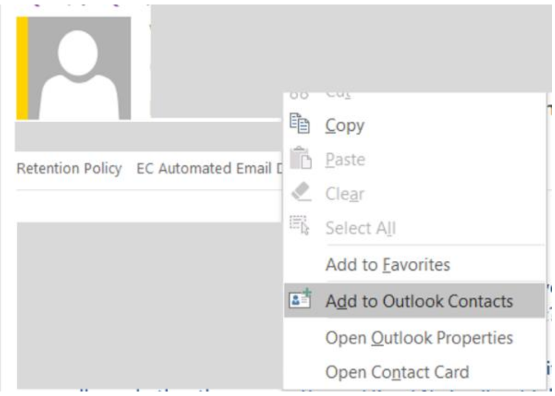
1.2.1. If the sender's Certification Authority root certificate is already trusted

If the message opens immediately and you see the **red ribbon** icon on the right, it means that the sender's Certification Authority root certificate already exists in your system.



Right click on the sender's name and click on **Add to Outlook Contacts**.

This will add the sender's address and certificate to your contacts. If the contact already exists, it will be updated.



1.2.2. If the sender’s Certification Authority root certificate is NOT trusted yet

N.B. This step should only be done with stakeholders that you know.

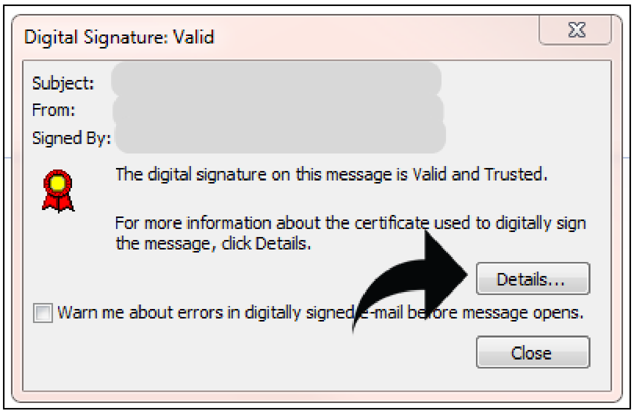
If you see a red warning on the right side of the e-mail, you must trust the sender’s Certification Authority root certificate.

Before trusting a certificate, you need to confirm the thumbprint with your stakeholders. The thumbprint is a code that you will find in the certificate’s properties (see points d & e below).

For this step, you may require assistance from the PKI team through the IT Helpdesk.

Follow the steps:

a) Click on the **Signature icon** and then on the **Details button**



Digital Signature: Valid

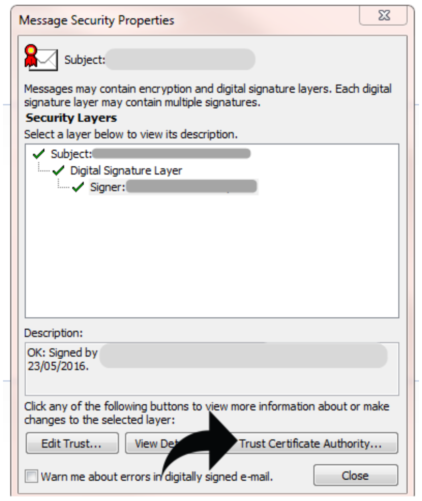
Subject: [redacted]
From: [redacted]
Signed By: [redacted]

The digital signature on this message is Valid and Trusted.

For more information about the certificate used to digitally sign the message, click Details.

□ Warn me about errors in digitally signed e-mail before message opens.

b) Click on the **Trust Certificate Authority** and then on **Trust**



Message Security Properties

Subject: [redacted]

Messages may contain encryption and digital signature layers. Each digital signature layer may contain multiple signatures.

Security Layers

Select a layer below to view its description.

✓ Subject: [redacted]
✓ Digital Signature Layer
✓ Signer: [redacted]

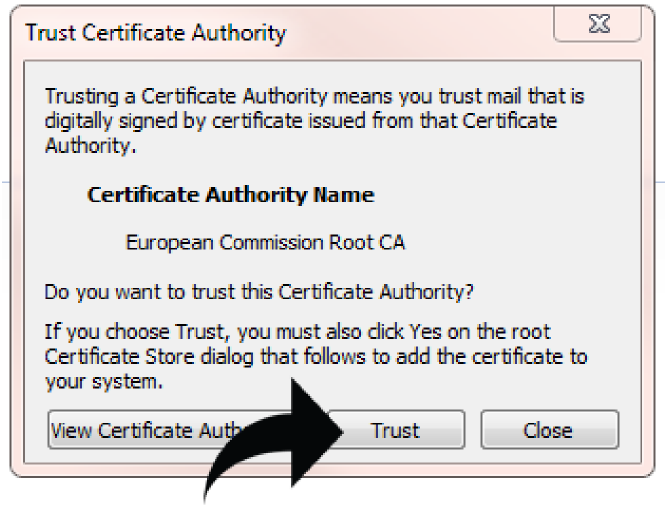
Description:

OK: Signed by [redacted] 23/05/2016.

Click any of the following buttons to view more information about or make changes to the selected layer:

□ Warn me about errors in digitally signed e-mail.

→



Trust Certificate Authority

Trusting a Certificate Authority means you trust mail that is digitally signed by certificate issued from that Certificate Authority.

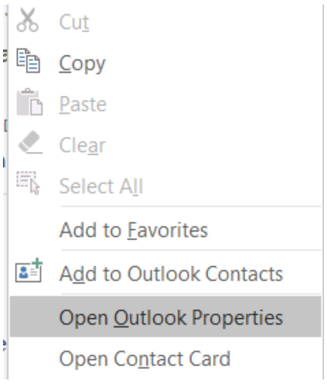
Certificate Authority Name

European Commission Root CA

Do you want to trust this Certificate Authority?

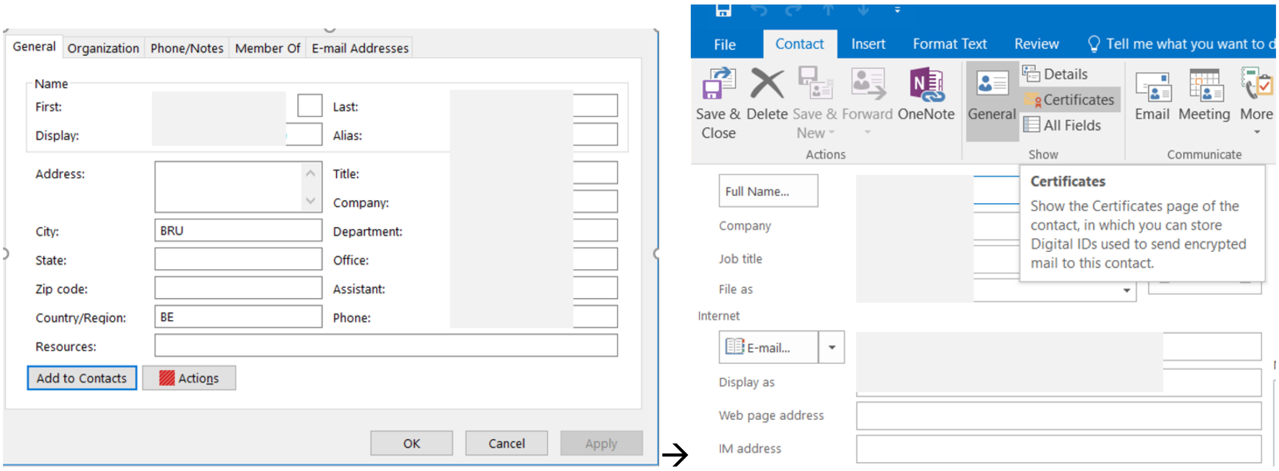
If you choose Trust, you must also click Yes on the root Certificate Store dialog that follows to add the certificate to your system.

c) Return to the signed message, right click on the sender’s name and click on **Add to Outlook Contacts**. This will add the sender’s address with certificate to your contacts. If the contact already exists, it will be updated.



d) To check if the certificate was imported correctly, right-click on the sender’s name, and then click on **Open Outlook Properties** in the menu.

e) In the window that opens up, click on **Add to Contacts**, and then click on **Certificates.** Double click then on the name of the user certificate (or digital ID) and under the **Details** tab you will find all the details of the certificate, including the thumbprint code mentioned above.



City: BRU
Department:
Country/Region: BE

Certificates
Show the Certificates page of the contact, in which you can store Digital IDs used to send encrypted mail to this contact.

1.2.3. If the sender’s Certification Authority root certificate is not sent with the e-mail

In this case, the **View Certificate Authority** button mentioned in the previous section is missing. The sender can be added as a contact, but the root certificate cannot be imported. Ask the external stakeholder to send the root certificate as **.cer** or **.crt** files.

1.3. Test the encrypted exchange of e-mails

You can now send encrypted e-mails to the external stakeholder, either in reply to his/her initial signed email, or by creating a new e-mail and clicking on the **Encrypt** and **Sign** buttons.

2. How to get S/MIME certificates - explanation for external stakeholders

These suggestions are for information only. We recommend that you contact your **IT support** and ask for the two following actions:

a) **To trust the Commission's Certificate Authority**, available online: http://ec.europa.eu/dgs/human-resources/commissign/index_en.htm

b) To receive **S/MIME certificates**, in line with your corporate policy.

In case you are a **personal user**, or your organisation does not provide IT support, please see below how to use an S/MIME certificate with Outlook. Guidance is available online for other popular e-mail clients by searching for S/MIME and the name of your e-mail client.

In a nutshell, **to exchange encrypted e-mails with Commission staff**, you must first:

a) Install your keys and certificates

b) Import the Commission's CommisSign certificates

c) Configure the security settings for your e-mail client

d) Send your public key(s) and, if necessary, the Certification Authority's root certificate(s) to your Commission partners. Your public key is needed for Commission staff to send you encrypted messages, while the certificate is required for the Commission staff to verify your digital signature.

2.1. Choose a Certification Authority

Choose a Certificate Service Provider (CSP) to issue your certificate, such as:

- **Symantec** (https://www.symantec.com/products/information-protection/digital-ids-secure-email),
- **GlobalSign** (http://www.globalsign.com/),
- **Thawte** (http://www.thawte.com/),
- **Ascertia** (http://www.ascertia.com/)

- Or any other CSP that delivers certificates to the public. Your government may also in deliver in some cases signing and encryption certificates.

To generate and install the certificates follow the provider's instructions.

2.2. Get your personal digital certificate or ID

The certification procedure depends on the Certification Authority you choose and the level of security you need. Most providers provide an online tutorial.

2.3. Verify your personal certificate in Internet Explorer

Go to **Tools > Internet Options > Content > Certificates > Personal**

If your certificate is not listed, you will need to import it manually from a PKCS12 certification file (.p12 or .pfx extension).

Refer to the guidance of your certificate provider on how to import your personal certificate if this is not done automatically.

2.4. Configure the security for Outlook (if not automatically done by your certificate provider)

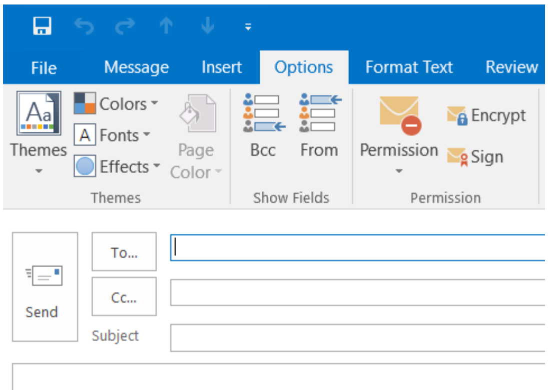
After importing your personal certificates in Internet Explorer, set up the Outlook security:

a) Go to: **File > Options > Trust Center > Trust Center settings > E-mail security**

b) Click on the **Settings** button.

c) Outlook looks for signing and encryption certificates that correspond to your e-mail 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 on the **Choose** button for **signing certificate** and **encryption certificate** and select the correct certificate.

d) Click the **OK** button to terminate.



e) Test that it works by creating a new mail. Go to the **Options** tab. The **Encrypt** and **Sign** buttons should both be available now. You can now send a signed, but not encrypted, e-mail to your counterpart in the Commission.

2.5. Import the Commission Certification Authority's root certificate in your system

You may download this from the **link below.** Open the link with Google Chrome or Mozilla Firefox. The certificate will be downloaded automatically.

http://ec.europa.eu/dgs/personnel_administration/commissign/csselfder.cer

Import the certificate in your certificate store and click on **Install**.

Alternatively, you may follow the **procedure for Commission users described above** - ask your counterpart in the Commission to first send you a signed e**-**mail, and then manually trust the CommisSign Certification Authority as explained in step 1.2.2. above.

You may also ask your local system administrator to trust the Commission Certification Authority for all the relevant users' workstations.

GLOSSARY

Digital certificate or digital ID

A digital certificate identifies you and guarantees the link between your public key and your identity. It must be obtained from a Certification Authority (CA), which your recipients must trust.

At the Commission, the Secure Email (SECEM-2) is based on standard X509 V.3 certificates and contains information such as:

- The user’s name and e-mail address
- The user’s public key
- The certificate’s expiry date
- The certificate’s serial number
- The name and digital signature of Certification Authority (the entity that issued the certificate)

The digital certificate must be stored in the software application(s): the E-mail application or the web browser.

Public & private keys

The most advanced way to sign and encrypt messages is through a mechanism using key pairs. A key pair consists of a private key and a public key. Both keys are generated at the same time and linked together.

In most cases, the signing key and encryption key are the same, but it is possible to have a key pair for signing and another key pair for encryption (this is the case for Commission users).

- **Same key pair for signing and encryption**

Your **private key** is used to digitally sign your messages and decrypt ciphered messages that you receive.

Your **public key** is used by others to encrypt messages for you. It can be distributed to all your recipients without harming its integrity.

- **Different key pairs for signing and encryption**

The **private signing key** is used to digitally sign your messages.

The **public signing key** is used by others to verify your signature. This key is always sent with a signed message, so you do not have to communicate it to your recipients separately.

The **private encryption key** is used to decrypt ciphered messages that you receive.

The **public encryption key** is used by others to encrypt messages for you. This key can be distributed to all your recipients without harming its integrity.

Secure/Multipurpose Internet Mail Extension (S/MIME) protocol

It is a technology based on asymmetric cryptography, which allows you to protect your e-mails against interference.

It also allows you to digitally sign your e-mails to guarantee to the recipient that you are the legitimate originator of the message. This makes it an effective weapon against phishing attacks, for example.

To read S/MIME packaged e-mail messages, your e-mail client must understand the S/MIME standard, otherwise secure messages appear as e-mails with attachment *smime.p7m*.
e.g.: Outlook, Outlook Express, Mozilla Thunderbird, Evolution, or, KMail.

Trusting certificates

The safest way to trust a digital certificate is by trusting the issuing Certification Authority. Once the Certification Authority is trusted, all the certificates issued by it will be trusted automatically.

Please note that Outlook allows you to trust a user's digital certificate directly, without the need of trusting first the Certification Authority.

Trusting user certificates

The sender's Certification Authority root certificate(s) must have been imported in your system to verify the sender's signature.

Although this is not generally recommended, in case you cannot obtain the root certificate(s), Outlook allows you to trust the sender’s digital certificate directly instead of inheriting the trust from the Certification Authority. For this you must:

a) Open the signed message of your counterpart

b) Click on the **Signature** icon

c) Click the **Details** button and select **Signer**

d) Click the **Edit Trust** button

e) Select **Explicitly Trust** this certificate