Monitoring of the Implementation of Digital Tachograph - MIDT

EU-MIDT

Card Issuing & Networking Committee

EU-MIDT/CINC/012-2006

TACHOnet Project

TESTA Secure Mail System

PREPARED BY: European Commission
DATE: 03/08/2006
EU-MIDT Card Issuing & Networking Committee 012-2006

REF : EU-MIDT/CINC/012-2006

EU-MIDT SECRETARIAT DOCUMENT PREPARATION

OPERATION	NAME	ORGANISATION	DATE
PREPARED BY	DG TREN	European Commission	03/08/2006
CHECKED BY	Thierry GRANTURCO	Granturco & Partners	03/08/2006
APPROVED BY	Marie-Christine BONNAMOUR	Cybèle – MIDT Secretariat	03/08/2006
ISSUED BY	Secretariat MIDT	MIDT	03/08/2006

CHANGE CONTROL LIST

VERSION	DATE	NAME	DESCRIPTION

EUROPEAN COMMISSION
Directorate General Transport & Energy

ITS Galileo -Unit B5

TACHONET PROJECT
–
TESTA Secure Mail System

Document Approval

	NAME	FUNCTION	DATE	REFERENCE
Prepared by:	Y. Hardy	Project Officer	21 April 2006	TESTA Secure Mail System
Checked by:	L. Huberts	Project Owner	15 May 2006	
Approved by:	L. Huberts	Project Owner	18 May 2006	

Distribution List

	NAME	FOR INFO / APPROVAL
Member States	Cards Issuing Authorities	Info
Member States	Enforcement Authorities	Info

Change Control History

VERSION	DATE	AUTHOR	DESCRIPTION	PARAGRAPHS
01	21 April 2006	Y. Hardy		
01.01	29 July 2006	Y. Hardy	Updated	Chapter 3 & 4

Document Information

Creation Date	21 April 2006
Filename	TCN-SecureMailSystem
Number of pages	43

Table of Contents

1. INTRODUCTION

Background

On several occasions Member States involved in the TACHOnet project have expressed the real need of having the ability to exchange sensitive and confidential electronics documents over a secured communication network between the Member States' Cards Issuing and Enforcement Authorities

To that end, during the plenary meeting held in Warsaw, the European Commission presented the outcome of its investigation with regard to the possibility to set up a secure mail system accessible via the EC private TESTA network which would allow the Member States to transmit their sensitive and confidential data in a secure, reliable and user-friendly way.

The technical approach proposed by the European Commission was approved and adopted by a majority of the members and consequently, this was the kick-off for proceeding to the installation and deployment of a new test environment on the TESTA network which will be used to conduct a test phase aiming at verifying that this proposed secure mail system architecture is fully compliant with the Member States' expectations and requirements prior to envisaging any further concrete action in this direction, such as the possibility to use this system in production. The outcome of this test activity which should not exceed one month will therefore be crucial as it will determine the "Go" or "No Go" of this specific project.

To participate in this test phase, the European Commission looks forward to receiving the candidate countries who will be willing to devote a part of their working time for testing this secure mail system. Normally, a few hours per week should largely suffice in this context, though, it is of major importance to read carefully this document beforehand so as to realise concretely what is to be done at national level from a technical point of view to be ready to take part in this test activity and on the other hand, your level of involvement in this activity.

The goal of this document is to describe the prerequisites and the technical requirements to be taken into consideration in the candidate countries before starting the test. This means in other word that this document should be read by IT people having a deep knowledge and skills in network, mail and DNS server management with in addition, a good understanding of the use of PKI (Public Key Infrastructure) and certificates management, fundamental elements to have a better overview and understanding of the workload to be carried out, the time required for setting up all this test infrastructure in the premises of the Member States and the possible technical constraint(s) and/or issues to be sorted out.

Background

It is pointed out at this stage that all those tests will be achieved on the EC private TESTA network and no access to the Internet will be allowed or even possible. This might be one of the major issues for your IT team because TESTA mail traffic will have to be separated from the Internet mail traffic, as it is rather difficult to live them together on the same mail server, nevertheless, alternative solutions exist to overcome this issue but the choice will closely depend on your local configuration and implementation in place.

That being said, the role of the Member States who will reply positively shall mainly consist of thoroughly testing and validating the following elements:

- The reliability of the TESTA secure mail system & communication channel end-to-end
- The confidentiality and integrity built-in modules and mechanism
- The use of personal certificates
- The use of your local mail server facility and user mail tool
- The interconnection and data exchanges between the different actors playing a vital role in this workflow

It is worth noting that no "*Test Management Plan*" will be delivered for that purpose, because nowadays, mail tools are commonly used in all the community and end-users are used to using them every day whatever the type of product and dealer chosen, the standard functionalities are the same.

However, there is a slight difference in terms of configuration when sending encrypted and/or signed e-mail messages to outside world, but this point is covered in the chapter 4 hereinafter so that the testers can familiarise themselves with the technique and the procedure.

Somehow, I will remain at your disposal if you have any further question in connection with this document and this test phase, do not hesitate to contact me by e-mail, if need be: Yves.Hardy@cec.eu.int

2. TESTA BACKBONE & SECURE MAIL SYSTEM

TESTA

In every Member State, there is a local domain network which is interconnected through the TESTA backbone (also called EuroDomain).

By default, all traffic transiting over TESTA is fully encrypted by means of crypto-devices until the entry point of the Member State and then decrypted automatically before continuing its route until the intended recipient.

Therefore when using the standard TESTA mail system, no guarantee can be given with regard to the confidentiality and integrity of data sent by e-mail end-to-end and consequently, it goes without saying that this has 2 major drawbacks in this context, namely:

1. the fact that sensitive information cannot be transmitted because at Member State level, network is not fully trustworthy, hence, high risk of security breach and vulnerability

2. At TESTA level, the unencrypted e-mail messages will pass through a TESTA mail relay server in clear text allowing any third party or malicious user(s) to access this information easily

To overcome this potential problem, the aim consists of securing user mail accounts by encrypting the e-mail messages in order to make them illegible for anyone except for the intended recipient(s).

The principle is to use modern techniques and high standard solutions to ensure that e-mails cannot be read during transit, preventing to that end, any kind of vulnerability when transiting through numerous network nodes before reaching its final destination.

How secure e-mail works

Secure e-mail can be split into two categories, namely:

A. Signed e-mail:

A signed e-mail is an e-mail attached with your digital signature. Digital certificate is the electronic counterpart to driving licence or passport. It is issued by a Certification Authority (CA).

When the e-mail recipient reads your e-mail attached with your digital certificate, his mail program (e.g. Outlook Express) first check whether or not the digital certificate matches with the sender

How secure e-mail works, *contd*

(it is you) in the e-mail header. If ok, then it will check the issuer (CA) of your digital certificate. If it trusts your CA (prior to acceptance of issuer's root certificate to recipient's mail client certificate store is required), it believes the e-mail is truly sent by you. This is similar when presenting your passport to a customs official, he trusts you to be citizen of your country because he trusts the issuer of your passport.

How a mail client can trust a CA? Well, when a mail client accepts the digital certificate (i.e. root certificate) of a CA, firstly, it starts to trust the CA. Some of them are well known on the market and trusted such as: Verisign, Globalsign, etc, and their corresponding root certificate is preinstalled and recognized by default.

B. Encryption and decryption e-mail:

Upon applying digital certificate, a pair of keys called: *public key* and *private key* are generated at the same time based on the official and unique e-mail address. Those keys can be used by most PKI applications (PKI stands for Public Key Infrastructure), for example by sending an encrypted e-mail message. As a result, only the intended recipient can read it.

The recipient's corresponding public key and private must work in pair. The sender uses recipient's public key to encrypt a message and the recipient must use the corresponding private key to decrypt the message. An encrypted e-mail message requires recipient's valid private key to decrypt before the recipient can read it, as usual.

Extreme care should be taken when this technology is used to encrypt e-mail messages. Encrypted messages can only be decrypted by the required private key. Because of the very nature of this technology, it might be impossible to recover an encrypted message when the required private key is lost or corrupted. If in any case the key pair does not match any longer, the encrypted message could never be recovered.

C. Authentication and Identification Benefits:

- Secure e-mails by encrypting them so that other than the intended recipient cannot open them

- Digitally sign e-mails and prevent identity theft, i.e. prevent anyone from sending information using someone else's e-mail address in the false pretence of being that person

- Secure e-mail also verifies the integrity of the communication, letting you know that the e-mail is genuine and that it has not been tampered with while in transit. It also prevents your organisation from being slandered or sued for e-mails that it never actually sent, thus providing your organisation with total e-mail security

2.1 PREREQUISITES

Steps

For conducting the test phase, each Member State shall set up beforehand a local mail server physically connected to the TESTA network. The function of this mail server will be fourfold:

1. management of the local mail user accounts by assigning a username/password per user

2. creation of one mailbox per user account

3. centralizing the incoming e-mails in the users mailboxes

4. sending and receiving e-mails to all registered recipients

At TESTA level, several Mail Relay Services are available and configured for high resiliency. In short, a Mail Relay is a SMTP (Simple Mail Transport Protocol) service which acts as an e-mail sending gateway function. Its role is to relay and forward e-mails to the intended recipients located remotely.

So when sending out an e-mail to another Member State via your local mail server, it is first delivered to the TESTA mail relay server acting as gateway and stored temporarily on that server, until it is routed out via the TESTA network and then forwarded to the remote recipient(s) who can open and read the received e-mail

The advantages of this feature are the following:

- 5 days store and forwarding
  - Repeated delivery attempt will be made for undelivered/returned messages for 5 days
  - Delivery is attempted every 2 minutes
- Non-delivery reports
  - If after for 4 hours, the service has been unable to deliver an e-mail, a message will be sent to the originator warning this latter that the mail item has not been delivered
  - A non-delivery report can also be sent to the originator after 5 days (if need be) if the mail item has not been delivered by then
- No additional hardware or software required at TESTA level

Steps,
continued

- Completely in-house e-mail service maintained by the EC support team
- Monitoring tool available for testing and verifying the availability of this latter 24 hours a day and 7 days a week
- All TESTA Mail Relay Servers are configured to scan all incoming e-mail against possible intrusion of viruses
- The log of the TESTA Mail Relay provides evidence that e-mails are routed and forwarded via the TESTA network
- In the event of non-availability of the destination mail servers, e-mails will be stored in a queue and as explained above, several attempt will be performed at regular interval until the remote mail server is operational again

Once the mail server is configured correctly at national level, the next step is to install and configure the Microsoft Outlook Express application (this latter can be downloaded for free from the Microsoft website) on the local workstation of the testers who will participate in this test phase. Communication between the mail client tool and the local mail server will be done through the use of the POP3 protocol (POP stands for: Post Office Protocol) in view of allowing the users to access their respective mailbox configured on the mail server

One of the built-in functions of the POP3 communication protocol is to transfer the e-mails stored on the mail server to the mail program of the user, so that, there is no need to remain constantly connected to the mail server for reading and replying to the received e-mails

It is worth noting that POP3 protocol cannot send e-mails. To send e-mails, the SMTP protocol is used instead. Technically speaking, SMTP is the single protocol used to transfer e-mail messages across the TESTA network between mail servers. In this context, both protocols are required.

The following diagram hereunder illustrates very briefly the different components intervening in the workflow between 2 Member States and the TESTA backbone. In this configuration the Member States' mail servers are instructed, by the DNS to forward all outgoing e-mails to the TESTA Mail Relay Servers. This is achieved by defining the IP addresses of those servers in the MX records of all zones.

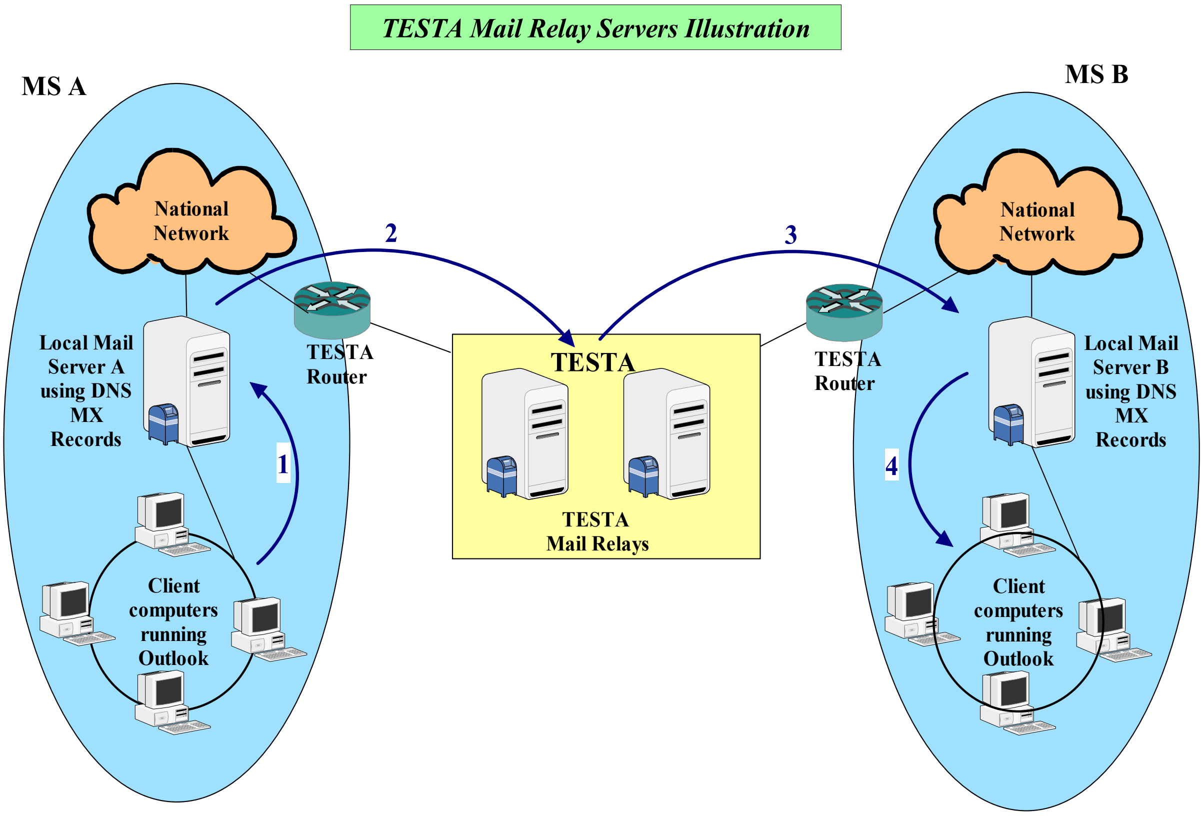

TESTA Mail Relay Servers Illustration
MS A
MS B
National Network
National Network
Local Mail Server A using DNS MX Records
Local Mail Server B using DNS MX Records
TESTA Router
TESTA Router
TESTA
TESTA Mail Relays
Client computers running Outlook
Client computers running Outlook
1
2
3
4

Figure 1 – Mail Relay Server Illustration

TESTA Mail Relay Server

1. The user of MS A belonging to the mail client community sends an e-mail to a user located in MS B, firstly, his e-mail is transmitted to the local mail server

2. Upon receiving this message, the local mail server detects that the domain name used in the e-mail address is: eu-admin.net, consequently, the mail server knows that this message has to be sent out to the TESTA Mail Relay service by using the DNS MX Record which points to the IP Address of the TESTA Mail Relay Servers

3. Once received, the Mail Relay service scans the incoming e-mail to check the absence of virus. If ok, the Mail Relay reads the message's header so as to know to whom the message is intended, then, the e-mail message is forwarded accordingly to the remote mail server of MS B.

4. The MS B mail server stores the e-mail message to the corresponding user mailbox and finally, warns the end-user that a new e-mail came in and is available for reading.

TESTA Mail Relay Server, *continued*

The information regarding the real TESTA Mail Relay Servers IP addresses are given in the next section of this document. Those addresses shall be configured by the Member State's mail server administrator in view of re-routing all the intended TESTA e-mail messages to the TESTA Mail Relay so that upon receiving them, this latter shall forward the messages to the corresponding destination recipients.

2.2 DNS IMPLEMENTATION

Introduction The goal of the DNS is to provide the name to IP address translation. A full description of the current DNS structure of TESTA is outlined in another document called: "*TESTA – DNS How To*", If need be, this document can be provided upon request to be sent to the attention of Yves Hardy by e-mail: Yves.Hardy@cec.eu.int

In the framework of this secure mail system project, a zone forwarding configuration option has been chosen and set up because this feature is the most commonly used nowadays in modern DNS servers, this is also the preferred technical solution as it limits the traffic to the needed information and moreover, is fully compliant with the security accreditation of the TESTA network backbone.

This configuration instructs the DNS server to forward all requests for a specific domain to one or more dedicated DNS servers. The main benefit of this is that after the first DNS request, the information is kept and retained in a local cache for a certain time, this time factor is determined automatically by the eu-admon.net DNS servers.

The figure below (Fig. 2) depicts the different sequences when submitting a new DNS query to the domain eu-admin.net:

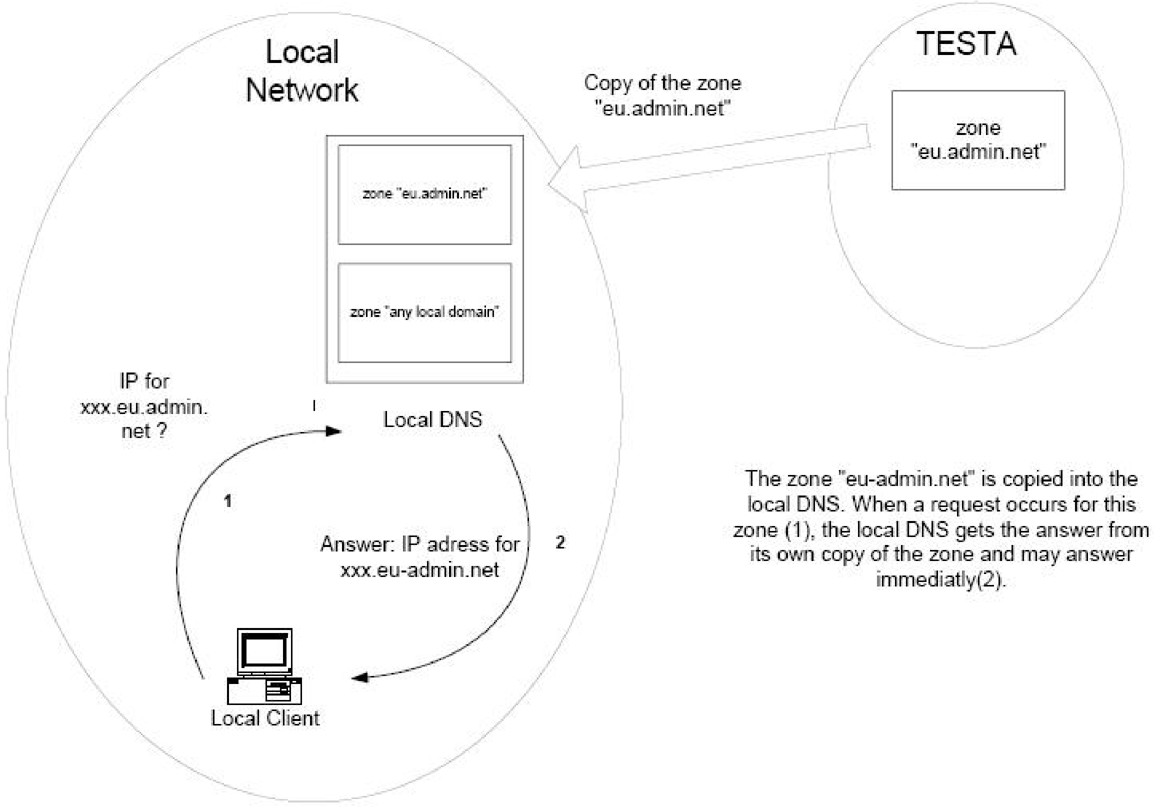

Local Network
TESTA
Copy of the zone "eu.admin.net"
zone "eu.admin.net"
zone "eu.admin.net"
zone "any local domain"
IP for xxx.eu.admin. net ?
Local DNS
1
Answer: IP adress for xxx.eu-admin.net
2
Local Client
The zone "eu-admin.net" is copied into the local DNS. When a request occurs for this zone (1), the local DNS gets the answer from its own copy of the zone and may answer immediatly(2).

Figure 2 – Zone forwarding diagram

2.3 DNS DOMAIN STRUCTURE FOR SECURE MAIL SYSTEM

Introduction

The internal policy the European Commission wants that for each project using the TESTA facilities, a specific sub-domain be created and assigned per country and per type of project. In the framework of the TACHOnet project, the following sub-domain has been allocated:

tcn.<country_code>.eu-admin.net

The structure of the TACHOnet sub-domain name can be regarded and depicted as follows in the figure 3:

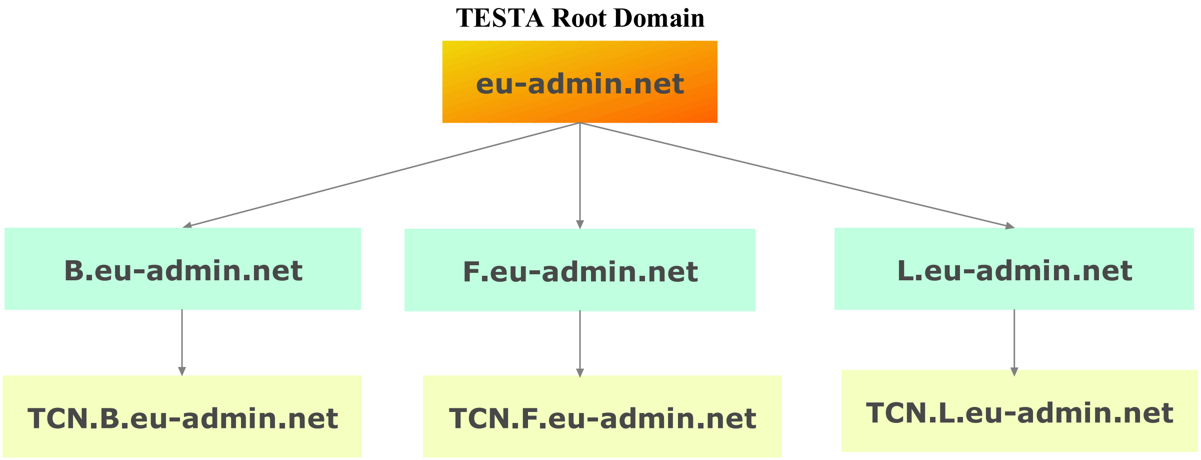


Figure 3 – TESTA Domain Name Structure

Email Address Syntax

The e-mail address to be used and configured in the Member States' local mail server shall be constituted of two parts. The first part before the '@' sign will comprise the first name and the surname of the tester followed after the '@' sign by the corresponding sub-domain name assigned for each country involved in the TACHOnet project.

For example, if the full name of the person located in Belgium is: Alain Dupont, the syntax of his e-mail address will be:

Alain.Dupont@tcn.b.eu-admin.net

This syntax is compulsory and in no case can be changed. It is pointed out at this stage that it is of major importance to stick to this rule because the mail client certificates will be issued based on this syntax and if there is a mismatch, the user will not be in position to encrypt and sign his e-mail messages and the test will fail.

Email Address Syntax, *continued*

It is worth noting and reminding that the management of the mail user accounts and mailboxes are under the responsibility of each Member State

Moreover, please pay attention to the fact that those e-mail addresses may only be used to exchange e-mails over the TESTA network, the domain name: **eu-admin.net** is a private domain name assigned to the European Commission but unknown on the Internet, this means in other words that Internet routing between Internet e-mail address and TESTA e-mail address is not allowed since TESTA is a private network not accessible via the Internet by any means.

3 TESTA ROUTING MAIL CONFIGURATION

The basis

The aim of this chapter is to give the reader a basic understanding of how mail servers are transmitting e-mails to the right destination servers. It covers only mail server dealing with SMTP traffic being the single communication protocol used to transfer e-mails between two or several external entities physically connected to TESTA.

When a mail server received an incoming e-mail, it checks the destination domain in extracting the full name after the "@" sign, which is used as delimiter to differentiate the name of the person from the domain name to whom she belongs to. Using this information, the mail server will attempt to find which server(s) is (are) currently managing this specific domain name.

The usual approach is to rely on DNS queries. DNS uses the MX (MX stands for Mail eXchange) resource record to implement mail routing, this is the easiest way and the most suitable technical approach for forwarding e-mails to other recipients. MX records specify a mail exchanger for a domain name.

The role of the mail exchanger is either to deliver the e-mail messages to the individual host it is addressed to, or, to dispatch them to other mail transports. MX records are given a preference value to prevent mail loops. This preference value of a mail exchanger determines the order in which a mail should use them.

Mailer will always attempt to deliver to the mail exchanger having the lowest preference value in priority (i.e. the highest priority). This means that the most preferred mail exchanger has the lowest preference value. If the highest priority mail exchanger fails, the mailer will attempt to deliver the messages to the next highest priority and so on.

If none of the destination mail server is available, the originated server will keep the e-mail message in its queue for a while and at regular interval (configurable in its settings) this latter will retry to transmit the message, after a number of failed retries, the e-mail message will be sent back to the mailbox sender with a warning message stating that the message could not be transmitted due to connection failure.

Practical Example

In the following DNS configuration, the Mail eXchanger (MX) record redirects all e-mail to a Mail exchanger. The format of the MX record is as follows:

Practical Example, *continued*

The syntax is: name IN MX preference hostname

Here is an example for the domain name: eu-admin.net being redirected to specific servers named: relay and relay2

```
eu-admin.net. MX 5 relay.eu-admin.net.
eu-admin.net. MX 10 relay2.eu-admin.net.
```

In this example, the MX records are configured to accept mail for the syntax: usernames@eu-admin.net and attempts to direct it to the host: relay.eu-admin.net, because this server has the lowest value assigned to the MX record, it gets the highest priority and preference.

However, if the relay.eu-admin.net is unreachable at the time of delivery, then the e-mail message is directed to the next MX record from the list, namely the host: relay2.eu-admin.net.

TESTA Mail Relay Servers

On TESTA, several mail relay servers have been configured in fault-tolerance in view of assuring the availability of the service 24 hours a day and 7 days a week without any interruption.

The diagram hereinafter (Fig. 4) shows you the deployment of those servers on the TESTA network backbone:

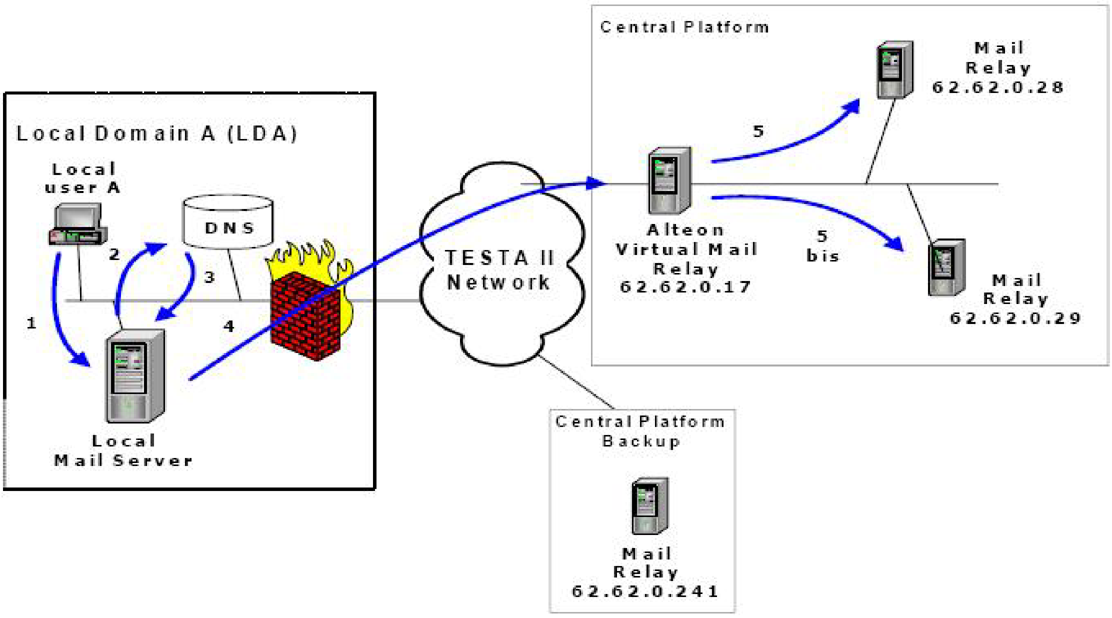


Figure 4 – TESTA Mail Relay Servers configured in high resiliency

TESTA Mail Relay Servers, *continued*

In a normal situation, e-mails are sent from the local Member State's mail server to the primary TESTA virtual mail relay server called: relay.eu-admin.net pointing to the IP address: 62.62.0.17

This server is also configured to balance the traffic load between the two real TESTA relay servers standing behind having as IP address:

- 62.62.0.28
- 62.62.0.29

On the diagram above (Fig. 4), they are represented by the blue arrows noted: 5 and 5bis

In case of failure of the load balancing switch, the Member State local mail server will send the traffic to the second TESTA mail relay server which has the second highest priority value. In this context, either the server: 62.62.0.28 or 62.62.0.29 will be used instead.

The figures hereunder (Fig. 5) depicts an example of simulation. The blue dashed arrows shows the possibility so communicate with one of the two backup TESTA mail relay servers:

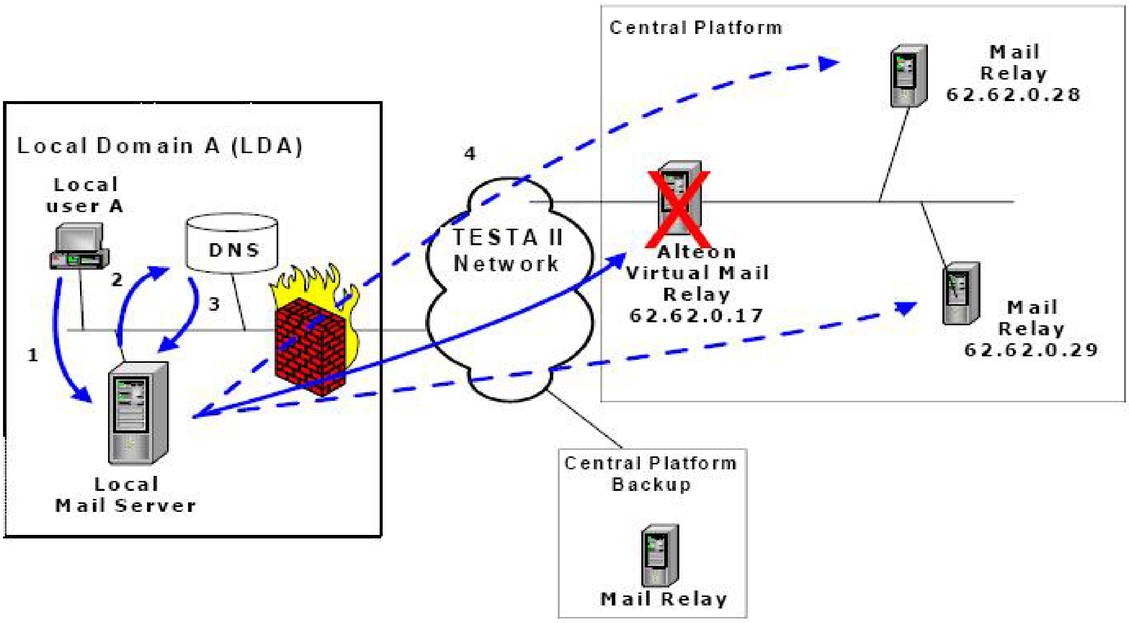


Fig 5 – one of the backup mail relay servers is used if the primary is down

TESTA Mail Relay Servers, *continued*

Last but not least, in case of major outage on the main mail relay servers, a backup server completely separated from the environment has also been set up in another premise so as to guarantee in any circumstance a high availability rate of the TESTA mail facilities as depicted in the figure hereunder (Fig. 6)

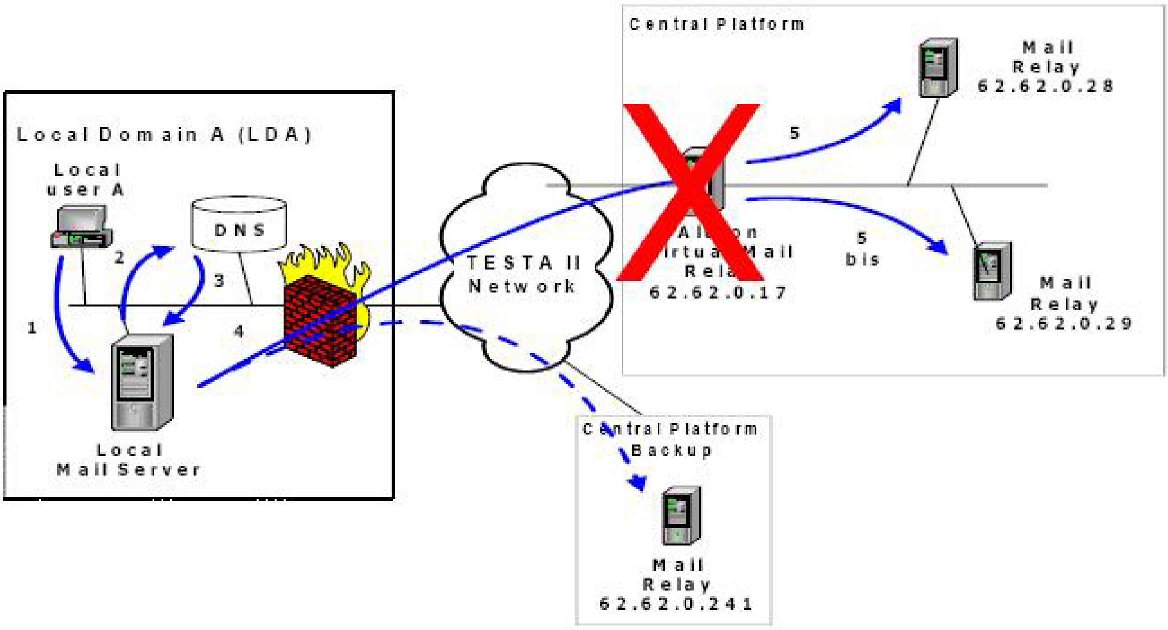


Fig 6 – Major outage, primary environment down – backup mail relay available

3.1 MEMBER STATES' MAIL CONFIGURATION & RESPONSIBILITY

Stage 1

A. In order to benefit from the resilience put in place on TESTA and in view of communicating and using efficiently all the TESTA mail relay servers, Member States' IT Administrators will be in charge of reconfiguring their local mail server and DNS entries by adding the following MX records accordingly:

```
eu-admin.net. MX 1   62.62.0.17  # primary mail relay server
eu-admin.net. MX 2   62.62.0.28  # backup mail relay server
eu-admin.net. MX 3   62.62.0.29  # 2nd backup mail relay server
eu-admin.net. MX 4   62.62.0.241 # 3rd backup mail relay server
```

B. Besides that, due to the fact that the communication protocol used between the Member States' local mail server and the TESTA mail relay servers is SMTP, the Member States' IT Administrator will ensure that their respective firewall be reconfigured to allow incoming and outgoing SMTP traffic to reach their destination. Keep in mind that SMTP traffic can be initiated in both directions

- ✓ Open Firewall port SMTP 25 from local mail server to:
  - ➢ 62.62.0.17
  - ➢ 62.62.0.28
  - ➢ 62.62.0.29
  - ➢ 62.62.0.249
- ✓ Form TESTA mail relay servers to MS local mail server

Once this action is successfully completely, as test, verify that you can open a 'telnet' session on port 25 on one of the TESTA mail relay servers. If the connection is established, your local firewall is configured properly, otherwise, the Firewall filtering settings need to be reviewed.

Stage 2

The second stage aims at filling in the "*TESTA SMTP Request Form*" document enclosed with this document in which you have to specify the local IP address and TESTA domain name assigned to your mail server as well as other administrative points in relation with the name of your organisation, the IT contact point, etc…

Once filled, the document must be sent back by e-mail to the attention of Yves Hardy for acceptance. Please note that if you have not received the TESTA form, please warn Yves Hardy by e-mail to get a copy.

MEMBER STATES' MAIL CONFIGURATION & RESPONSIBILITY

Stage 3 After completed stages 1 and 2, the next step is to create your local mailboxes on your mail server in respecting the syntax as mentioned in the previous section, namely:

First_name.surname@tcn.<country_code>.eu-admin.net

Note:

<country_code> is the Unece list of country code supported by the Member States involved in the TACHOnet project. You can find a copy of this list in Annnex A at the bottom of this document for more details.

For performing this test activity, Member States participating in this test phase will only create a maximum of 3 e-mail addresses per country following the syntax outlined above.

Once created, each Member State will send its list of addresses per e-mail to the attention of Yves Hardy (Yves.Hardy@cec.eu.int). In return, they will receive the corresponding mail personal certificate(s) to be installed on each individual workstation of the testers following the procedure described in the next section so that the test can be performed afterwards.

Test mail certificates will have a life span limited to 1 month, not renewable!, this means that Member States will have to devote time and commit themselves to participate actively in this test activity within the given month

4. DIGITAL ID

What is a Digital ID

A Digital ID, sometimes called a digital certificate is a file on your computer that identifies who you are. Some software applications use this file to prove your identity to another person or computer. Here are two common examples:

- When you bank online, your bank must be sure that you are the correct person to get account information. Like a driver's licence or passport, a Digital ID confirms your identity to the online bank

- When you send important e-mail to someone, your e-mail application can use your Digital ID to "digitally" sign the e-mail message. A digital signature does two things: it lets the recipient know the e-mail from you, and it tells them the e-mail was not tampered with from the time you sent it to the time they received it

A Digital ID contains the following information

- Your public key
- Your name and official e-mail address
- Expiration date of the public key
- Name of the company (CA) who issued your Digital ID
- Serial number of the Digital ID
- Digital signature of the CA (Certification Authority)

What can I do with a Digital ID

Software applications, networks and computers can use your Digital ID in several ways:

- ***Encryption*** (or data scrambling) is a way of protecting information before sending it from one computer to another. Typically e-mail applications use the Digital ID that belongs to the person receiving the encrypted e-mail message. In order to send someone encrypted messages, you need their public key

- ***Client authentication*** is the term used to describe how you (the client) prove your identity to someone else or to a computer. For example, online banks need to make sure that you are the correct customer for a given bank account. To prove your identity at the bank in person, you usually present your passport. When online, your software application (e.g. e-mail tool) presents your Digital ID

What can I do with a Digital ID, *contd*

- ***A Digital signature:*** like a hand-written signature. It shows that a person created or otherwise agreed to the document containing the signature. A digital signature actually provides a greater degree of security than a handwritten signature because this latter verifies both that the message originated from a specific person and that the message has not been altered either intentionally or accidentally. Furthermore, you sign a document and you cannot later disown it by claiming the signature was forged , in other words, this is called non-repudiation

How can I get a Digital ID?

If the test results are positive and satisfactory for the Member States, the TESTA secure mail system may be deployed in production to become fully operational for all the stakeholders.

In order to obtain your official personal certificates, it will be requested to fill in another administrative form produced by POSTECOM our new Certification Authority since 1st of June 2006 replacing Belgacom E-Trust, to acquire your personal Digital ID key which will be issued by POSTECOM, one Digital ID key will be issued per CIA clerk.

On the other hand, concerning this test phase, only 3 test Digital ID keys will be issued per candidate country selected to participate in this test activity. Their life span will be limited to 1 month

4.1 HOW DOES DIGITAL ID WORK

Key Pair

When you communicate with another person, you need a way to exchange information securely, so no one can intercept and read the information. Currently, the most advanced way to scramble (encrypt) data is through a system that uses key pairs.

A key pair consists of a public and a private key. The keys are used similarly to keys in a lock, except the key pair requires one key to secure the lock and another to open the lock.

With key pairs, the e-mail application uses one key to encrypt the message. The person who receives the encrypted message (or e-mail) then must use the matching key to decrypt the corresponding message. The problem with this process is how do you give someone the “key” to decrypt your message without allowing anyone else to get the key?

The solution is in the way the keys are used. When you want to send someone an encrypted message, you must first get their public key. You do this by asking the person concern to send you a signed e-mail message which contains the Digital ID and public key, then your local e-mail application can automatically store the Digital ID until you need to use it.

4.2 HOW DO I USE DIGITAL IDS

Basic Principle

Once you receive a Digital ID, you need to install it in the Outlook Express mail application required for this test. Once set up correctly, the mail application does most of the work for you, which makes using Digital IDs fairly easy.

In this context, you can secure e-mail to do the following:

- Digitally sign a message so that the recipient can verify the message came from you and not from an impostor. It is worth noting that signing a message also ensures its integrity, that is, it ensures that no one tampered with the message

- Encrypt a message so that no one can read it while it travels from your computer to another

As explained here above, when sending encrypted (secure) e-mails, firstly, you need to retrieve Digital IDs from people you communicate with, and then you can configure your e-mail application to encrypt your messages to those people.

In addition, it is pointed out that you can set up most e-mail applications to automatically sign and/or encrypt your messages or you can manually choose to do it on a case-by-case basis.

4.3 INSTRUCTIONS FOR INSTALLING YOUR PERSONAL CERTIFICATES

Purpose

Before sending and receiving secure e-mail, you have to install your personal certificate (digital ID) and the root certificate on your local workstation. The digital ID will allow you to sign e-mail with a digital signature that can verify who you are. It will be unique to you, just like your signature.

On the other hand, the root certificate is also mandatory because it will identify the official Certification Authority (CA) being in charge of signing and issuing the personal certificates for this test activity. It is called a root certificate because it is the certificate for the root CA. There is no higher certifying authority to sign its CA certificate.

Both certificates will be sent to the persons participating in this test phase by e-mail and the instructions described below will have to be carried out step-by-step:

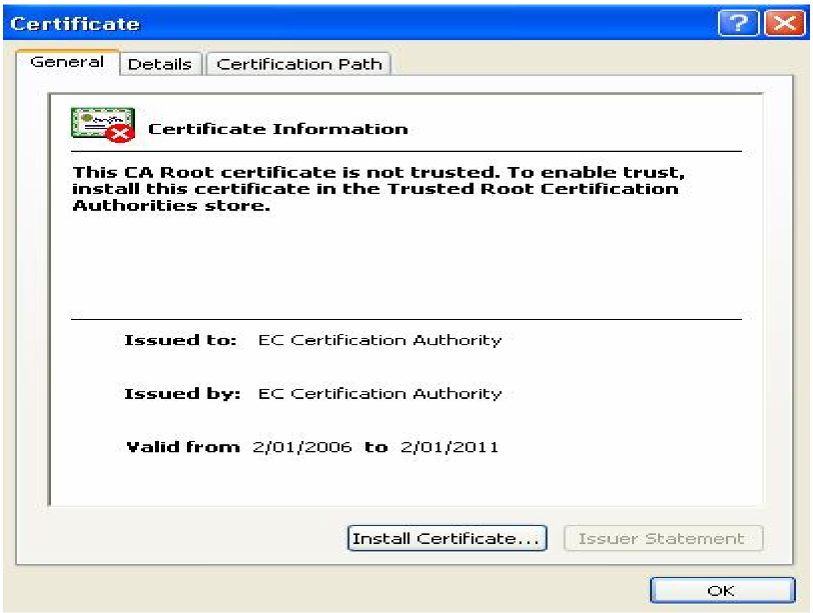
Installation instructions

The following certificate files will be attached to the e-mail:

- ✓ Root_CA
- ✓ EC_CA
- ✓ Mail.pfx

1. Root_CA file installation

Once copied on the local hard drive, you just double-click on the Root_CA file and follow the wizard:



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: EC Certification Authority

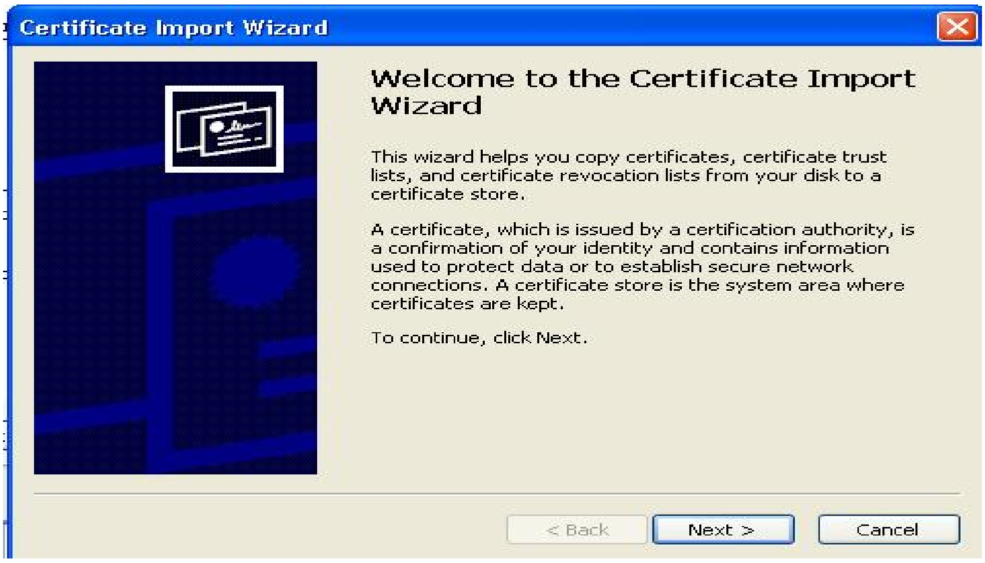
Issued by: EC Certification Authority

Valid from 2/01/2006 to 2/01/2011

Installation instructions, *continued*

As you can notice, by default the CA Root certificate is not trusted by windows and therefore, to enable trust, the aim is to install this certificate in the Trusted Root Certification Authorities store by simply clicking on the “Install Certificate” button

- Click on “**Install Certificate**” to proceed to the installation of the root certificate



Certificate Import Wizard

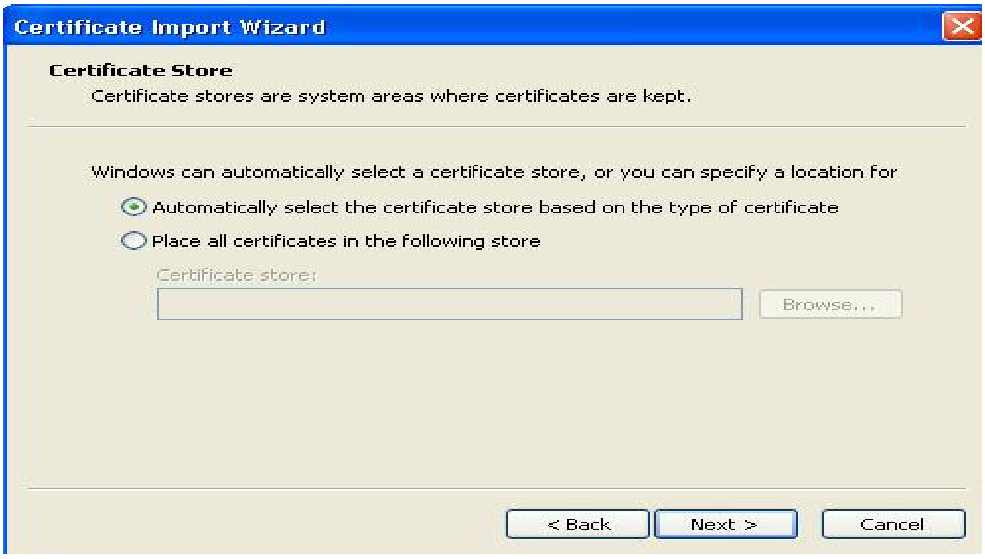
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

- Click on “**Next**” to continue



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

● Automatically select the certificate store based on the type of certificate

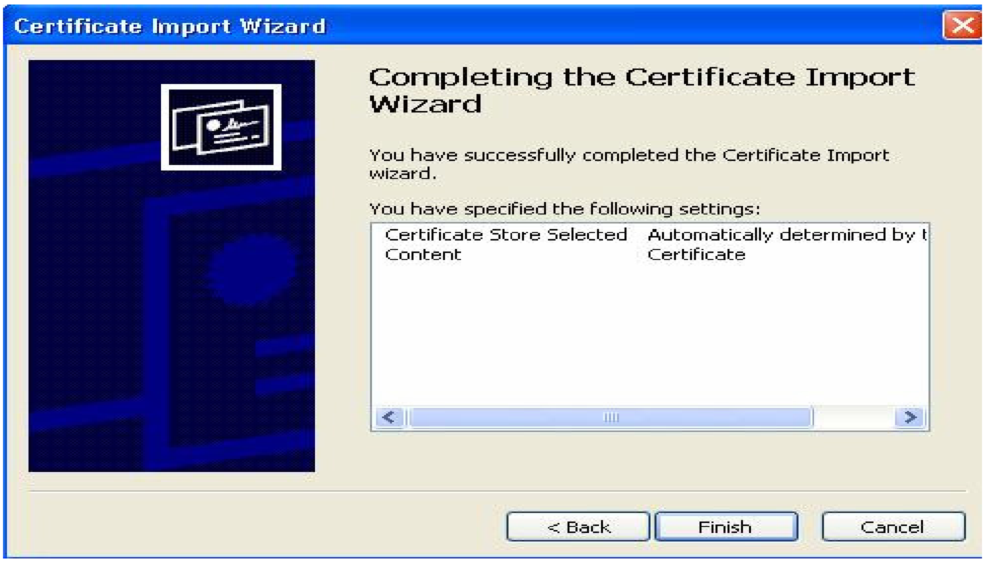
○ Place all certificates in the following store

Certificate store:

This stage is to copy the root CA certificate in the Microsoft Trusted Root Certification Authorities store. Use the default parameter and click on “**Next**” to continue:

INSTRUCTIONS FOR INSTALLING YOUR PERSONAL CERTIFICATES, *CONTINUED*

Installation instructions, *continued*



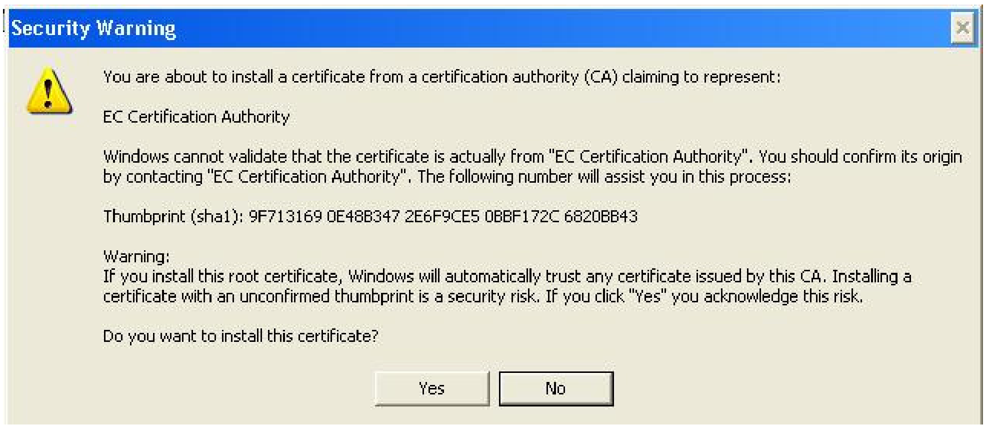
Completing the Certificate Import Wizard

You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	Certificate

The installation is completed. When clicking on “**Finish**”, the following security warning message will pop up on screen:



You are about to install a certificate from a certification authority (CA) claiming to represent:

EC Certification Authority

Windows cannot validate that the certificate is actually from "EC Certification Authority". You should confirm its origin by contacting "EC Certification Authority". The following number will assist you in this process:

Thumbprint (sha1): 9F713169 0E48B347 2E6F9CE5 0BBF172C 6820BB43

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

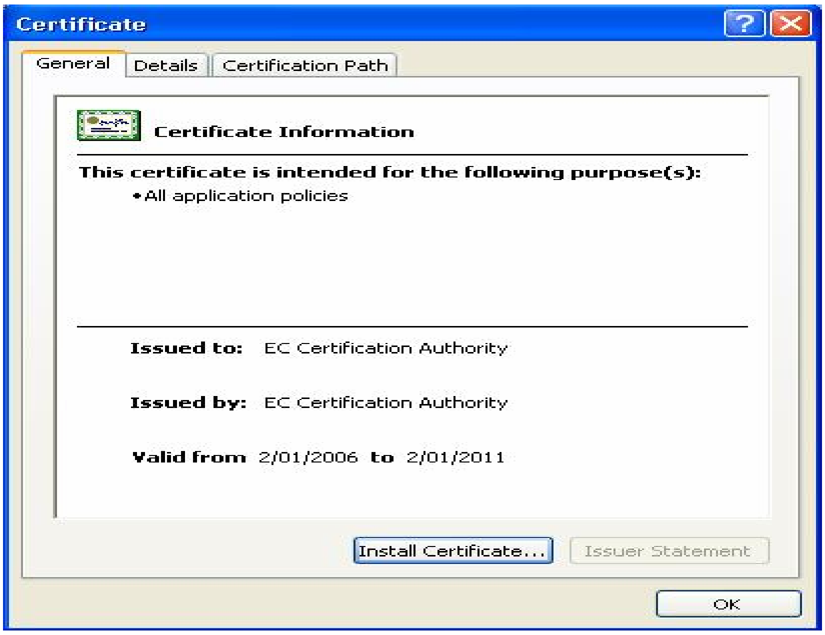
Do you want to install this certificate?

This message is a normal behavior because the official certification authority (i.e. EC Certification Authority) is unknown by default by Windows and therefore is not trustworthy. To trust it, you just have to click on “**Yes**” so that the process can be successfully completed.

2. EC CA file installation

This certificate is required to recognize the official Certification Authority. To install this file in Windows, simply double-click it and follow the wizard.

Installation instructions, *continued*



Certificate Information

This certificate is intended for the following purpose(s):
- All application policies

Issued to: EC Certification Authority

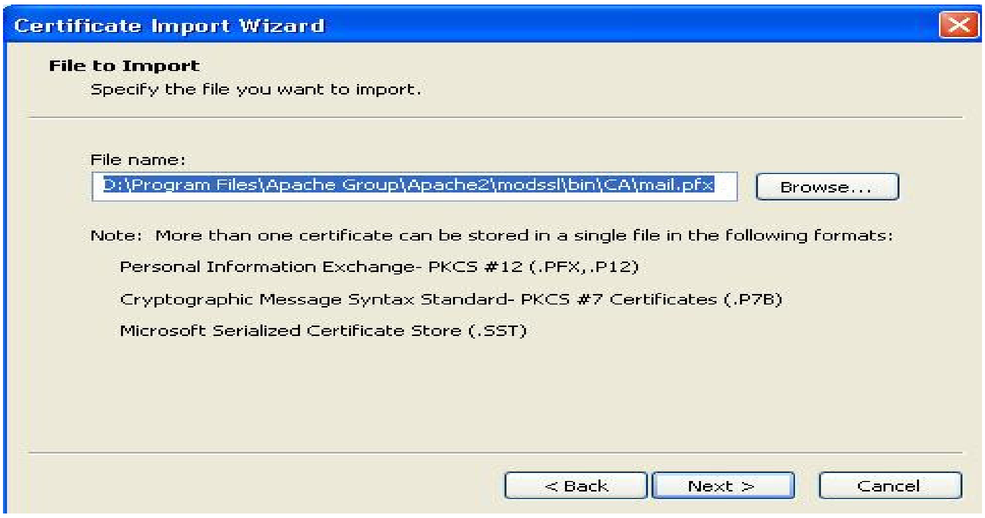
Issued by: EC Certification Authority

Valid from 2/01/2006 to 2/01/2011

You click on “**Install Certificate…**” and then when other windows appears, you just click on “**Next**” until its completion without changing any parameter

3. Mail.pfx file installation

To install this file in Windows, simply double-click it and follow the wizard:



File to Import
Specify the file you want to import.

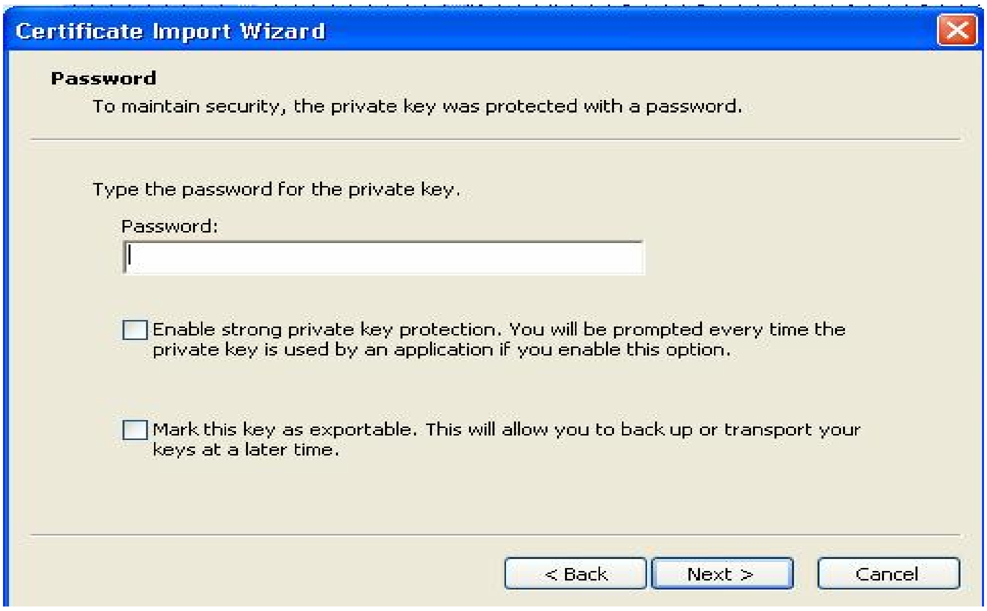
File name:
D:\Program Files\Apache Group\Apache2\modssl\bin\CA\mail.pfx

Note: More than one certificate can be stored in a single file in the following formats:
Personal Information Exchange- PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Store (.SST)

This window shows you the file name location. By default the location is correct and you can click on “**Next**” to continue

INSTRUCTIONS FOR INSTALLING YOUR PERSONAL CERTIFICATES, *CONTINUED*

Installation instructions, *continued*



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

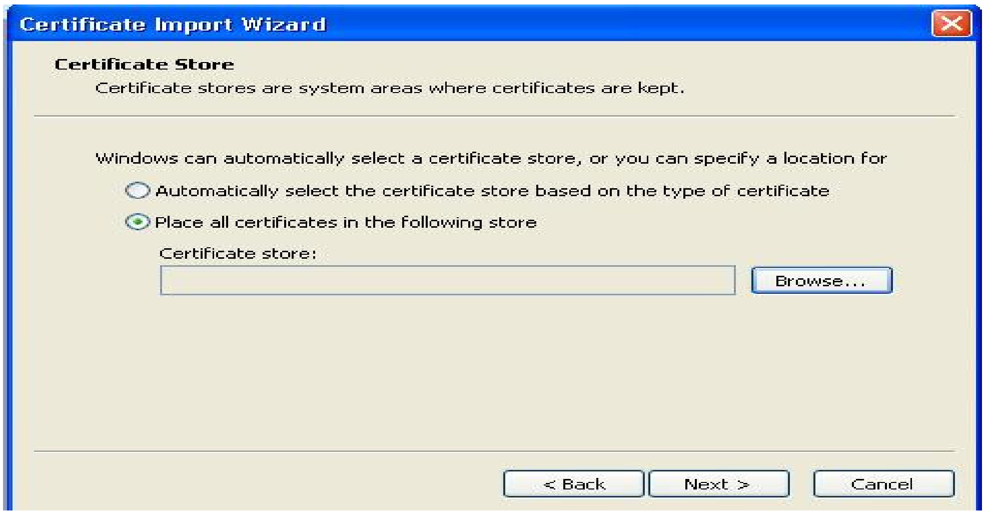
Password:

□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

□ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

Your personal certificate is protected by a password so as to ensure that it will not be used by any unauthorized or malicious user. Even though it is for test purpose, the same level of security policy is into force. To obtain your password, you have to send an e-mail to the following recipient: Yves.Hardy@cec.eu.int

Once received, to continue the installation process, you just have to click on the “**Next**” button



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

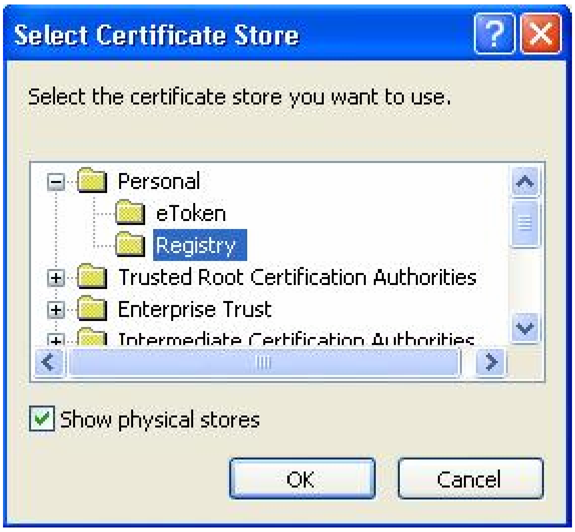
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

In this new window, you have to select “**Place all certificates in the following store**” and then click on the “**Browse**” button:

Installation instructions, *continued*



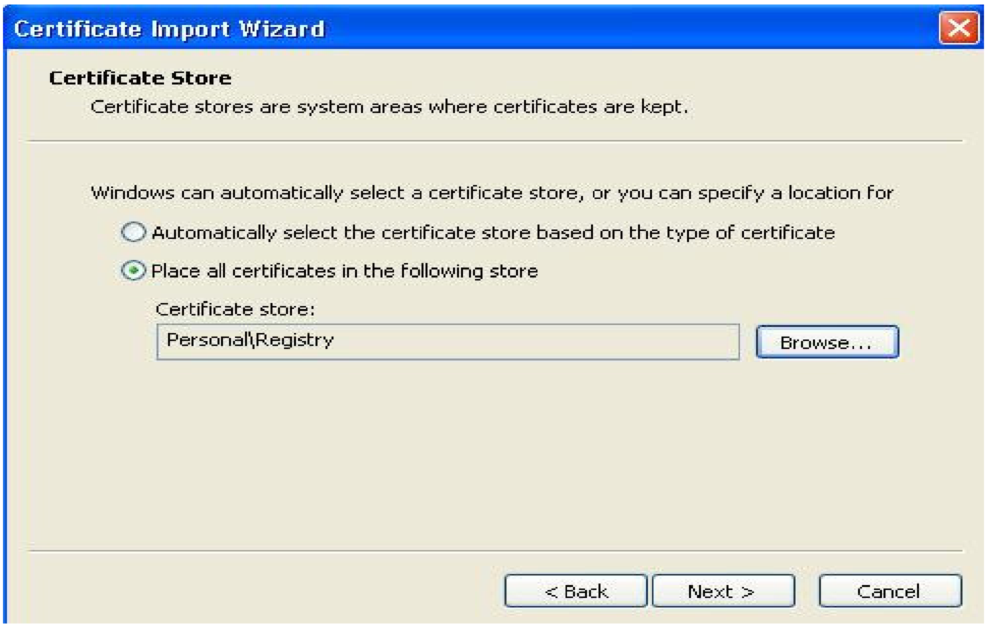
Select Certificate Store

Select the certificate store you want to use.

- Personal
  - eToken
  - Registry
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities

☑ Show physical stores

Here, firstly, you enable “**Show physical stores**”. From the list, you click on “**Personal**” and then “**Registry**”. Once done, click, on the button “**OK**” to continue.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

○ Automatically select the certificate store based on the type of certificate

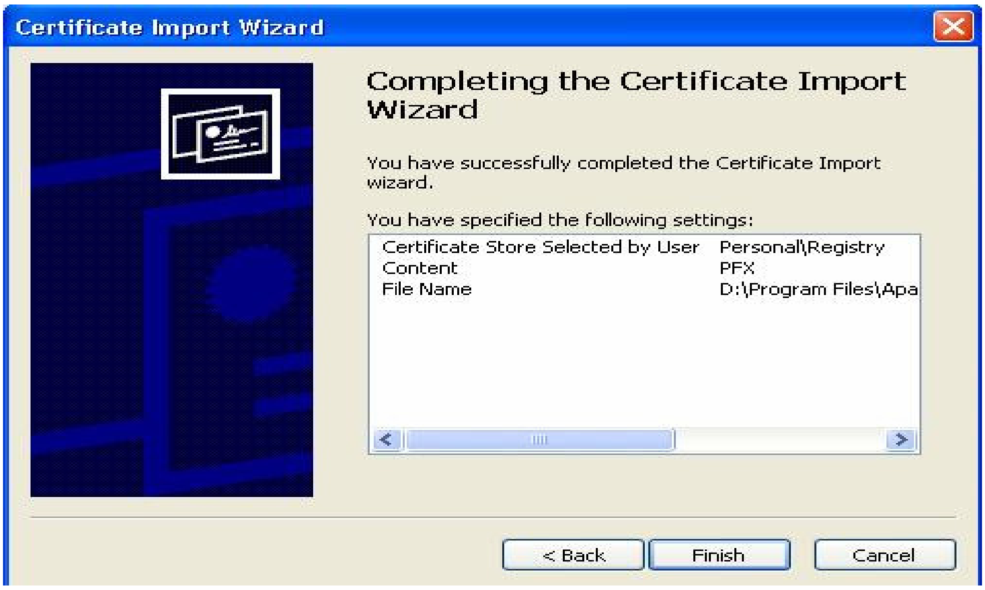
● Place all certificates in the following store

Certificate store: Personal\Registry

This new window pops up, click “**Next**”

INSTRUCTIONS FOR INSTALLING YOUR PERSONAL CERTIFICATES, *CONTINUED*

Installation instructions, *continued*



Completing the Certificate Import Wizard

You have successfully completed the Certificate Import wizard.

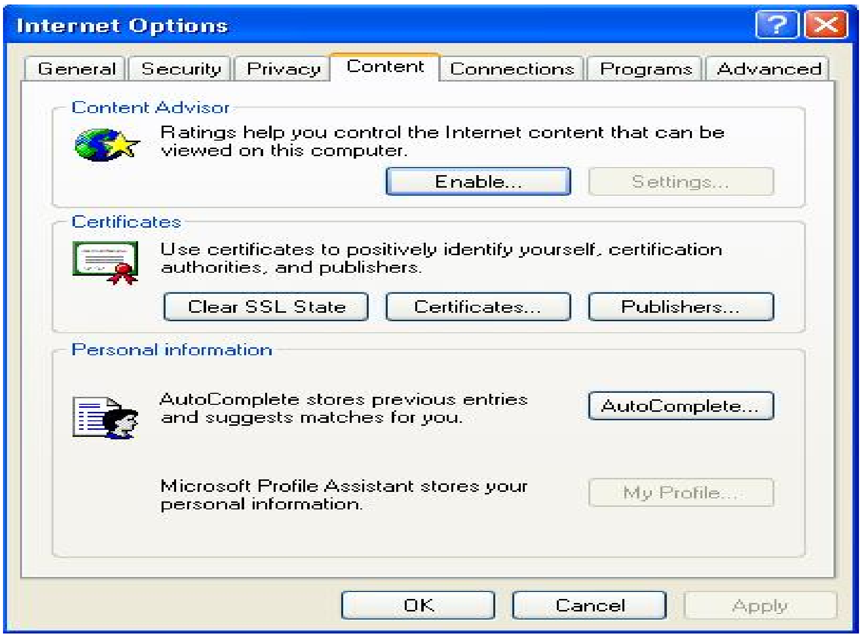
You have specified the following settings:

Certificate Store Selected by User	Personal\Registry
Content	PFX
File Name	D:\Program Files\Apa

The installation is about to be completed. Click “**Finish**” to import your personal certificate in the Windows Registry

Once that package is installed, the next step is to follow the directions below to export your public key in your Outlook Express Address Book.

1) Open your “Internet Explorer” and select the following menu: **Tools -> Internet Options -> Content**. You should get this window:



Ratings help you control the Internet content that can be viewed on this computer.

Use certificates to positively identify yourself, certification authorities, and publishers.

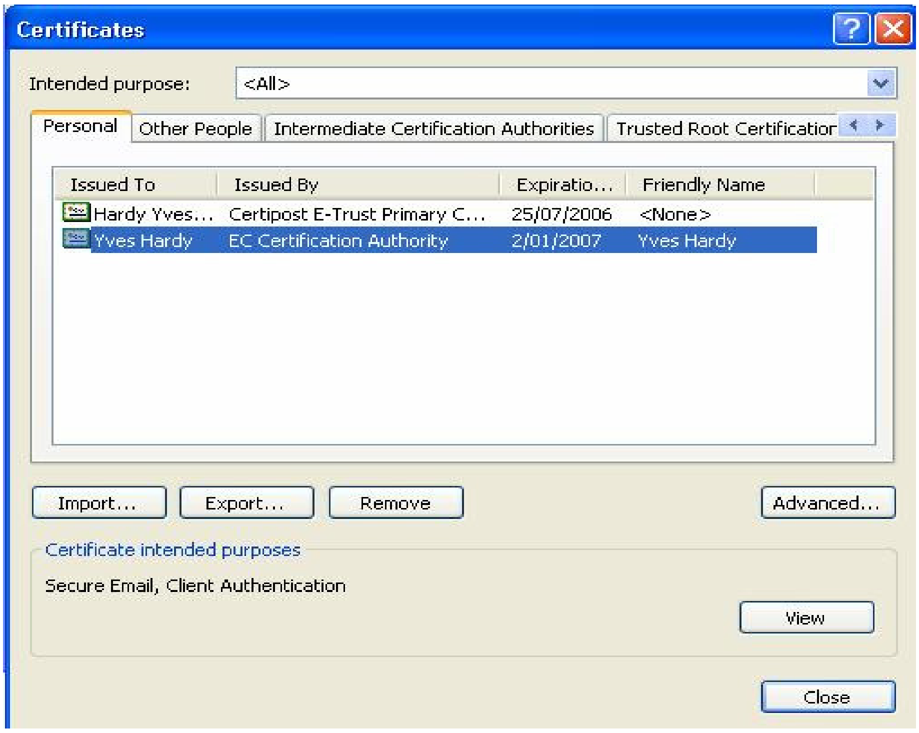
AutoComplete stores previous entries and suggests matches for you.

Microsoft Profile Assistant stores your personal information.

INSTRUCTIONS FOR INSTALLING YOUR PERSONAL CERTIFICATES, *CONTINUED*

Installation instructions, *continued*

Click on “**Certificates**” button, the following new window should appear on screen:



Intended purpose: <All>

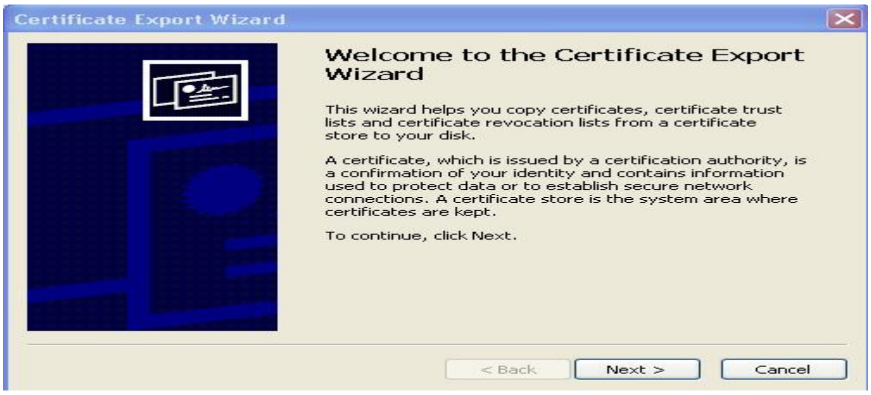
Issued To	Issued By	Expiratio...	Friendly Name
Hardy Yves...	Certipost E-Trust Primary C...	25/07/2006	<None>
Yves Hardy	EC Certification Authority	2/01/2007	Yves Hardy

Certificate intended purposes

Secure Email, Client Authentication

In the Personal menu, you should see appearing the name of your personal certificate. In this example, I have highlighted my personal certificate to be used in this context.

Then click on the “**Export**” button. The aim of this step aims at exporting and copying your personal certificate’s public key in order to import it afterwards in the Microsoft Outlook Express mail tool and in your Address book. Without this procedure, Outlook Express cannot be used for sending and receiving encrypted and digitally signed e-mails to/from the other mail recipients.



Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

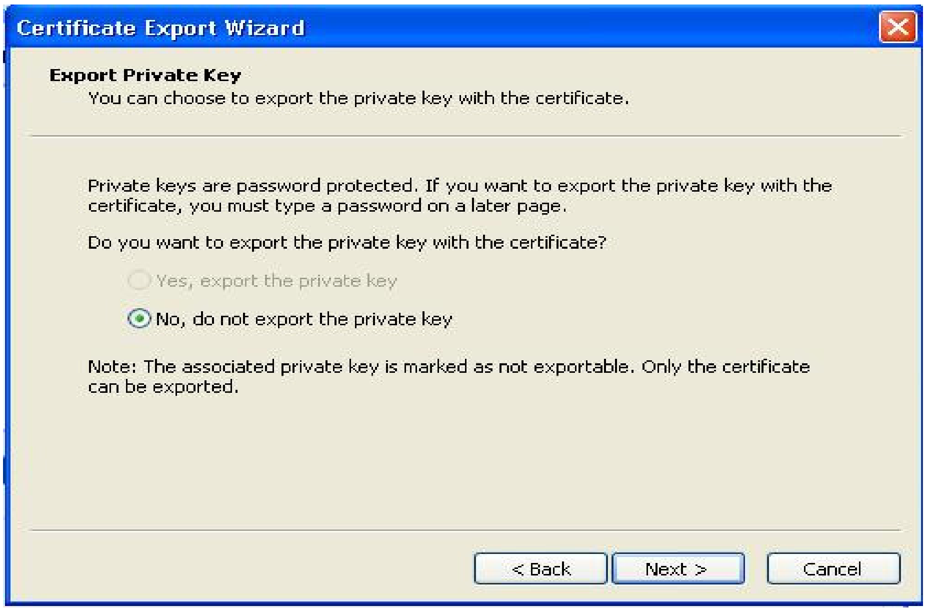
To continue, click Next.

INSTRUCTIONS FOR INSTALLING YOUR PERSONAL CERTIFICATES, *CONTINUED*

Installation instructions, *continued*

Click “**Next**” to continue

2) Now, the wizard asks you whether you want to export your private key which is embedded in your personal certificate, the answer is no! Select “**No, do not export the private key**” then click on “**Next**” to go further



Certificate Export Wizard

Export Private Key

You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

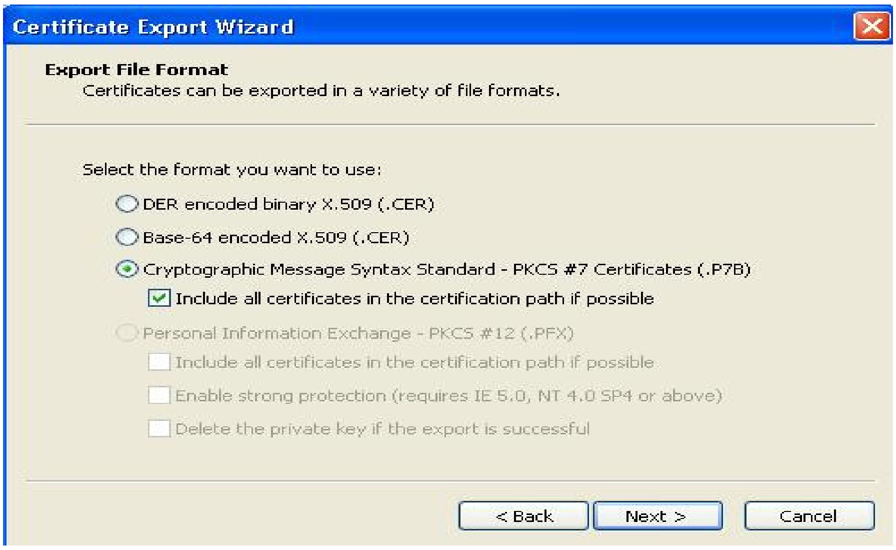
Do you want to export the private key with the certificate?

○ Yes, export the private key

● No, do not export the private key

Note: The associated private key is marked as not exportable. Only the certificate can be exported.

3) The next step is to specify the type of data format to be used for exporting the personal certificate. It is important to select the **Cryptographic Message Syntax Standard format: PKCS#7** including **all certificates in the certification path** as shown hereunder:



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

● Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

☑ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

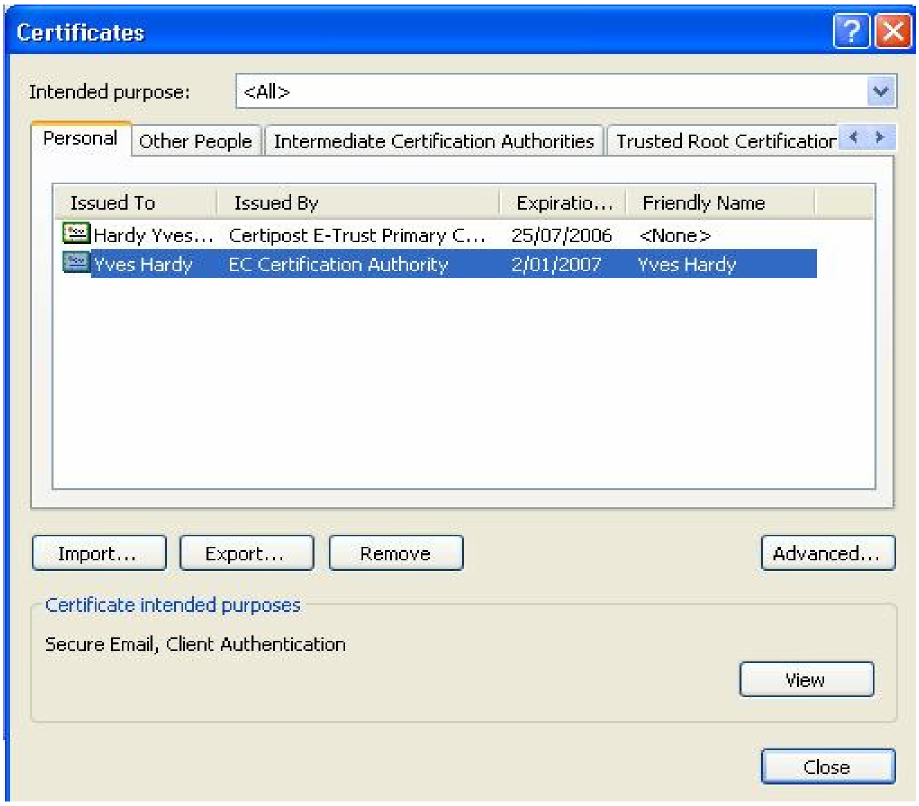
☐ Include all certificates in the certification path if possible

☐ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)

☐ Delete the private key if the export is successful

Installation instructions, *continued*

When done, click on “**Next**” to continue the process



Certificates

Intended purpose: <All>

Personal
Other People
Intermediate Certification Authorities
Trusted Root Certificatior

Issued To	Issued By	Expiratio...	Friendly Name
Hardy Yves...	Certipost E-Trust Primary C...	25/07/2006	<None>
Yves Hardy	EC Certification Authority	2/01/2007	Yves Hardy

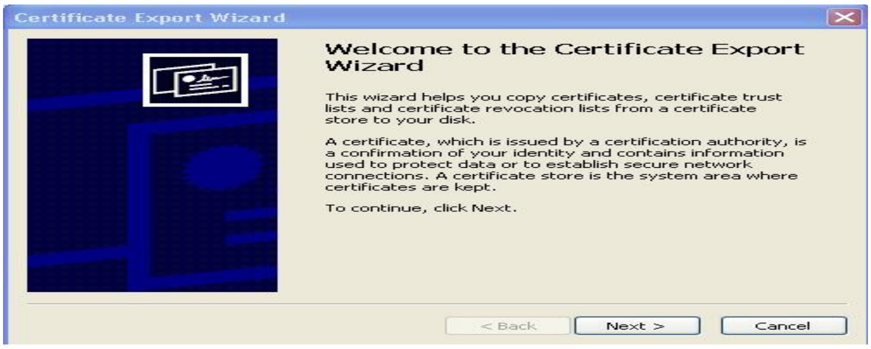
Import...
Export...
Remove
Advanced...

Certificate intended purposes

Secure Email, Client Authentication

In the Personal menu, you should see appearing the name of your personal certificate. In this example, the personal certificate is highlighted to be used in this context.

Then click on the “**Export**” button. The aim of this step aims at exporting and copying your personal certificate’s public key in order to import it afterwards in the Microsoft Outlook Express mail tool and in your Address book. Without this procedure, Outlook Express cannot be used for sending and receiving encrypted and digitally signed e-mails to/from the other mail recipients.



Certificate Export Wizard

Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

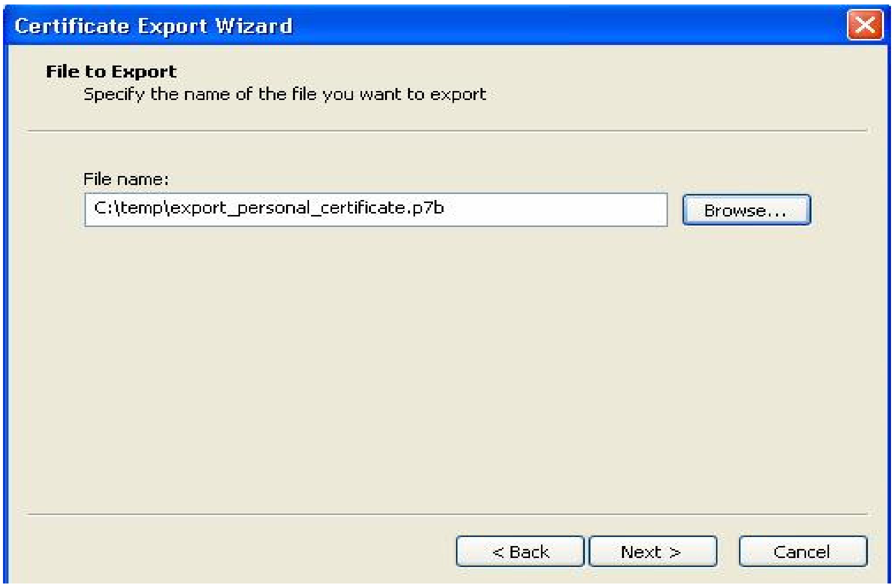
To continue, click Next.

INSTRUCTIONS FOR INSTALLING YOUR PERSONAL CERTIFICATES, *CONTINUED*

Installation instructions, *continued*

Click “**Next**” to continue

4) Then, you have to specify the name of the file you want to export as well as its location on your local hard drive. By default, it can be stored in the C:\temp directory but it is not mandatory, it is up to you. In this example, the file is named: *export_personal_certificate.p7b*



Certificate Export Wizard

File to Export
Specify the name of the file you want to export

File name: C:\temp\export_personal_certificate.p7b

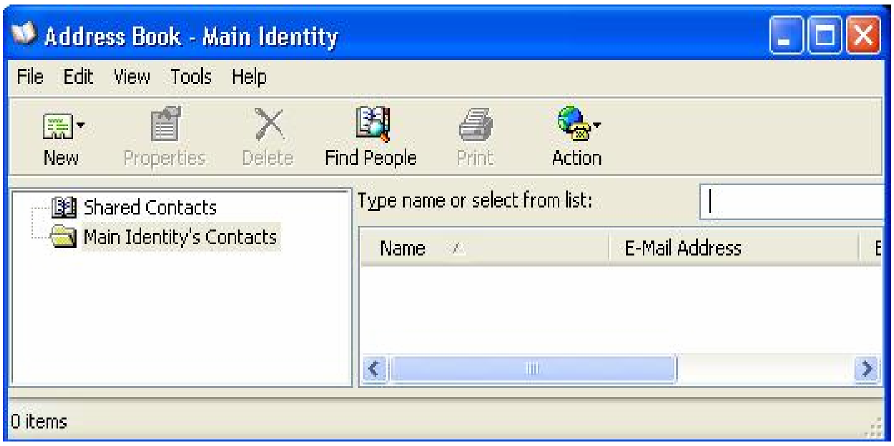
Click “**Next**” to continue and this will terminate the exportation process. From now on, a copy of the personal certificate is stored in the C:\temp directory and can be imported in the Microsoft Outlook Express tool.

4.4 INSTRUCTIONS FOR CONFIGURING OUTLOOK EXPRESS TOOL

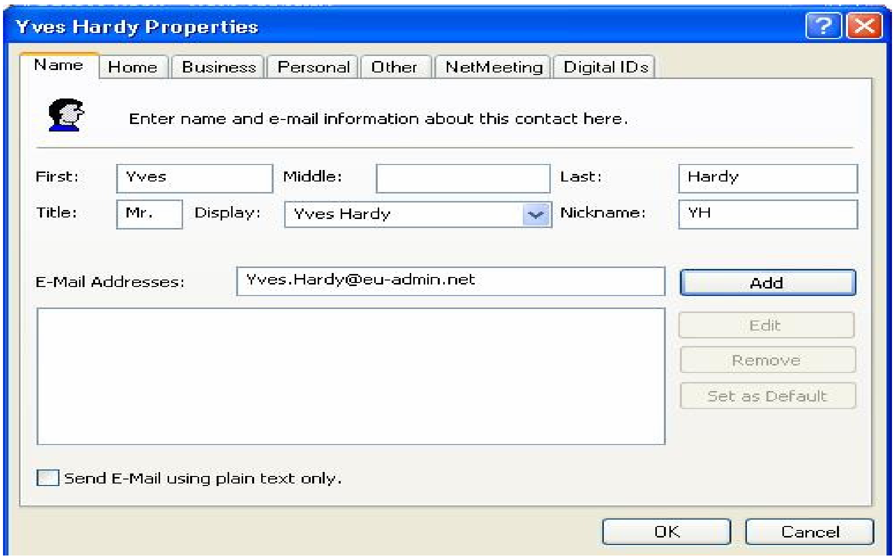
Procedure

The last stage is to import the copied personal certificate in the Outlook Express mail setting and Address book which will allow you to sign and encrypt mail messages over the TESTA network.

a. Open your Microsoft Outlook Express and click on the button called: "**Addresses**" in the main window. The following window should pop up



b. Click on the button "**New**" and you select "**New contact**" to create and register your local e-mail address in Outlook Express. By this step, we will associate your e-mail address with your personal certificate



Enter name and e-mail information about this contact here.

First: Yves Middle: Last: Hardy

Title: Mr. Display: Yves Hardy Nickname: YH

E-Mail Addresses: Yves.Hardy@eu-admin.net

□ Send E-Mail using plain text only.

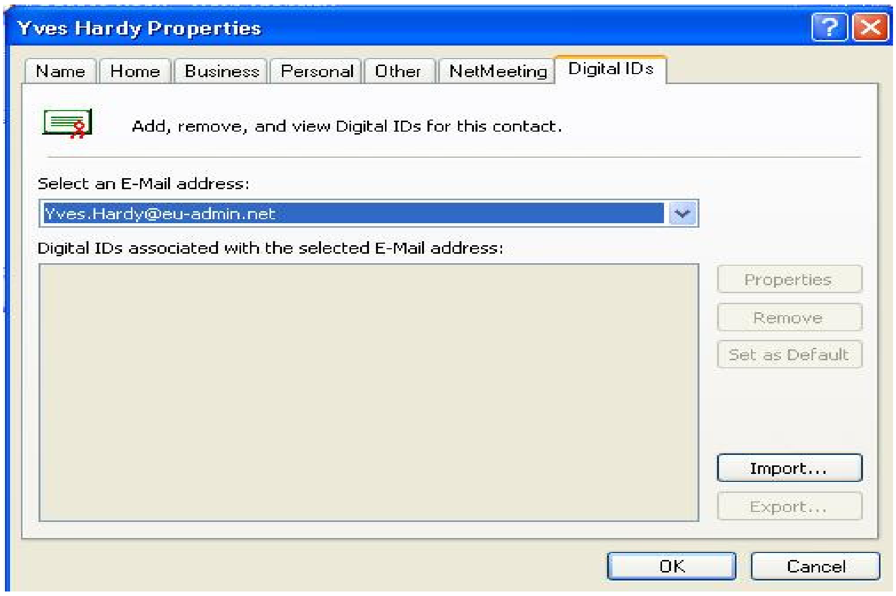
Fill in the form by typing in your first name, last name, title and most importantly the correct syntax of your e-mail address to be used On TESTA: (i.e. firstname.surname@tcn.<country_code>.eu-admin.net)

INSTRUCTIONS FOR CONFIGURING OUTLOOK EXPRESS TOOL, *CONTINUED*

Procedure, *continued*

When done, you just click on the "**Add**" button for the creation

c. Still in the same window, you select the menu called: "**Digital IDs**" and the following window appears on screen:



Yves Hardy Properties

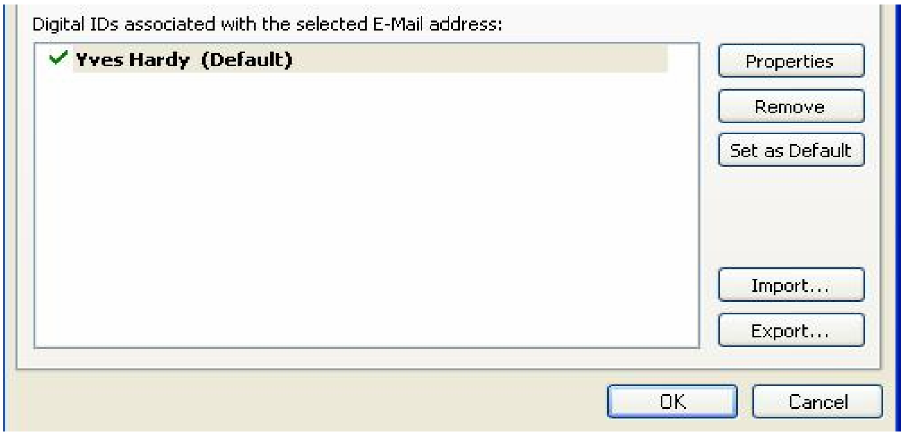
Add, remove, and view Digital IDs for this contact.

Select an E-Mail address: Yves.Hardy@eu-admin.net

Digital IDs associated with the selected E-Mail address:

It is worth noting that your e-mail address must be displayed in the selection field criterion. If not, please select it before continuing the installation process.

d. Click on the "**Import**" button. The objective is to import your exported personal certificate performed in the previous section in order associate this latter with your local e-mail address. Once imported you should get this result:



Digital IDs associated with the selected E-Mail address:

✓ Yves Hardy (Default)

Procedure, *continued*

You can easily verify whether your personal certificate has been imported and associated correctly to your local e-mail address by looking at the "**V**" sign preceding your name as shown here above. If you get a "**X**" sign in red, then something wrong occurred in the importation process preventing the personal certificate to be deployed and used correctly. If this happens, it would be advisable to restart the whole installation procedure from the beginning.

e. Last but not least, the final step is to install in Microsoft Outlook Express so that encrypted and/or signed e-mails can be sent to the other recipients;

1. Open Microsoft Outlook Express
2. Click on **Tools -> Options** from the menu
3. Click on the "**Digital IDs…**" button in the middle
4. Select your personal certificate and click "**Close**"
5. Click "**OK**" to finish

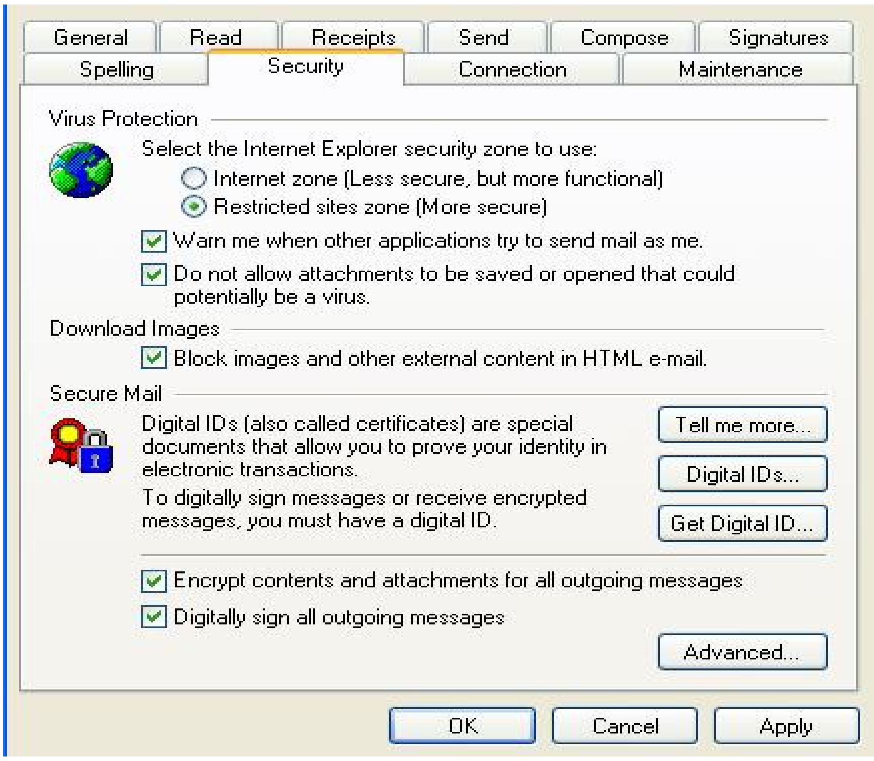
Your Outlook Express mail tool is now configured to send digitally signed and encrypted e-mail messages over the TESTA network

5. SENDING AND RECEIVING SECURE E-MAIL THROUGH OUTLOOK

Basic Principle

Once your user's personal certificate (Digital ID) is stored in your contacts list and associated to your e-mail address, you can send secure e-mail by signing and encrypting messages to other recipients. To enable this mode of transmission, firstly you have to reconfigure the Outlook Express settings as follows:

1. Open Microsoft Outlook Express and in the menu **Tools -> Options**, select **Security.** You should get the following output:



Virus Protection

Select the Internet Explorer security zone to use:

○ Internet zone (Less secure, but more functional)

● Restricted sites zone (More secure)

☑ Warn me when other applications try to send mail as me.

☑ Do not allow attachments to be saved or opened that could potentially be a virus.

Download Images

☑ Block images and other external content in HTML e-mail.

Secure Mail

Digital IDs (also called certificates) are special documents that allow you to prove your identity in electronic transactions.

To digitally sign messages or receive encrypted messages, you must have a digital ID.

☑ Encrypt contents and attachments for all outgoing messages

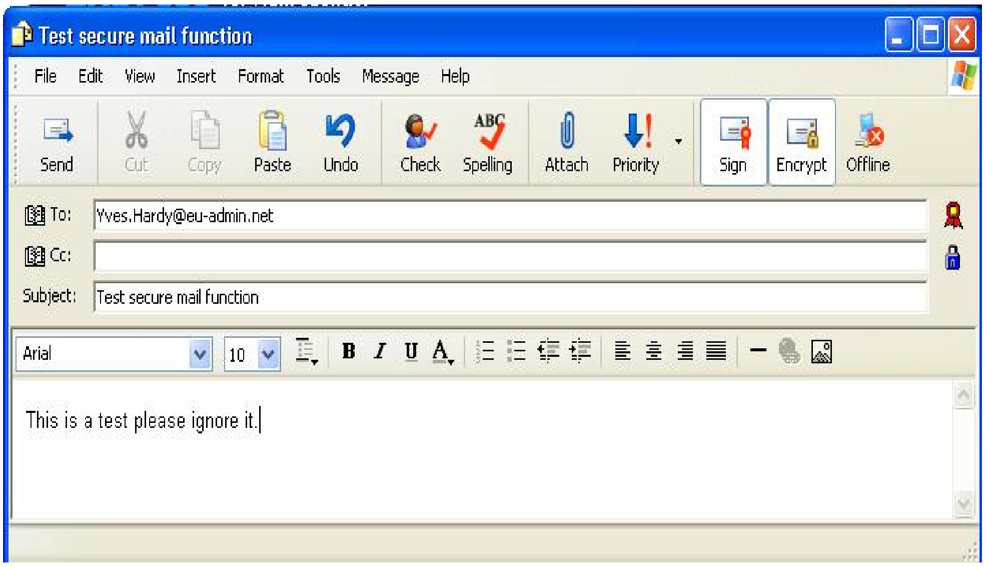
☑ Digitally sign all outgoing messages

2. There, you have to click on "**Encrypt contents and attachments for all outgoing messages**" and "**Digitally sign all outgoing messages**" as shown above and then once done, you click on "**Apply**" to submit and register the changes and then "**OK**". Please note that this change needs to be done only once.

3. Now you are ready to send sign and encrypted email. In Outlook, open a new mail message by clicking the "**New Mail**" button (or "**Create Mail**"). A similar window should appear on screen:

SENDING AND RECEIVING SECURE E-MAIL THROUGH OUTLOOK, *CONTINUED*

Basic Principle, *continued*



To: Yves.Hardy@eu-admin.net

Cc:

Subject: Test secure mail function

This is a test please ignore it.

On top of the window, in the toolbar, you have the liberty to enable/disable the “Sign” and “Encrypt” modules by simply clicking on the corresponding buttons. By default, both buttons are pressed down and the Signed and Encrypted icons should appear at the far right of the address fields, this means in other words that your message will be digitally signed and fully encrypted prior to be sent remotely

In this context, your secure e-mail will be sent and only the recipient will be able to read it and will have the assurance that you only sent it.

Note:

You will not be able to encrypt the message unless the e-mail address you type into the “To field” has a Digital ID associated with it and you have stored a copy of the public key in your local mail Address Book

5.1 ESTABLISH A SECURE LINK WITH ANOTHER MAILBOX USING OUTLOOK EXPRESS ON TESTA NETWORK

Procedure

To establish a secure link with another mailbox allowing you to send encrypted e-mails over the network and in addition to ensure that the recipient will be able to decrypt the contents to read it, as explained in section 1 above, you have to follow the instructions hereafter.

It is worth noting that this procedure is only required once, there is no need to repeat it whenever you intend to send an encrypted e-mail.

- First, you compose a new message to send to your list of recipients asking them to reply to your e-mail in which they will sign their e-mail with their corresponding personal certificate.
- Click the **Digitally Sign** Icon button prior to sending your message.
- Upon receiving your e-mails, the recipients will get a copy of your personal public key which is attached in your message, then they will have to add your e-mail address in their contacts address book in such a way that they will be willing to send you encrypted messages thanks to the use of your public key
- When you receive their individual response, you have to proceed the same way, you just have to add their e-mail address in your local contacts address book. By proceeding as such, you will store a copy of their personal public key locally allowing you to encrypt your upcoming messages with they keys. The secure link is now established end-to-end

In Outlook Express this can be translated as follows: when receivig a signed message from someone for the first time, to store its Digital ID in your address book you:

1. open the signed message from Outlook Express
2. Select **Properties** from the **File** menu
3. Click on **Security** tab
4. Click the **Display certificates**
5. Click the **Add Digital ID to Address Book** button
6. Click **OK**

Furthermore, this Security dialog also shows the ability of the sender's Digital ID and the encryption, if applicable

5.2 MANAGING THE DIGITAL IDS IN YOUR ADDRESS BOOK

Principle

To view one of your contacts' Digital IDs (personal certificates) you have to:

a) Open the address entry for the person whose Digital ID you want to view

b) Click the **Digital IDs** tab in the **Properties** dialog

c) Select Digital ID that you want to view

d) Click the **Properties** button

To delete a Digital ID from the Address Book:

a) Click the **Digital IDs** tab in the **Properties** dialog
b) Select the Digital ID that you want to remove
c) Click the **Remove** button

When deleting the default Digital ID for a contact, you will no longer be able to send encrypted e-mail to that person

6. ANNEX A

List of country code

The following table lists the country codes of the Member States involved in TACHOnet. The complete list is available at:

http://www.unece.org/trans/conventn/disting-signs-5-2001.pdf .

Country Name	Country Code
AUSTRIA	A
BELGIUM	B
DENMARK	DK
FINLAND	FIN
FRANCE	F
GERMANY (Deutschland)	D
GREECE	GR
ICELAND	IS
IRELAND	IRL
ITALY	I
LIECHTENSTEIN (Fürstentum Liechtenstein)	FL
LUXEMBOURG	L
NETHERLANDS	NL
NORWAY	N
PORTUGAL	P
SPAIN (España)	E
SWEDEN	S
UNITED KINGDOM (Great Britain)	GB
SWITZERLAND (Confederation of Helvetia)	CH
CYPRUS	CY
CZECH REPUBLIC	CZ
ESTONIA	EST
HUNGARY	H
LATVIA	LV
LITHUANIA	LT
MALTA	M
POLAND	PL
SLOVAK REPUBLIK	SK
SLOVENIA	SLO