# E-mail encryption with business partners

## (Guideline for business partners)

| | |
|---|---|
| Date: | 2013-07-15 |
| Document type: | user description |
| Version: | 3.2 |
| Author: | Editorial team PKI |

# Table of contents

# 1. Intention of the document:

This guideline is written for Siemens business partners who need to communicate with their partners at Siemens via encrypted emails. It describes the system requirements and the necessary configurations (Outlook and Windows) to enable a secure communication (signed and/or encrypted emails). It shows especially the possibilities for key exchange.

Please contact your Siemens partner if you have any problems.

# 2. Prerequisites on business partner side

## 2.1 Certificates:

The business partner needs certificates to send encrypted e-mails.

There are different standards for certificates. X.509(S/MIME) is supported by Microsoft Outlook and many other programs, therefore this standard should be used for secure communication. Because of this reason all Siemens employees are equipped with their own X.509 certificates. PGP is only supported as a sideline and is available for Siemens employees only on demand.

If your organization has its own trust center or your company is using a public trust center it should be used to obtain certificates. A few known public trust centers which are already listed in the Siemens IT infrastructure are:

- Verisign (http://www.verisign.com/)
- TC Trust Center (http://www.trustcenter.de/en/index.htm),
- Telesec (http://www.telesec.de/)

## 2.2 Prerequisites for Software:

To encrypt with X.509 certificates your e-mail program has to support this standard. Also it has to evaluate the “key usage” field in the certificate. Outlook (since version 2003) already contains an encryption functionality which is compatible to the Siemens PKI and can be used without any further installation.

The following user guideline describes which steps have to be taken before a business partner and a Siemens employee can exchange encrypted and signed emails on the example of Outlook 2003. Therefore it is necessary that the business partner has installed his certificates in his e-mail program.

# 3. Possibilities for certificate exchange

Depending on the number of communication partners, different possibilities for certificate exchange are useful.

These alternatives can be applied:

- Basically the usage of the Siemens external repository is recommended. This is a directory service for PKI keys in the Internet. It enables secure communication with every Siemens employee. This repository contains the latest certificates of Siemens employees. After setting up of the repository, no separate key exchange is needed any more. But it must be possible to send LDAP request over the internet. Otherwise this option is not possible. Please contact your network administrator in case of problems with LDAP-requests.

- If the usage of the Siemens external repository is not possible or the business partner does not have a repository on the Internet, certificates must exchanged manually.

# 4. Guideline for business partners: „Outlook Native encryption“

## 4.1 Transfer of own certificates to the Siemens partner

This paragraph describes how a business partner can transfer his own certificates to a Siemens employee.
Check out if the Siemens employee is able to send you an encrypted e-mail. If this is possible, no other actions have to be taken because a direct access to the directory service of your organization is possible.

If this is not the case, please send a signed e-mail to your Siemens partner. Please check the following settings so that he can access your certificates from your e-mail:

- Open Outlook and the menu Tools → Options, in the tab security click below *“encrypted emails”* on *“Settings...”*
  (Since Outlook 2007: Tools → Trust Center in the Section „*E-mail Security*”)
  Activate in the following window “*Change Security Settings” (Since Outlook 2007: on “Settings...”)* the option “*send these certificates with signed messages”*
- Close all windows with “*OK*”
- Send a signed e-mail to your Siemens partner. In such an e-mail all your certificates which are necessary for a secure communication are added automatically.

## 4.2 Transfer of Siemens certificates to a business partner

### 4.2.1 Usage of the Siemens external repository or http directory service of Siemens or the European Bridge-CA

#### *4.2.1.1 Siemens Root Signing*

Root signing certificates are certificates that you can use to sign other certificates that are linked up to a trusted root certificate. Since Siemens has its own Certification Authority the certificates of a Siemens employee are usually valid at the business partner.

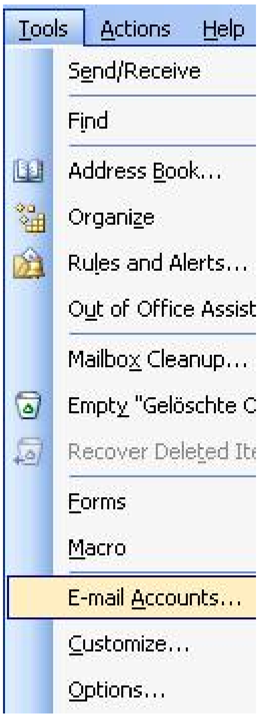
#### *4.2.1.2 Integration of the Siemens External Repository*

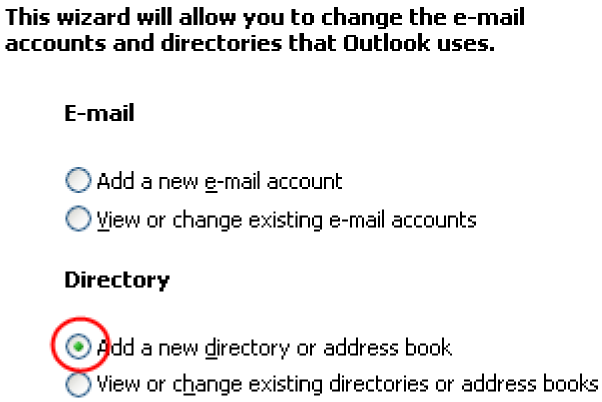
The usage of the Siemens External Repository is generally recommended. It is possible to access all certificates of Siemens employees from the Internet.

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.

Follow these instructions for the integration:

- Open the Outlook menu Tools → E-mail Accounts. (Since Outlook 2007: Tools → Account Settings in the tab “*Address Books*”)
- Choose the Radio-Button *“Add a new directory or address book”* (Since Outlook 2007: On “*New…*”)





**This wizard will allow you to change the e-mail accounts and directories that Outlook uses.**

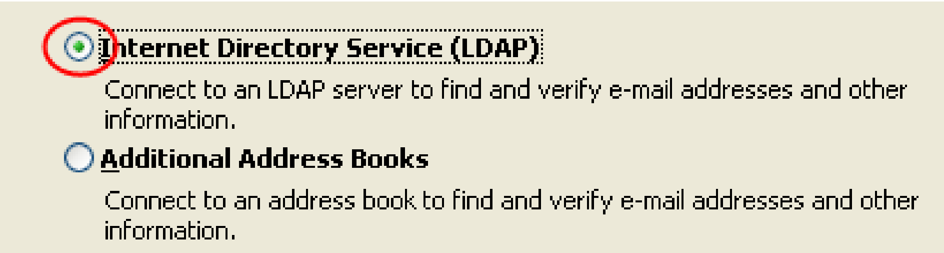
**E-mail**

○ Add a new e-mail account
○ View or change existing e-mail accounts

**Directory**

● Add a new directory or address book
○ View or change existing directories or address books

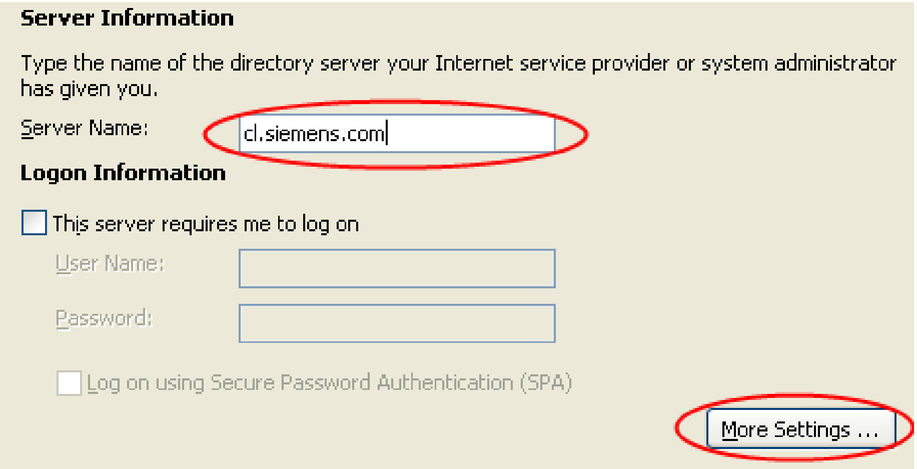
- Choose “*Internet Directory Service (LDAP)”.*



● **Internet Directory Service (LDAP)**
Connect to an LDAP server to find and verify e-mail addresses and other information.

○ **Additional Address Books**
Connect to an address book to find and verify e-mail addresses and other information.

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



**Server Information**

Type the name of the directory server your Internet service provider or system administrator has given you.

Server Name: cl.siemens.com

**Logon Information**

□ This server requires me to log on

User Name:

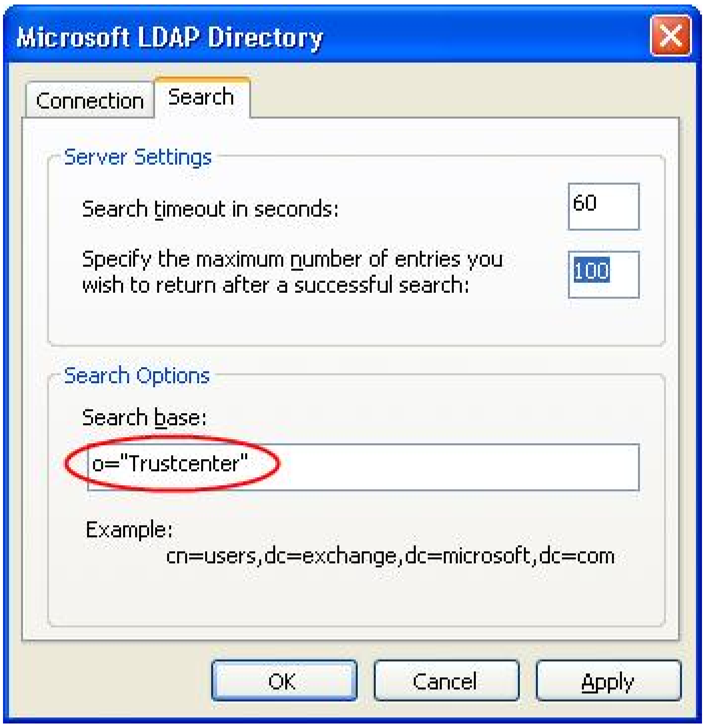
Password:

□ Log on using Secure Password Authentication (SPA)

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.



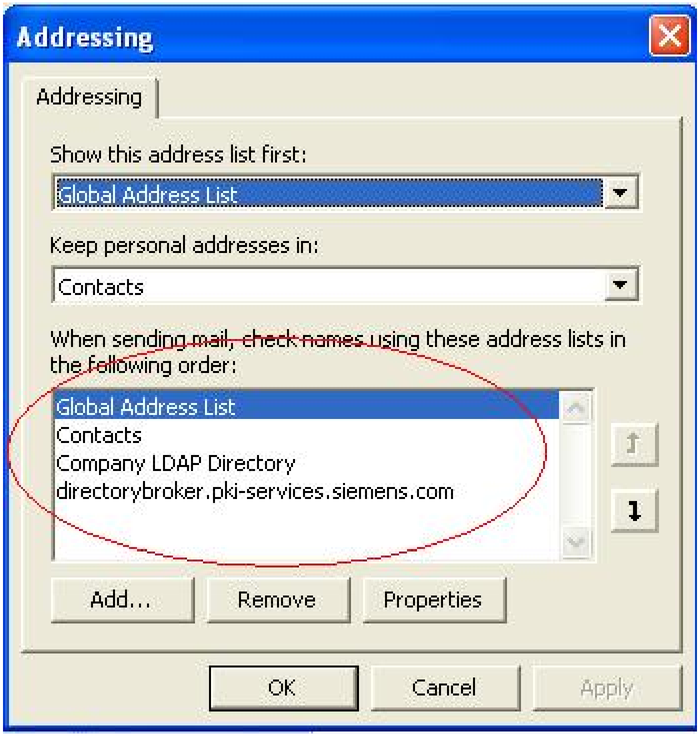
Search timeout in seconds: 60

Specify the maximum number of entries you wish to return after a successful search: 100

Search base: o="Trustcenter"

Example: cn=users,dc=exchange,dc=microsoft,dc=com

- At the end it is necessary that the directory services are in the right order in the address Book. Please open your address book
- Click on “*tools*” and then on “*Options*”
- Make sure that the directories are in the right order.



Show this address list first: Global Address List

Keep personal addresses in: Contacts

When sending mail, check names using these address lists in the following order:

Global Address List
Contacts
Company LDAP Directory
directorybroker.pki-services.siemens.com

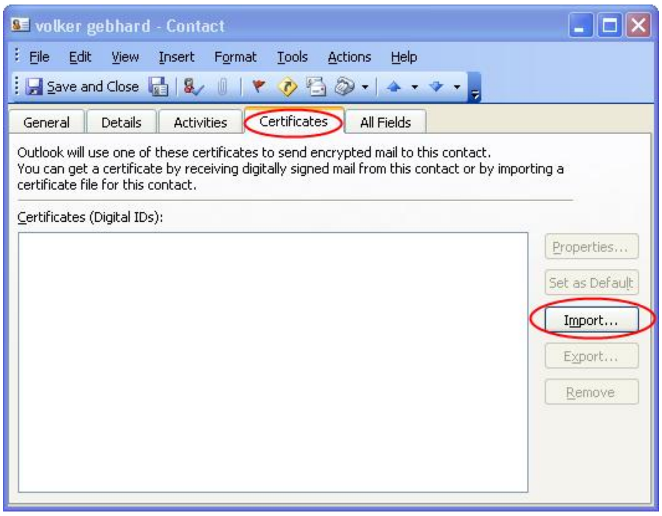
### 4.2.1.3 *HTTP Directory or European Bridge CA*

Siemens is providing a HTTP Directory service where Certificates of all Siemens employees can be downloaded via the following link: http://cl.siemens.com

Above that is Siemens a 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, too. This HTTP-Directory Service can be found here: https://www.ebca.de/en/tools/finding-certificates/

To find a certificate, just enter the email address of the employee and save all offered certificates to your hard drive. If the saved certificates are .crt-Files you must change it into .cer-Files because the other files are not supported.

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:



Outlook will use one of these certificates to send encrypted mail to this contact.
You can get a certificate by receiving digitally signed mail from this contact or by importing a certificate file for this contact.

Certificates (Digital IDs):

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

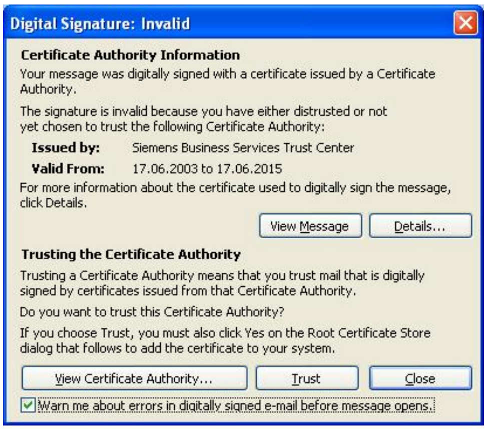
### 4.2.2 Manual certificate exchange via signed e-mail

If you cannot use the European Bridge-CA, please ask your communication partner at Siemens to send you a signed e-mail.

After you have received the signed e-mail you should be able to communicate securely with the Siemens employee. Normally there are no further actions necessary. If there appears a “Digital Signature: Invalid” reference, please follow the instruction below.

Follow these instructions if you have received a signed e-mail with a “Digital Signature: Invalid” reference:

- This window opens if you receive a signed e-mail, whose Root-CA Certificate was not yet imported.



**Certificate Authority Information**

Your message was digitally signed with a certificate issued by a Certificate Authority.

The signature is invalid because you have either distrusted or not yet chosen to trust the following Certificate Authority:

**Issued by:** Siemens Business Services Trust Center

**Valid From:** 17.06.2003 to 17.06.2015

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

**Trusting the Certificate Authority**

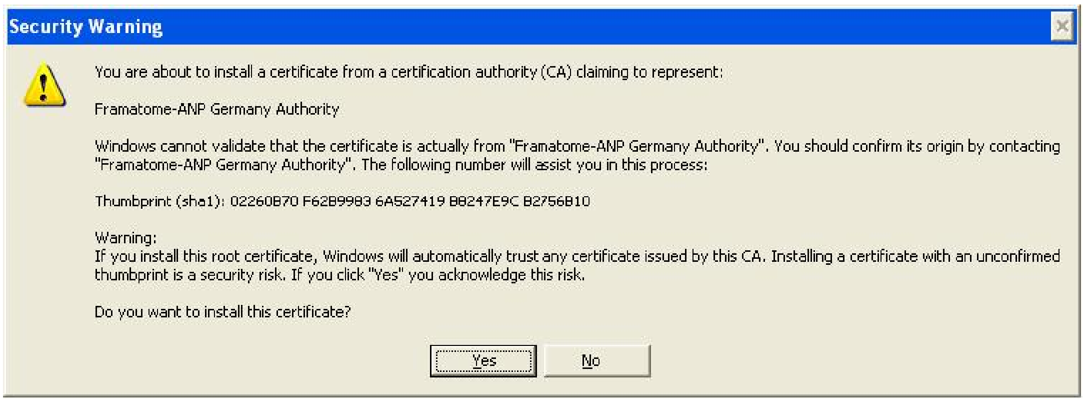
Trusting a Certificate Authority means that you trust mail that is digitally signed by certificates issued from that Certificate Authority.

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.

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

- 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.



Security Warning

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

Framatome-ANP Germany Authority

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

Thumbprint (sha1): 02260B70 F62B9983 6A527419 B8247E9C B2756B10

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?

- 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 communicate with securely.

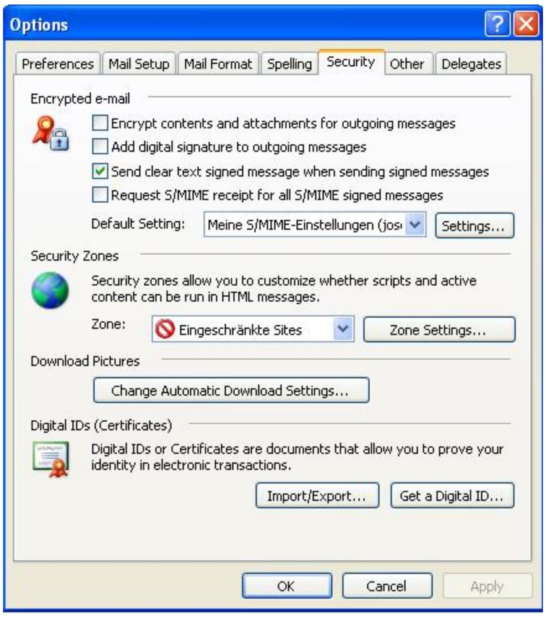
Note: The signatures of the business partners will only be displayed as valid after opening the e-mail again.

# 5. Final settings for first usage in Outlook

To use e-mail encryption now the right certificate and the suitable encryption mode has to be chosen. Please consider that you can ignore this chapter if you have already installed and used e-mail encryption before on your system.

Please follow these steps:

- Start Outlook
- On Tools → Options on the tab „*Security*“ you can find information to send encrypted e-mails. Click on “*Settings*”, located next to “*My S/MIME-Settings*”



Options

Encrypted e-mail

□ Encrypt contents and attachments for outgoing messages

□ Add digital signature to outgoing messages

☑ Send clear text signed message when sending signed messages

□ Request S/MIME receipt for all S/MIME signed messages

Default Setting: Meine S/MIME-Einstellungen (jos

Security Zones

Security zones allow you to customize whether scripts and active content can be run in HTML messages.

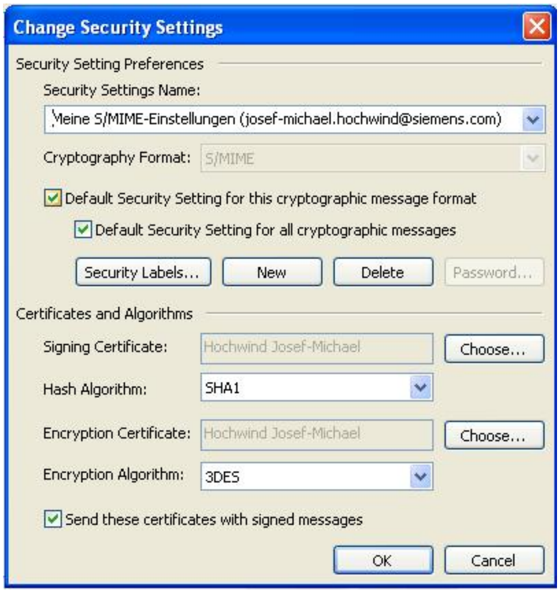
Zone: Eingeschränkte Sites

Download Pictures

Digital IDs (Certificates)

Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions.

- Choose the suggested certificate right next to „Signing Certificate“. Then choose a encryption algorithm. Siemens demands “*3DES*” here. Close everything with „*OK*“.  
If “*3DES*” is not available, it could happen that a weaker encryption method will be used. In this case the e-mail cannot be read by Siemens employees. To solve this problem, please contact your Siemens partner and refer to the corresponding manual for Siemens employees.



Change Security Settings

Security Setting Preferences

Security Settings Name: Meine S/MIME-Einstellungen (josef-michael.hochwind@siemens.com)

Cryptography Format: S/MIME

☑ Default Security Setting for this cryptographic message format

☑ Default Security Setting for all cryptographic messages

Certificates and Algorithms

Signing Certificate: Hochwind Josef-Michael

Hash Algorithm: SHA1

Encryption Certificate: Hochwind Josef-Michael

Encryption Algorithm: 3DES

☑ Send these certificates with signed messages

- Close Outlook and restart it to assume the changes.