SIEMENS

Email-Encryption with business partners

Date:	02. November 2006
Document type:	User description
Version:	1.2
Author:	Volker Gebhard, Redaktionsteam WG PKI

Corporate Information Office

cio.siemens.com

Table of contents:

1. Intention of this document

This guide focuses on Siemens employees and their external business partners. It describes the premises and the configurations (Outlook and Windows), that ensure secure communications (signed and / or encrypted emails), as well as different methods to exchange cryptographic keys and which method is the best fit.

If you have any problems, please contact your helpdesk. You will find an overview of helpdesks at Siemens here:

https://pki.siemens.com/content/view/full/889.

2. Premises at the business partner

2.1 Certificates and standards:

There are different standards for certificates. Microsoft Outlook and many other programs support X.509 (S/MIME); therefore this standard should be used as basis for secure communication. This is the reason why every Siemens Employee has his own X.509 certificate. PGP is also supported, but only as a sideline. PGP certificates must be ordered separately.

If the business partner has their own Trust Center, like Siemens, or uses a public Trust Center, those should be used for applying for certificates. If the business partner needs support in finding a Trust Center, he can be referred to http://www.pki-page.org. There he will find Trust Centers (Certification Authorities) in different countries.

2.2 Siemens specifics:

At Siemens two X.509 implementations exist. They are called "PKI 1" and "PKI 2". The most important differences are:

PKI 1	**PKI 2**
There is only one certificate for a Siemens Employee. This certificate can be used for encryption and authentication. ("Multipurpose"-certificate). PKI 1 does not support certificate revocation lists (CRL's) PKI 1 expires on June, 30th, 2007.	There are two certificates for a Siemens Employee. One certificate is only for encryption, the other is for authentication and digital signature. PKI 2 supports certificate revocation lists (CRL's).

Siemens supports **PGP** as well

PGP certificates are issued on demand. They are not automatically available. At Siemens the software CryptoEx is necessary for the usage of PGP certificates.

2.3 Requirements to the software:

To encrypt with X.509 certificates, the email client of the business partner has to support this standard, as well as honor the certificate field “key-usage”. Outlook 2003 already contains an encryption functionality compatible to the Siemens PKI and can be used without any additional software.

The following instructions describe how Outlook 2003 needs to be configured, so that Siemens employees and their business partners can communicate in a secure way. Therefore it is necessary, that the business partner has its own certificates installed into his email-client.

Hint to PKI 1:
If the Siemens employee has “PKI 1” certificates it is highly recommended that he migrates to “PKI 2”!
Otherwise these Registry entries have to be set on the business partner side, because there is no email-address within the PKI 1 certificate.

[HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Outlook\Security]
"SupressNameChecks"=dword:00000001
"ExternalSMime"=dword:00000001

3. Possibilities to exchange certificates

Depending on the numbers of communication partners there are different suitable possibilities to exchange certificates.

These alternatives can be used:

- In general, the usage of the Siemens External Repository is recommended. In this way a business partner can securely communicate with every Siemens employee by directly accessing the certificates of his communication partners. After installing the access to the Siemens External Repository a separate key-exchange is not necessary. However, the business partner must be able to do LDAP-queries through his firewall. If this is not possible, this method of key-exchange cannot be used. The business partner needs to ask his network-administrator, if LDAP-queries are possible. For Siemens employees it is not possible to integrate a business partner's repository.
- If the usage of the Siemens External Repository is not possible, the certificates of the communication partners must be exchanged manually. This is the only way for Siemens employees to receive certificates from business partners.

4. Instructions for Siemens employees: "Outlook Native" (without CryptoEx)

4.1 Transmission of Siemens certificates to the business partner

This chapter describes how a Siemens employee can make his certificates available for his business partners.

- With the usage of the External Repository or a single key-exchange via the HTTP-Directory service of the European Bridge-CA no further actions are necessary, because the business partner can access all Siemens certificates through these two services.
- If the usage of the External Repository or the single key-exchange via the HTTP-Directory service of the European Bridge-CA is not possible, then simply send your business partner a signed email. Ensure that the following Outlook settings are applied, so that the business partner can extract your certificates from your signed email.
    - Open the Outlook Menu **Tools→Options,** choose the tab **Security** and click on ***Settings*** in the area *"Encrypted email"*.
    - Within the new window *"Change Security Settings"* activate the option *"Send these certificates with signed messages"*.
    - Close all open windows by clicking the ***OK*** button.
    - Afterwards, send a signed email to your business partner. This email now includes all of your certificates that are necessary for a secure communication with Siemens.

4.2 Transmission of the certificates of the business partner to Siemens

4.2.1 European Bridge-CA

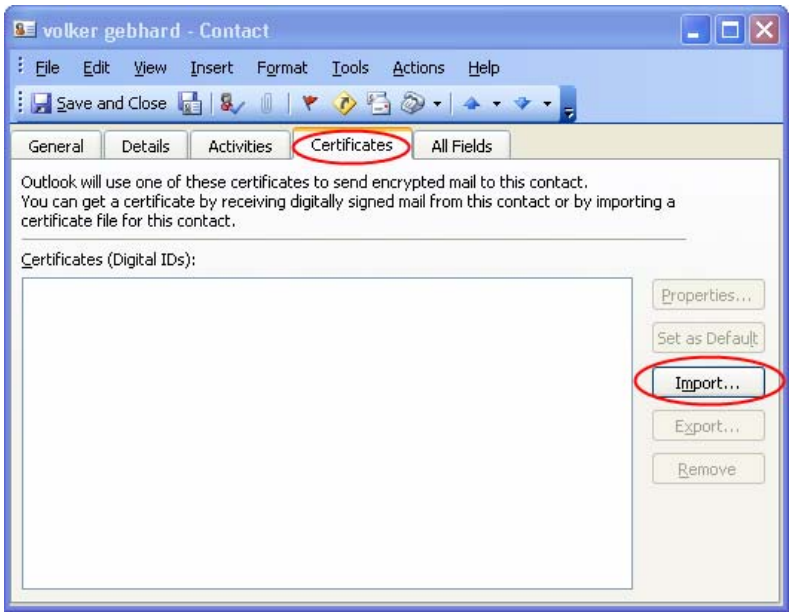
If the business partner's company is a member of the European Bridge-CA, the certificates of the business partner can be downloaded via the HTTP-Directory service of the Bridge-CA. In that case, a separate installation of the respective Root CA certificate is not necessary because they are deployed to all Siemens employees automatically. You will find a list of all members of the European Bridge-CA here[1]

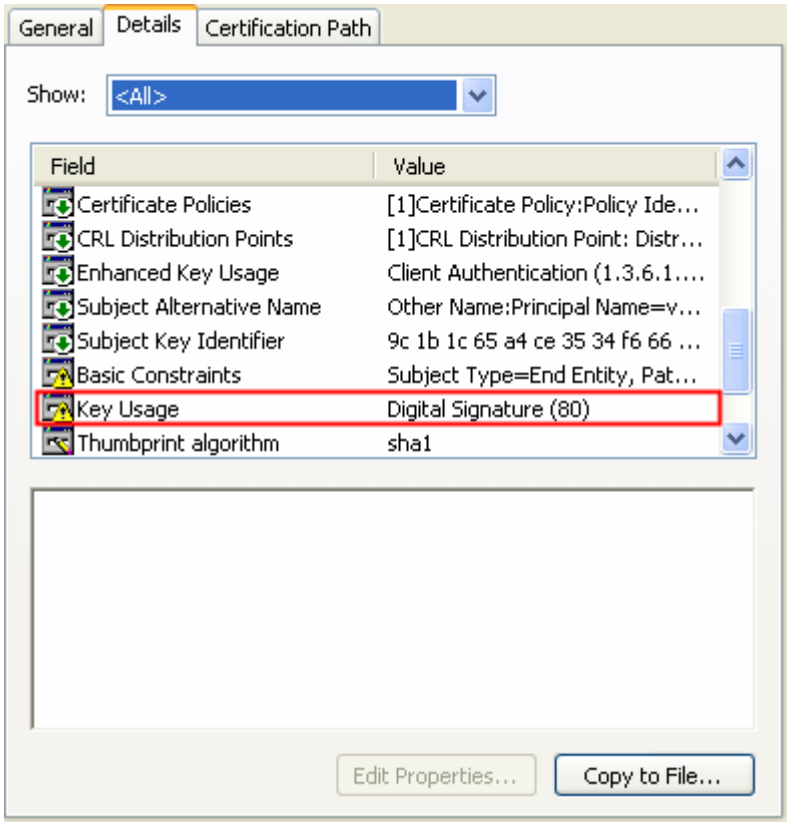
The HTTP-Directory service of the Bridge-CA is available at http://www.bridge-ca.org/eb-ca2/directory. Search for the email address of your business partner and save the provided certificates on your computer. If your business partner owns more than one certificate, it is recommended to save all of them.

[1] http://www.bridge-ca.org/eb-ca2/index.php?option=com_content&task=view&id=20&Itemid=76

To enable Outlook to use the saved certificates, you need to add them to an Outlook contact. Use the following instructions to do so.

- Open the respective contact of the business partner you want to securely communicate with.
- Choose the tab *"Certificates"* and click on ***Import.***
- Choose the directory with the saved certificates and mark them for import.
- Repeat this for all business partners you want to securely communicate with.
- Please note, that for every contact one certificate has to contain *"Key Encipherment, Data Encipherment (30)"* in the field "Key Usage" because Outlook analyses this field and if it is missing or empty Outlook will not send the message encrypted.
- To see field the *"Key Usage"*, choose an imported certificate and click on ***Properties*** and then on the tab *"Details"*.
- Close the "Details" - View with ***OK***.
- Leave the contact via ***Save*** and ***Close.***



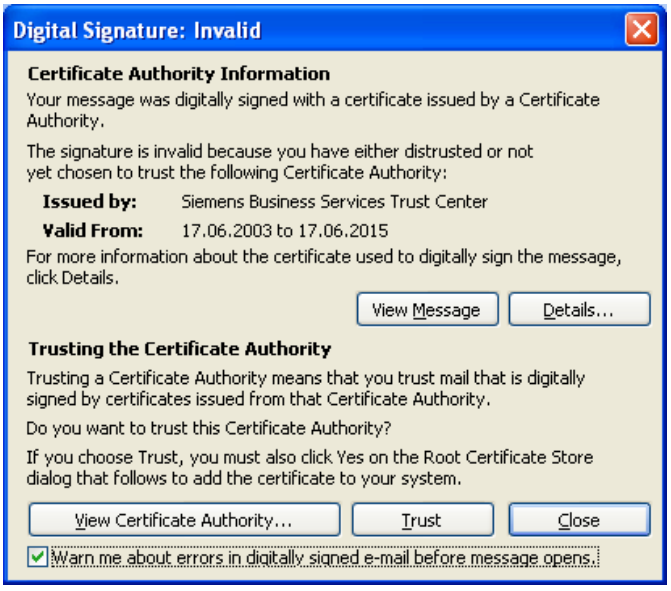


4.2.2 Manual exchange via signed email

If the European Bridge-CA cannot be used, please ask your business partner to send you a digitally signed email. This email must contain his certificates. The necessary settings for business partners are described in chapter 6.1.

After receiving a signed email, perform the following steps:

- After opening a signed email whose Root-CA-Certificates are not yet imported this window will be shown:



- To import the transmitted certificates, click on ***Trust***. A Security Warning that asks you to verify the Fingerprint of the certificate will appear.

- Click on ***Yes***, to copy the certificate into the Windows Certificate Store.
- Right-click onto the sender's email address.
- Choose the menu-option ***Add to Contacts***. Hereupon a new contact with the sender's data opens. Choose the *"certificate"* tab and check if the sender's certificates were imported properly.
- Leave the contact via ***Save*** and ***Close.***
- Repeat this for all business partners you want to securely communicate with.

Note: The signatures of the business partners will only be displayed as valid after opening the email for a second time.

5. Instructions for Siemens employees: CryptoEx

5.1 Transmission of Siemens certificates to the business partner

This chapter describes how a Siemens employee can make his certificates available to his business partners.

- With the usage of the External Repository or a single key-exchange via the HTTP-Directory service of the European Bridge-CA no further actions are necessary, because the business partner can access all Siemens certificates through these two services.
- If the usage of the External Repository for the single key-exchange via the HTTP-Directory service of the European Bridge-CA is not possible, then simply send your business partner a signed email. Ensure that the following CryptoEx settings are applied, so that the business partner can extract your certificates from your signed email.
    - Open the CryptoEx Certificate Manager via the Outlook Menu **Tools→CryptoEx Certificate Manager**.
    - Then open **Options→Advanced Settings** and click on the tag *"Default keys"*.
    - Choose your Default key. (Note: PKI 2 Users find their keys in the Store *SmartCard*, the correct key will be automatically displayed.)
    - Close all open windows in CryptoEx.
- Afterwards, send a signed email to your business partner. This email now includes all of your certificates that are necessary for a secure communication with Siemens.

5.2 Transmission of the business partner certificates to Siemens

5.2.1 European Bridge-CA

If the business partner's company is a member of the European Bridge-CA, the certificates of the business partner can be downloaded via the HTTP-Directory service of the Bridge-CA. A separate installation of the respective Root CA certificate is not necessary in this case, because the Root CA certificates are deployed to all Siemens employees automatically. You will find a list of all members of the European Bridge-CA here[2]

The HTTP-Directory service of the Bridge-CA is available at http://www.bridge-ca.org/eb-ca2/directory. Search for the email-address of your business partner and save the provided certificates on your computer. If your business partner owns more than one certificate, it is recommended to save all of them.

[2] http://www.bridge-ca.org/eb-ca2/index.php?option=com_content&task=view&id=20&Itemid=76

Import of the downloaded certificates into the CryptoEx Default Store

The downloaded certificates need to be imported into the CryptoEx Default Store. For this purpose open the CryptoEx Certificate Manager via the Outlook Menu **Tools→CryptoEx Certificate Manager**.

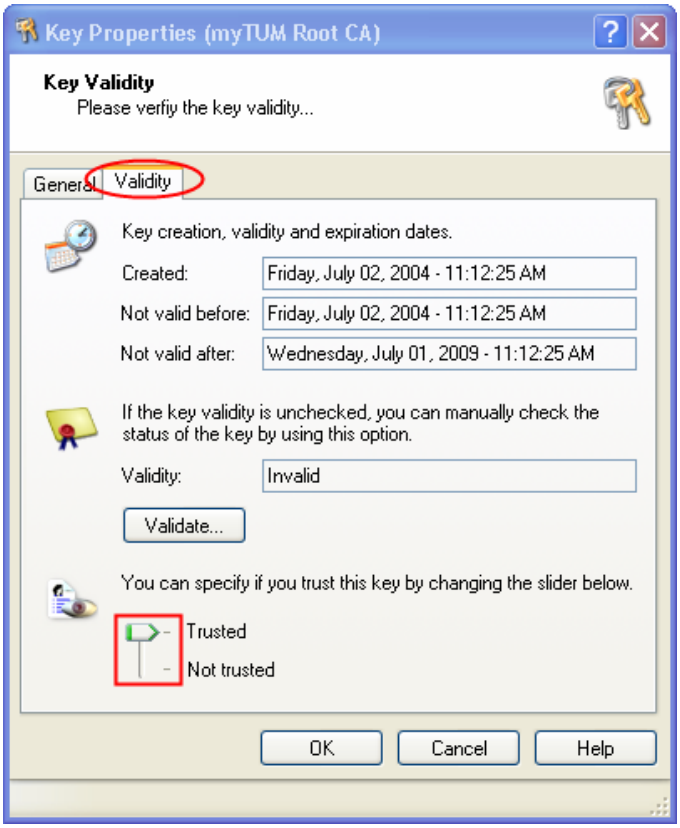
You can import the certificates via **File→ Import key** or via **Drag & Drop** from the Explorer into the *„Default Store"*.

5.2.2 Manual exchange via signed email

If the European Bridge-CA cannot be used, please ask your business partner to send you a digitally signed email. This email must contain his certificates. The necessary settings for business partners are described in chapter 6.1.

After receiving a signed email follow these instructions:

- Open the email. A window *"Security information"* will be shown. Check the option *"Import embedded keys"*. Then click on ***Open.*** The certificates of your business partner will be imported into your CryptoEx Default Store.
- If you want to communicate with more business partners of this company, repeat this step for each one.
- Now you have to trust the Root-CA-Certificate of your business partner. Therefore open the CryptoEx Certificate Store via your Outlook Menu **Tools→CryptoEx Certificate Manager**.
- Double click the "Default Store" and open the Root-CA-Certificate of your business partner with another double-click. (You find the name of the Root-CA-Certificate in the business partner's certificate in the field "*Issuer and serial number*".)
- Now select the tab "Validity" and mark the certificate as "*Trusted*". If this is not possible, your business partner likely has some more Root-CA-Certificates. In this case the respective superior Root-CA-Certificate must be selected as "*Trusted*" You'll find this superior Root-CA-Certificate name in the field "*Issuer and serial number*" in the Root-CA-Certificate you've tried now.



6. Instructions for business partners: „Outlook Native Encryption“

6.1 Transmission of certificates to the Siemens partner

This chapter describes how a business partner can make his certificates available for his Siemens partner.

With the usage of the HTTP-directory service of the European Bridge-CA, no further actions are necessary, because in that case the Siemens employee can access the business partner’s certificates via this service. The instructions for the HTTP-Directory Service of the European Bridge-CA can be found in chapter 6.2.1.

- If the usage of the External Repository or the single certificate exchange via the HTTP-directory service of the European Bridge-CA is not possible, please send your Siemens partner a signed email. In this case the Siemens employee can get your certificates out of your signed email. Please make the following settings in your Outlook configuration:
  - Open the Outlook Menu **Tools→Options,** choose the tab “Security” and click on ***Settings*** in the area “Encrypted email”.
  - Within the new window “Change Security Settings” activate the option “Send these certificates with signed messages”.
  - Close all open windows by clicking the ***OK*** button.
  - Afterwards send a signed email to your Siemens partner. This email now, holds all your certificates that are necessary for a secure communication.

6.2 Transmission of Siemens certificates to the business partners

6.2.1 Using the Siemens External Repository or the HTTP-Directory service of the European Bridge-CA

6.2.1.1 Installation of the Siemens Root-CA Certificates

If the Siemens External Repository is used, the Siemens Root-CA-Certificates must be imported. This is also necessary if the HTTP-Directory Service of the European Bridge-CA is used and if the business partner is not a member of the European Bridge-CA. Root-CA Certificates of the members will be automatically deployed.

If you exchange certificates via signed emails, please follow the instructions in chapter 6.2.2.

Follow these instructions to import the Siemens Root-CA certificates:

- The Siemens Root-CA Certificates can be downloaded here: https://www.siemens.com/pki. We recommend to download all Siemens Root-CA

Certificates (collected here: "hierarchy of the Siemens CA certificate"[3]) and to save them to your hard drive. This file contains all necessary certificates.

- To import the certificates into the Windows Certificate Store, choose one of the following possibilities:

■ Open the Menu **Tools→Internet Options→Content→ Certificate.** ■ Click on ***Import.*** ■ Choose the saved file containing the Siemens Root-CA Certificates (select the type of file p7b) ■ Close the open Windows via ***Close*** or ***OK.***	■ Click with your right mouse-button the downloaded p7b-file. ■ Choose ***Install Certificate.*** Click on ***Next.*** ■ Make sure the option "choose Certificate Store automatically" is set. ■ Click on ***Finish***.

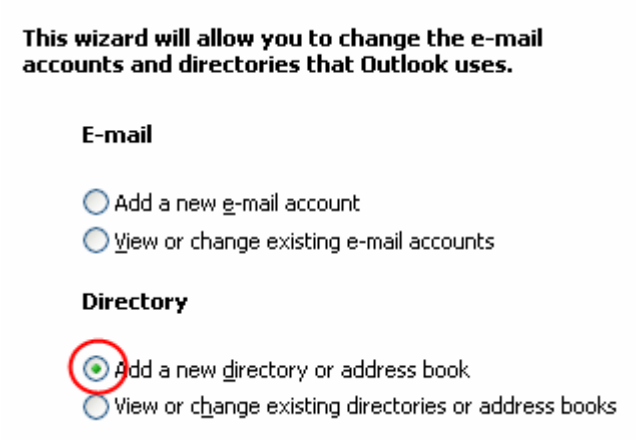
6.2.1.2 Integration of the Siemens External Repository

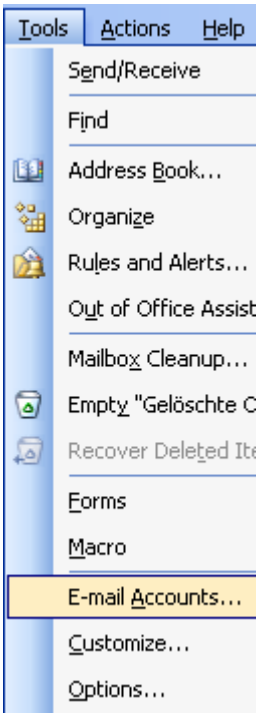
The usage of the Siemens External Repository is generally recommended. It is possible to then access all certificates of the Siemens employees from the Internet.

Once the External Repository is installed, no further key exchanges are necessary. Make sure that the integration of the Repository is not blocked by your Firewall policies (see chapter 3.).

Follow these instructions for the integration:

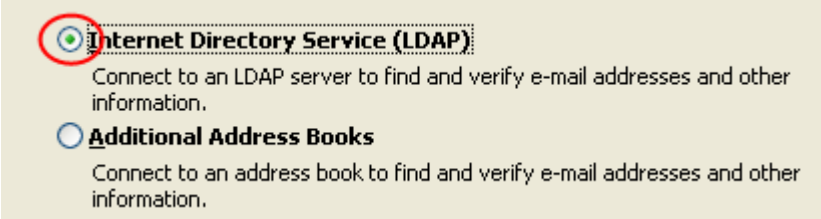
- Open the Outlook menu **Tools → email Accounts**.
- Choose the Radio-Button *"Add a new directory or address book"*



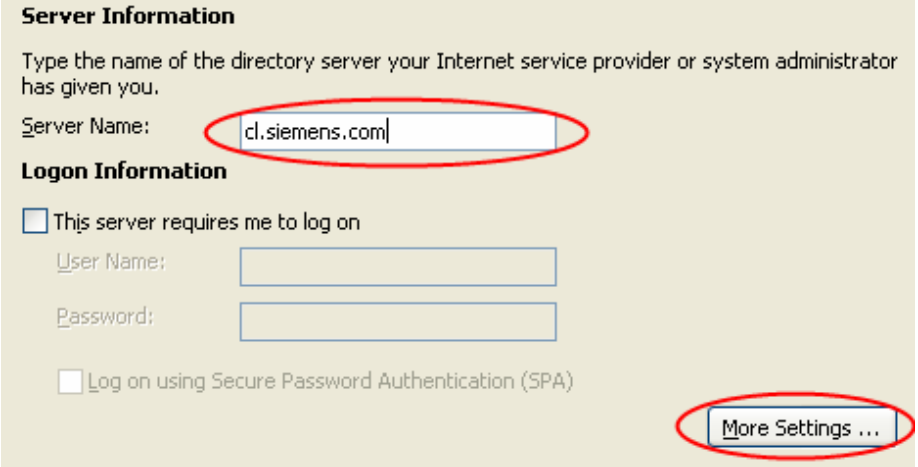


[3] http://www.siemens.com/Daten/siecom/HQ/eB/Internet/CoEE_Unitwide/WORKAREA/pki_ed/templatedata/Deutsch/file/binary/Siemens_CA_Certificates_1378885.p7b

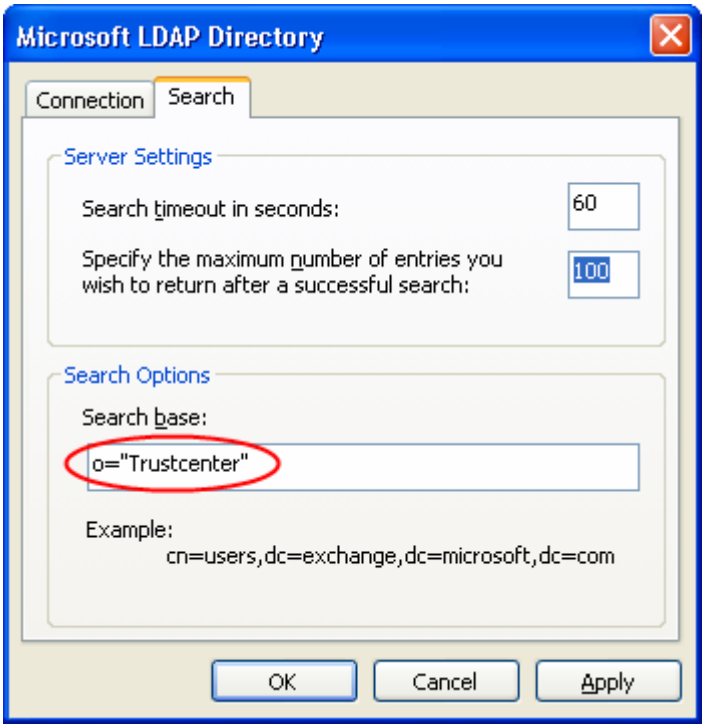
- Choose "*Internet Directory Service (LDAP)*".



- The Servername is: "*cl.siemens.com*". Click on ***More Settings***.



- Change to the tab "*Search*" and enter the Search base: "o=Trustcenter".
- Continue with ***OK***.
- Click in the previous Window ***Finish***.
- Note: It is necessary to restart Outlook to use the directory service.

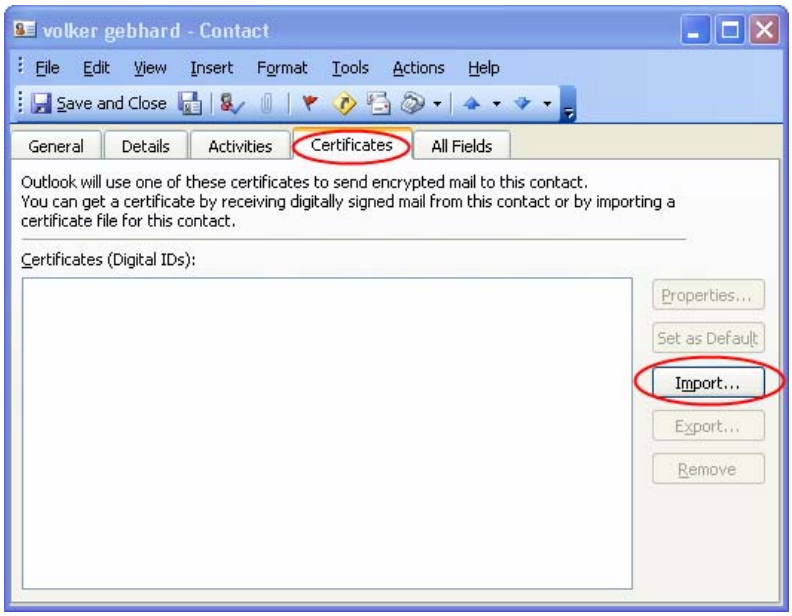


6.2.1.3 European Bridge-CA

Siemens is member of the European Bridge-CA. That is why you can get all certificates of all Siemens employees via the HTTP-Directory Service of the European Bridge-CA. This HTTP-Directory Service can be found here: http://www.bridge-ca.org/eb-ca2/directory/. To find a certificate, just enter the email address of the employee and save **all** offered certificates to your hard drive.

In order for Outlook to use these downloaded certificates, you need to add them to an Outlook contact. Follow these instructions to add a certificate to a contact:

- Open your Outlook contacts and the contact of the Siemens employee you want to communicate securely.
- Choose the tab "Certificates" and click on ***Import.***
- Choose the directory in which you saved the downloaded certificates and mark them for the import.
- Leave the contact via ***Save*** and ***Close.***
- Redo this for all Siemens employees you want to securely communicate with.



6.2.2 Manual exchange via signed email

If you cannot use the European Bridge-CA, please ask your communication partner at Siemens to send you a signed email. The necessary settings for the Siemens employee can be found in chapter 4.1 (Outlook native) or chapter 5.1 (CryptoEx).

Follow these instructions if you have received a signed email:

- This window opens if you receive a signed email, whose Root-CA Certificate was not yet imported.
- To import the CA-Certificates that come with the signed email, click on ***Trust*** afterwards a "Security Warning" appears, that asks you to verify the fingerprint of the certificate.

- Click on ***YES*** to import this certificate into your Windows Certificate Store.
- Click with your right mouse-button on the Sender's email address.
- Choose the menu option ***Add to Contacts***. Hereupon the contact window with the user's details opens. Open the "certificate" tab and check if the certificates were imported.
- Leave the contact via ***Save*** and ***Close.***
- Repeat this for all the business partners you want to securely communicate with.

Note: The signatures of the business partners will only be displayed as valid, after opening the email again.