Multipurpose Business Partner Certificates
Guideline for the Business Partner

09.09.2015
Guideline for the Business Partner, V1.4
Dagmar Planer

IT creates business value

SIEMENS

Document Status

Document details	
Siemens	Corporate Information Technology
Topic	Multipurpose Business Partner Certificates – Guideline for the Business Partner
Project name	Multipurpose Business Partner Certificates
Document type	Guideline for the Business Partner
Classification	
Bindingness	
Document name / path	mpbp_guideline_businesspartner_en.doc
Original document/ language	Original document / english

Document Management

Change history, version management and revision status (Basic concept, detailed concept, coordination in process, agreed, released, scrapped)				
Date	Edited by	Department	Phone	E-mail
	Version	Status	Comment	
20.8.2009	Dagmar Planer	CIT CA CS 33	+49 89 636 43194	dagmar.planer@siemens.com
	V0.8	draft	Ready for internal approval	
23.08.09	Markus Wichmann	CIT G	636-1343162	markus.wichmann@siemens.com
	V0.9	draft	Rewrite chapter 4-6	
24.8.2009	Dagmar Planer	CIT CA CS 33	+49 89 636 43194	
	V1.0	released	Edit chapter 4-6. Release.	
19.05.2011	Dagmar Planer	CIT CA CS 33	+49 89 636 43194	
	V1.1	released	New: Registration of certificates for authentication (chapter 7). Released after review by Markus Wichmann and Leonardo Morales	
31.10.2011	Dagmar Planer	CIT CA CS 33	+49 89 636 43194	

Change history, version management and revision status (Basic concept, detailed concept, coordination in process, agreed, released, scrapped)				
Date	Edited by	Department	Phone	E-mail
	Version	Status	Comment	
	V1.2	In work	New: Chapter 6 and chapter 8; new chapter 4.1 Baltimore Root Deleted: Chapter 9 Register your Certificate for Use as Authentication Certificate, since registration is no longer necessary.	
07.12.2011	Dagmar Planer	CIT CA CS 33	+49 89 636 43194	dagmar.planer@siemens.com
	V1.2	released	Minor corrections after review with Markus Wichmann	
	Josef Hochwind	CIT ISEC	josef-michael.hochwind@siemens.com	
		In work	Instructions provided for Office 2007 (see chapter 5 and 6	
15.05.2013	Dagmar Planer	CIT CA CS 33	+49 89 636 43194	dagmar.planer@siemens.com
	V1.3		Introducing the Multipurpose Partner Certificates	
09.09.2015	Markus Küchler	GS IT HR 7 4	+49 89 636 43380	markus.kuechler@siemens.com
	V1.4		Added new screenshots of new PKI Solutions Downloadserver	
11.09.2015	Dagmar Planer	GS IT HR 7 4	+49 89 636 43194	dagmar.planer@siemens.com
	V1.4		Released	

Table of Contents

1. Introduction

To ensure secure communication between Siemens employees and business partners business partners can be provided with specific certificates. Also, the business partner can use these certificates for authentication when accessing defined Siemens applications for business partners.

This guideline addresses the business partner for whom certificates are provided for.

It describes how to receive and install your certificate.

What has changed with V1.4 of this guideline?

- A new PKI Download Server release has been provided.

  The handling and the new screenshots are described in chapter “Download Certificates from the PKI-Download-Server”.

What has changed with V1.3 of this guideline?

Multipurpose Business Partner Certificates

The former General Business Partner Certificates have been renamed to Multipurpose Business Partner Certificates.

As the name implies these certificates are no longer restricted to General Business Partners but can now also be issued for all Siemens business partners.

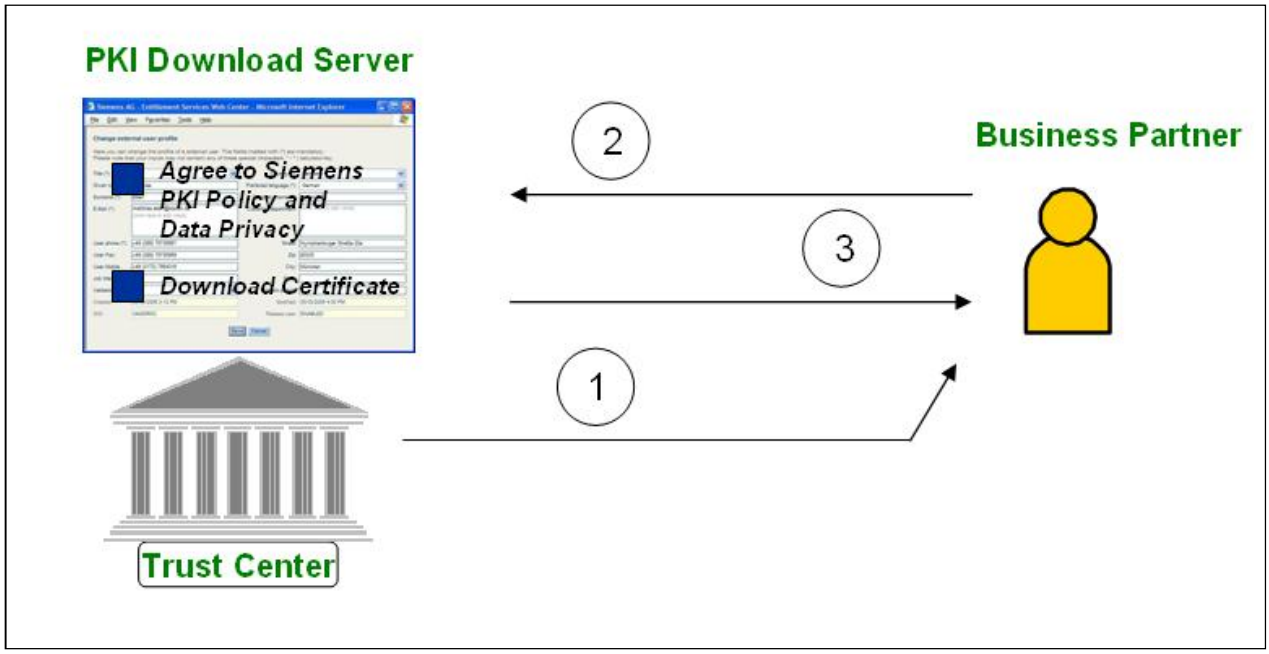
Typically, these business partners do not have a Siemens ID Card with certificates on it.

Office 2007

Chapters 5. and 6 now also provide instructions for Office 2007.

- “Download Certificates from the PKI-Download-Server”.

2. Process Overview



1. The Trust Center sends you an e-mail informing you that a certificate has been created.
   The e-mail also contains the link to the PKI Download Application and the PIN needed for installing the certificate.
2. To access the PKI download application, click on the link in the e-mail and request a temporary password that you have to change when logging in. After login you have to check your data. You have to agree to the Siemens policy and data privacy rules. This information will be stored by the PKI download application.
3. Only after agreeing to the policy and data privacy rules you can download your certificate.

Please note: Your Siemens partner triggers the process to provide you with an certificate. In case of questions or problems always contact your Siemens partner.

3. Download Certificates from the PKI-Download-Server

Your certificate will be made available for download on a specific download server.

This is the case, if

- You receive a certificate for the first time.
- Your current certificate has expired and a new certificate has been issued.
- A previously valid ("old") certificate was again made available (to read your old e-mails).

3.1 Access the Download Application

When a certificate has been issued for you, the Siemens Trust Center sends you an e-mail with the following information:

That a certificate has been issued for you

The link to application to download the certificate (https://pkidownload.siemens.com/)

How to login to the application

The PIN needed to import the certificate

Example:

Please scroll down for the German translation.
Die deutsche Uebersetzung finden Sie im Anschluss an den englischen Text.

---- ENGLISH ----------

Dear Ms./Mr. Stein.

Your Digital Certificate issued to you for encrypted e-mail communication with Siemens is now available for download.

To import the certificate you need the following PIN:

Multipurpose key: 10C53EF5E5942F1B0BD9
(0 in the PIN is always a digit and not the letter O)

You can download the certificate at

https://pkidownload.siemens.com/

In case you do not have a password yet, please go to the above mentioned web site, click on Login and request a password. Your username will be your e-mail address.

Instructions how to import the certificate at the example of MS Outlook will be available for you after login to the download page.

In case of problems, please consult your Siemens partner.

Yours sincerely,
Siemens Trust Center

--- DEUTSCH ----------

Sehr geehrte/r Frau/Herr Stein.

Ihr Digitales Zertifikat, welches Ihnen fuer die verschluesselte E-Mail-Kommunikation mit Ihren Partnern bei Siemens ausgestellt wurde, steht fuer Sie zum Download bereit.

Zum Import des Zertifikats benoetigen Sie die folgende PIN:

Multipurpose key: 10C53EF5E5942F1B0BD9
(0 ist in der PIN immer eine Ziffer und nicht der Buchstabe O)

Sie koennen das Zertifikat unter

https://pkidownload.siemens.com/

herunterladen.

Sollten Sie noch ueber kein Passwort verfuegen, rufen Sie bitte die obige Website auf, klicken Sie dort auf Login und lassen Sie sich ein Passwort zuschicken. Ihr Username ist Ihre E-Mail-Adresse.

Eine Anleitung zum Import des Zertifikats am Beispiel von MS Outlook steht Ihnen nach dem Login auf der Download-Seite zur Verfuegung.

Bei Problemen setzen Sie sich bitte mit Ihrem Siemens-Partner in Verbindung.

Mit freundlichem Gruss,
Ihr Siemens Trust Center

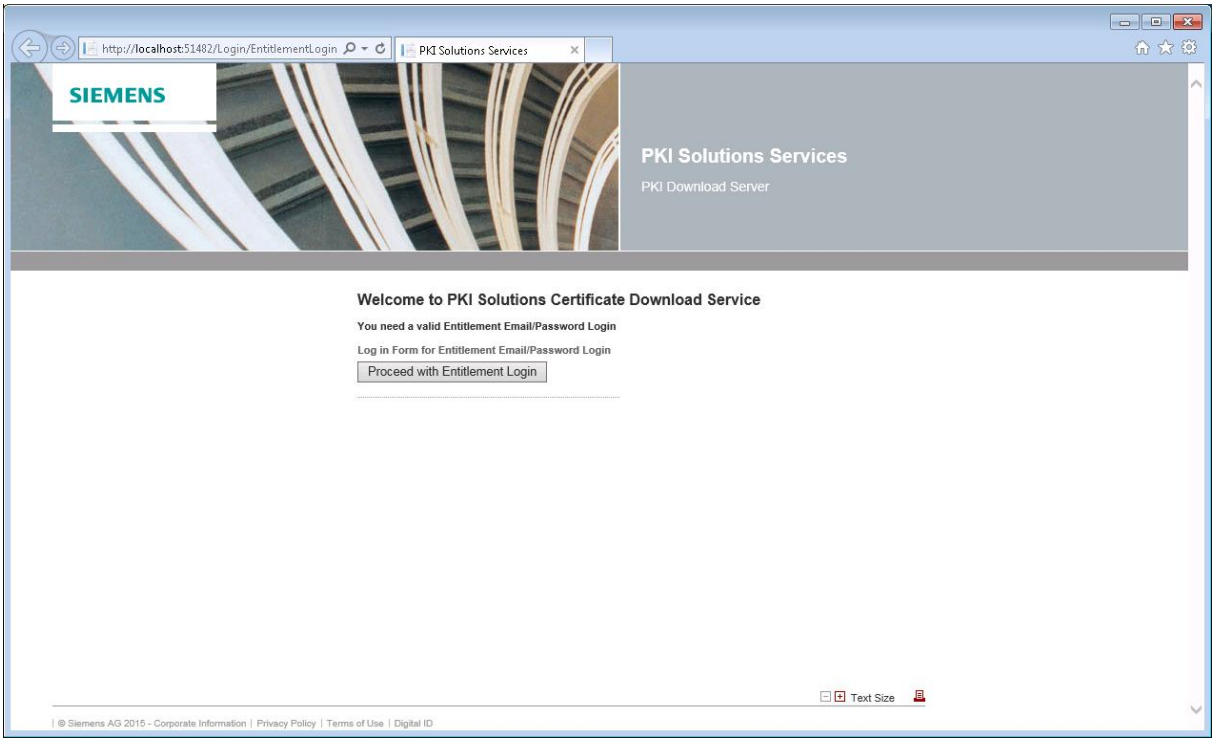
PKI key data (for support requests):

Issued to: Stein Thomas
GID: AC56KBP3
Key Format: Multipurpose
Serial Number: 406949332
Valid from: 8/3/2009 11:15:05 AM
Valid to: 9/14/2009 11:15:05 AM

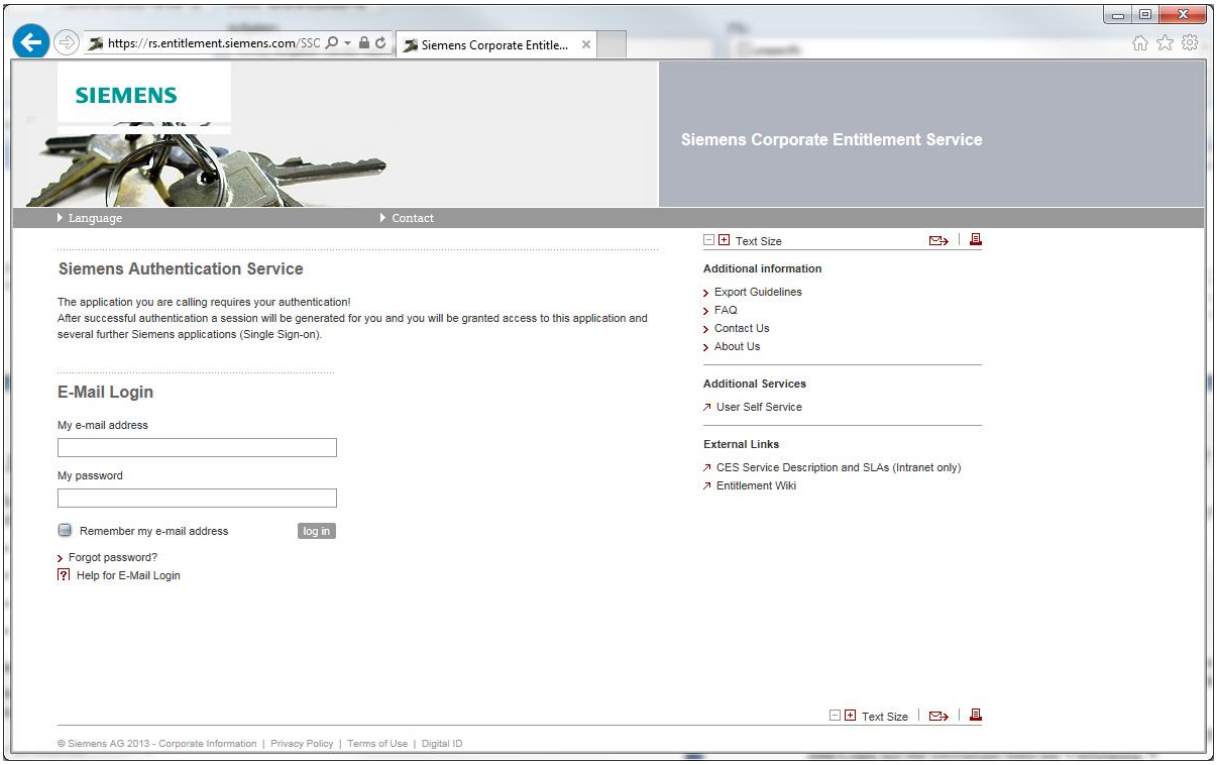
Access the PKI Download Server

Use the link https://pkidownload.siemens.com/ provided in the mail.

The login window will be displayed.

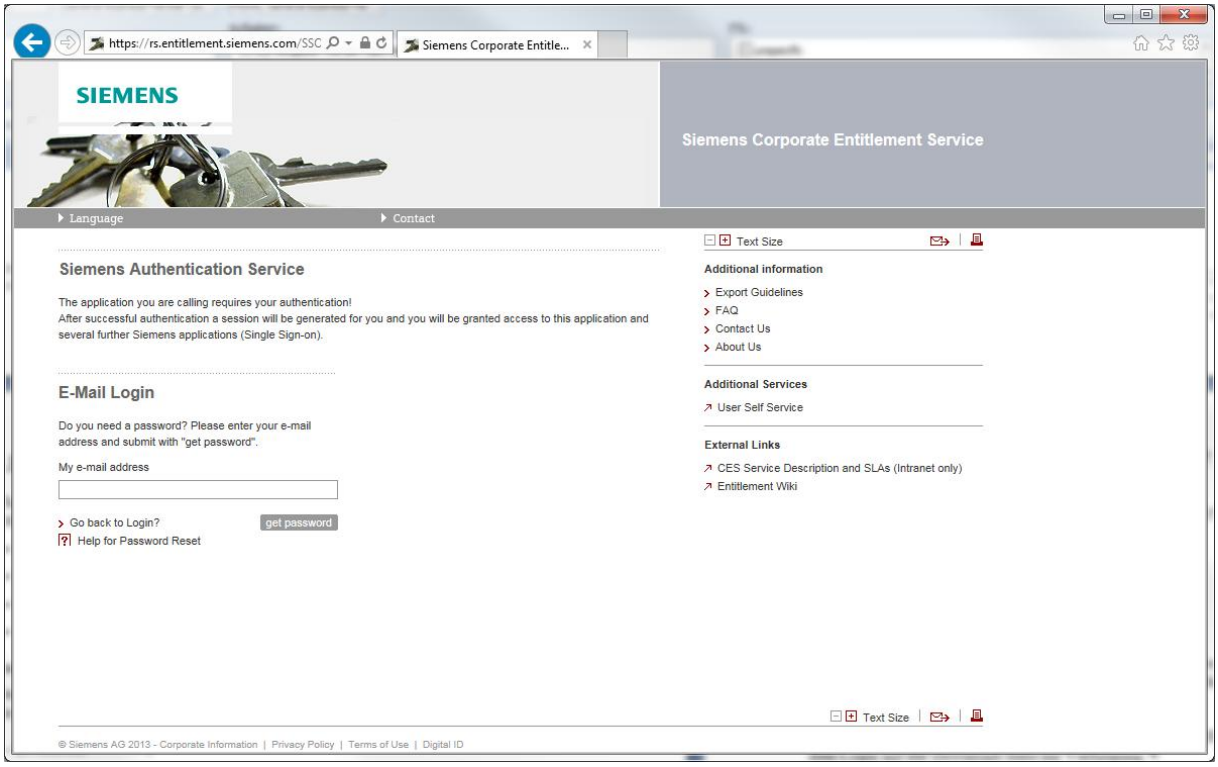


Click "Proceed with Entitlement Login".



To login use your e-mail address as user name and your password.

Please note: If you login for the first time click "Forgot password?"

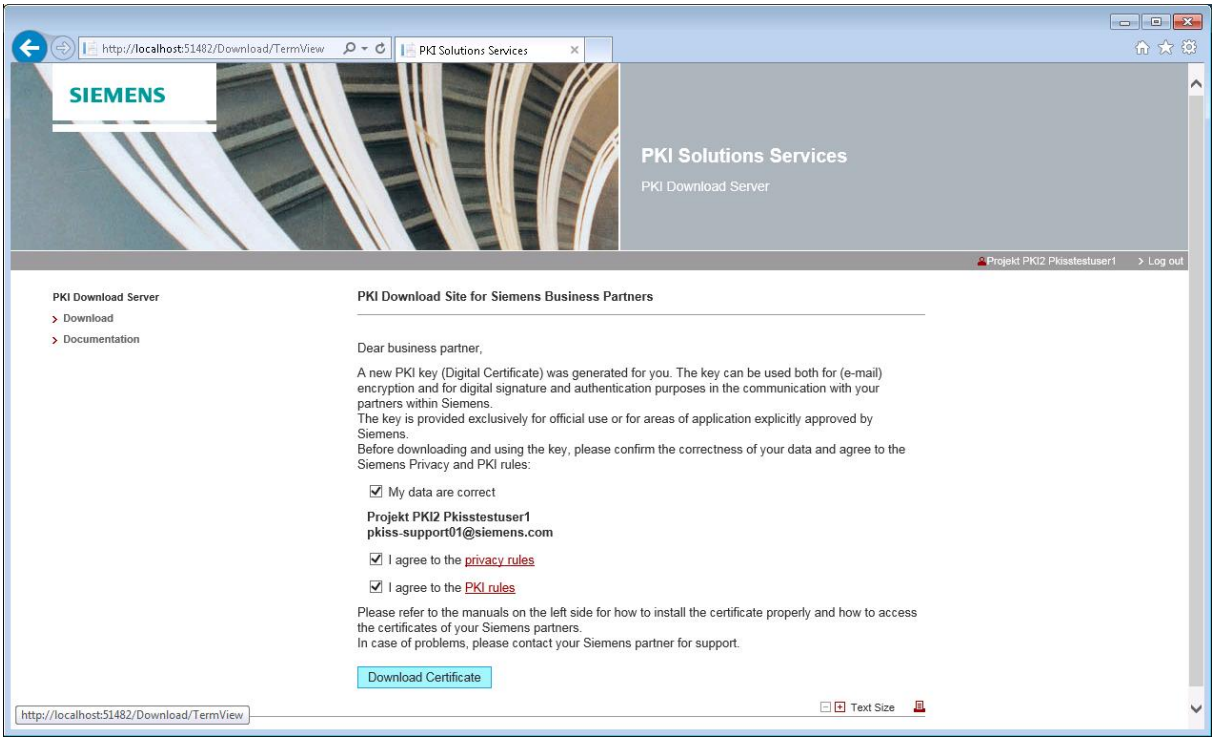


Type in your e-mail address and click "get password" to request a temporary password. The password will be sent to you in an e-mail.
After logging in with your temporary password you will be forced to change it immediately.

In case that your user data does not yet exist, you will receive a message asking you to contact your Siemens partner for support.

3.2 Confirm your Data and Agree to the Siemens Privacy and PKI rules

Before downloading your certificate, you have to confirm the correctness of your data and agree to the Siemens Privacy and PKI rules:



For details on the privacy and PKI rules click "privacy rules" and "PKI rules".

Check the check boxes and click the button "Download Certificate" to continue.

No certificate available

If there is no certificate available for you to download you will receive a message.

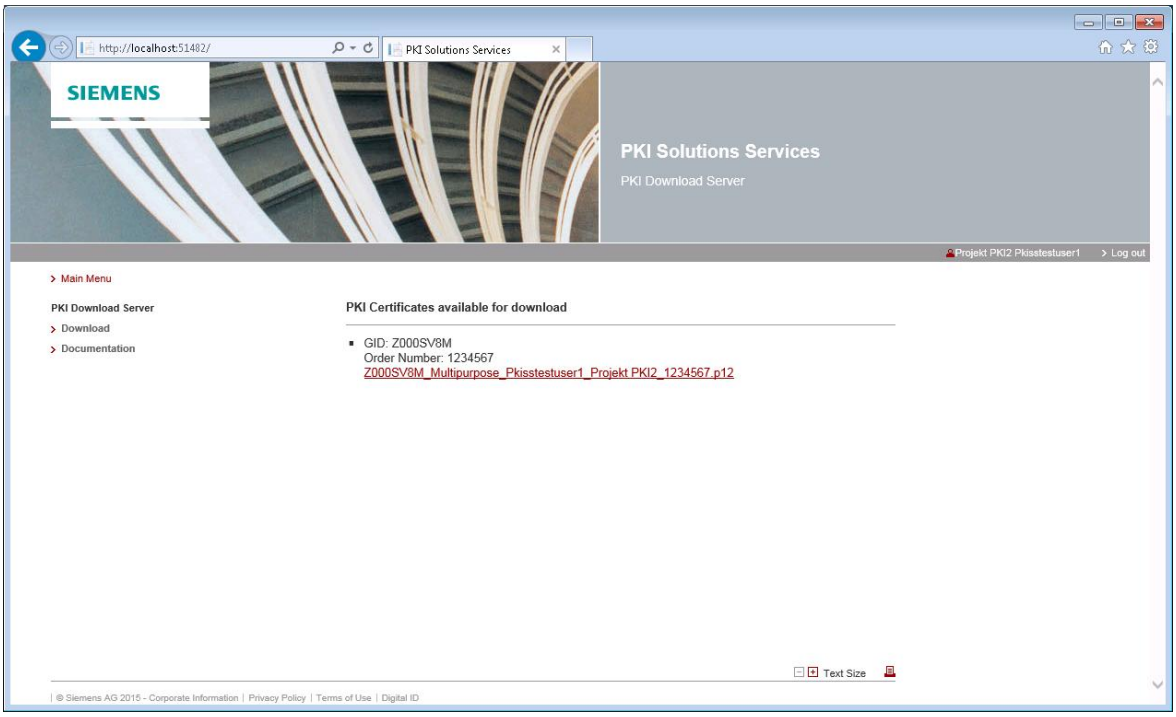
There may be various reasons for this, such as providing the certificate has been delayed, you have already downloaded the certificate, the download was not successful.

Please contact your Siemens partner for support.

3.3 Download your Certificate

After logging in the list of certificates available for download is displayed.

As a rule the list will contain one certificate, namely a new one, but it can also contain "old" certificates that have been provided for you to be able to read your e-mails encrypted with the "old" certificates.

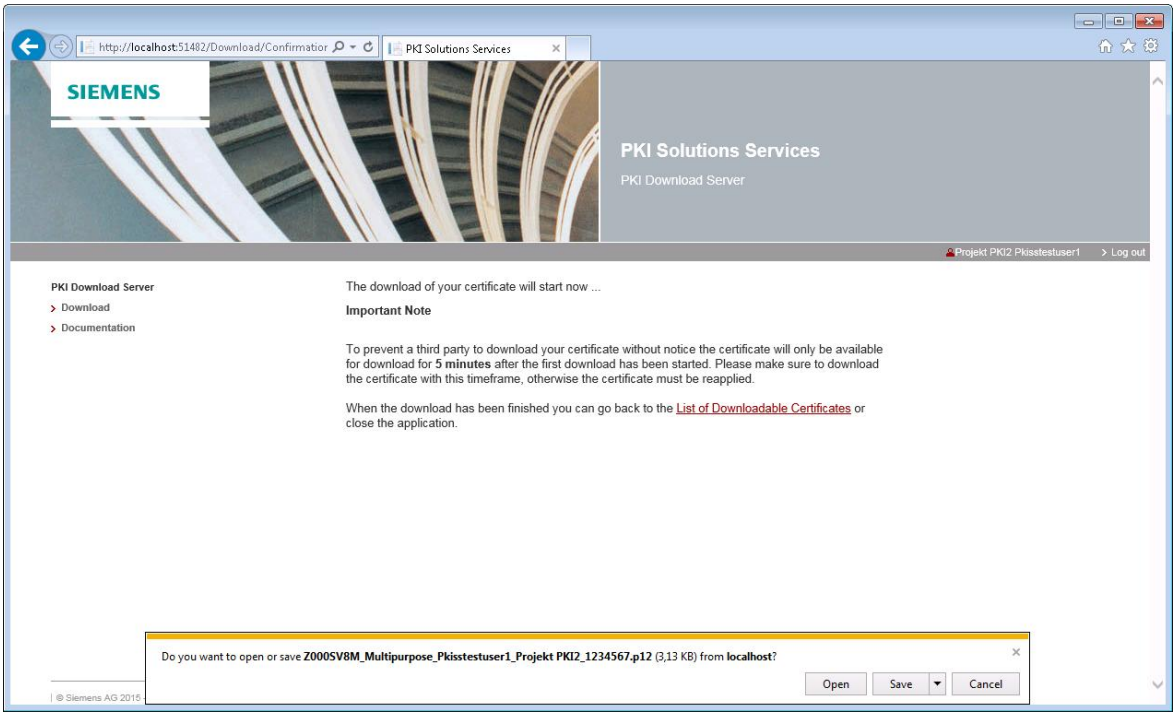


Please note:

> In case of any error during download (e.g. connection loss, cancellation by user) you are able to download the certificate again during a 5 minute timeframe. After this timeframe the certificate will be removed from the server.

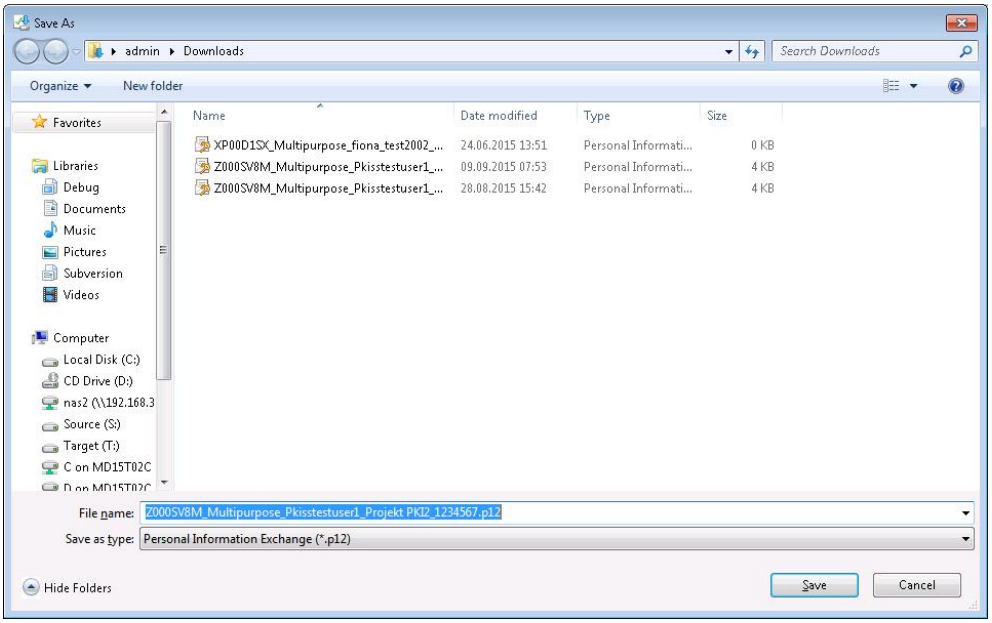
Click the certificate you want to download.

Your browser opens the download window.



Click the arrow at the button "Save". Choose “Save as” and select the directory where you want to save the certificate.

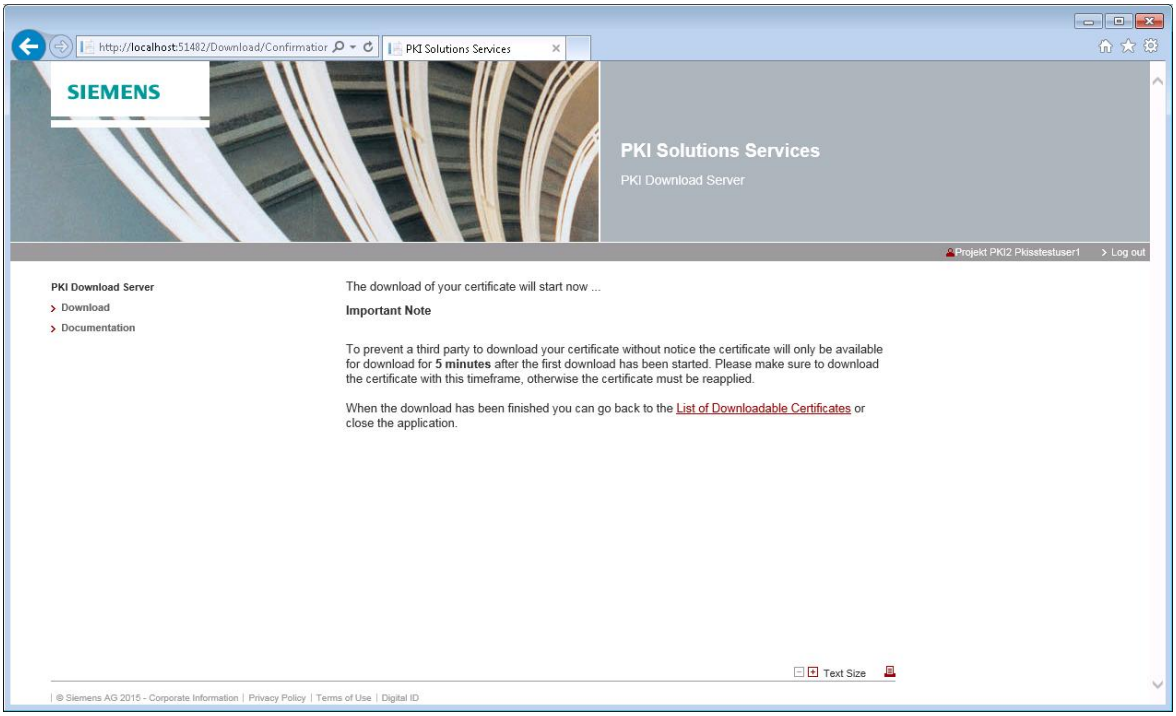
Please be sure to remember where you saved the certificate. You will need to know that to import the certificate later on.



After downloading a certificate you can

- close the application or
- in case there are further certificates available, click the link "List of downloadable certificates".

Be sure to use the link and not to use the back button.



To be able to use your certificate you have to import it on your computer (see chapter 4. Importing your Certificate).

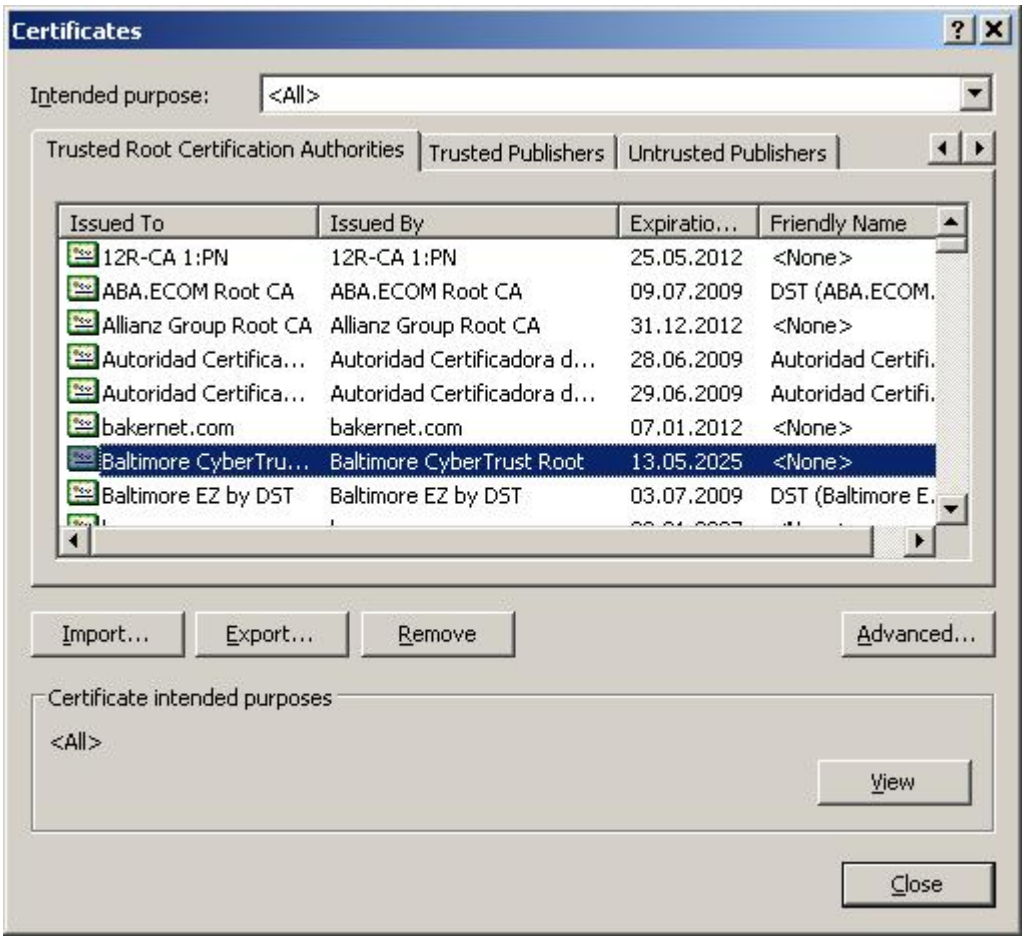
4. Importing your Certificate

4.1 Baltimore CyberTrust Root

Siemens has placed its user certificates for encryption under a public “Root Certification Authority”, the ”Baltimore CyberTrust Root“ from Verizon Business.

The "Baltimore CyberTrust Root" Certificate is pre-installed in all common operating systems and browsers. Thus, external partners have automatically a trust position to the Siemens PKI. The explicit installation of the Siemens Root Certificate is not necessary.

Please make sure that the Baltimore CyberTrust Root" Certificate is installed on your computer:



Please note:

- In some cases for encryption it may nevertheless be necessary to import the Siemens Root-CA Certificates (see chapter 4.2 Installation of the Siemens Root-CA Certificates).
- The Baltimore CyberTrust Root covers trust to the Siemens encryption certificates. For digitally signing mails and for authentication you have to install the Siemens Root-CA Certificates (see chapter 4.2 Installation of the Siemens Root-CA Certificates).

4.2 Installation of the Siemens Root-CA Certificates

Please note:

This chapter does not apply if you want to use your certificate only for encrypting emails. See chapter 4.1 Baltimore CyberTrust Root.

If you want to use your certificate for digitally signing mails and for authentication please follow the instructions in this chapter.

First, the Siemens Root-CA-Certificates must be imported to enable your computer to validate a Siemens certificate as trusted.

The Siemens Root-CA Certificates can be downloaded at https://www.siemens.com/pki.
We recommend to download all Siemens Root-CA Certificates (collected here: "hierarchy of the Siemens CA certificate"1) 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*.

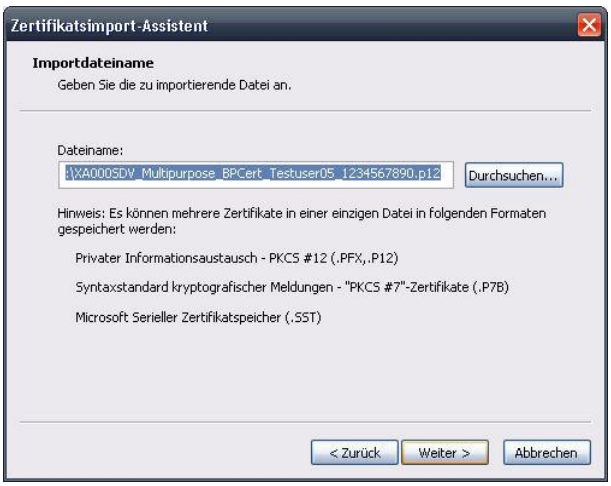
- Click with your right mouse-button the downloaded p7b-file.
- Choose *Install Certificate*. Click on *Next*.
- Make sure the option "choose Certificate Store automatically" is set.
- Click on *Finish*.

[1] http://w1.siemens.com/pki/siemens_ca_certificates.p7b

4.3 Importing your Siemens Certificate

To import a certificate the certificate-file (*.p12) has to be opened. A Certificate Import wizard opens and directs trough the next steps.

In the following window the certificate file name is given once more. Click "Next".



In the field “Password” enter the Transport PIN sent to you from the Siemens Trust Center.

Use the option "automatically" as proposed by the system. Click "Next".

The window for setting the security level is opened.

Choose the highest security level. Only this level grants that the certificate is not used by a malicious attacker without your knowledge.

For the highest security level a separate password has to be defined. This password is needed every time the certificate is used. As it can not be modified afterwards, make sure that you choose a password that you will remember.

In the last step you acknowledge and finalize the import.

The system gives the message that the import was successful.

5. Accessing the Certificates of your Partners at Siemens

5.1 Using the Siemens External Repository or the HTTP-Directory Service of the European Bridge-CA

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

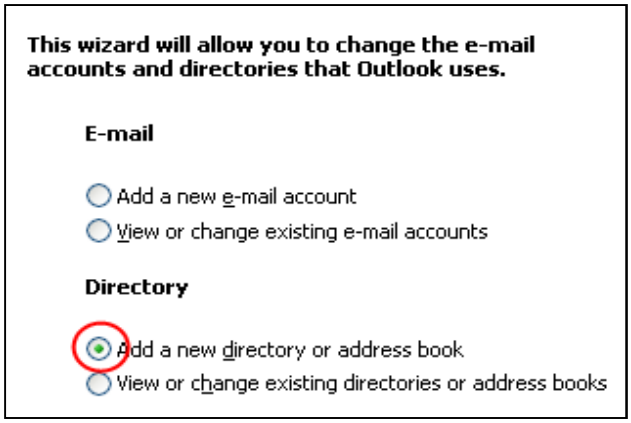
Once the External Repository is installed, no further key exchanges are necessary. Make sure that the integration of the repository is not blocked by your firewall policies.

Follow these instructions for the integration:

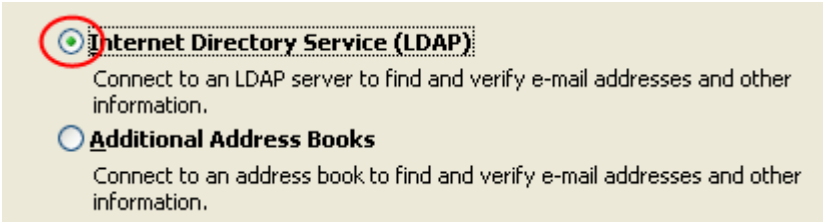
For Office 2007:

Open the Outlook menu Tools →Account Settings

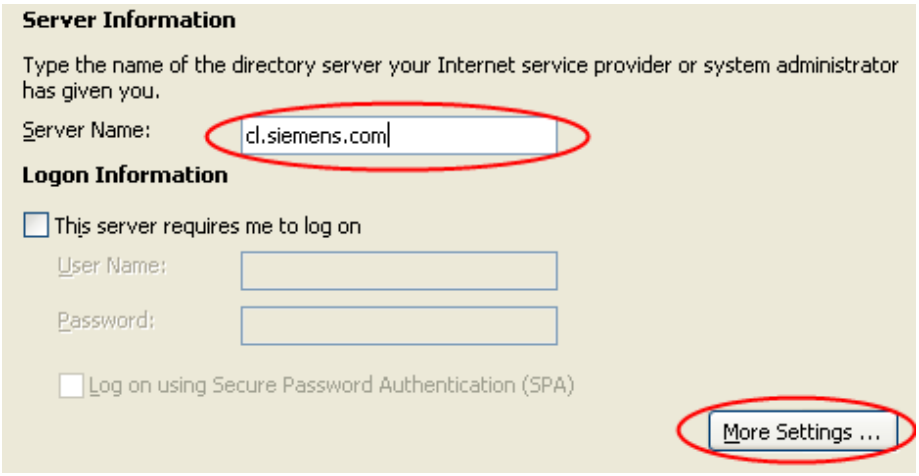
Change to the tab "*Address Books*" and click on "*New...*"



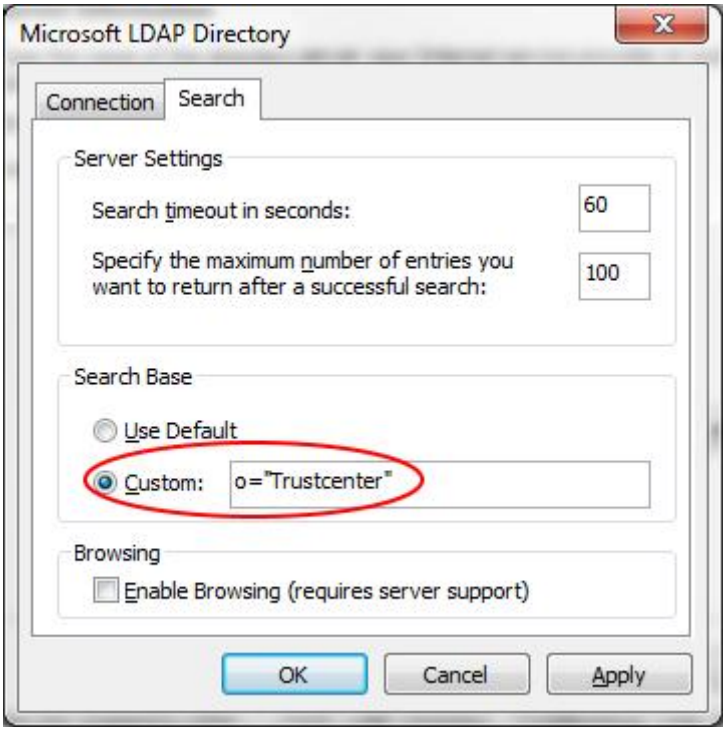
Choose "Internet Directory Service (LDAP)".



The server name is: “*cl.siemens.com*“. Click on "*More Settings".*



Change to the tab “Search” and enter the custom search base: “o=Trustcenter”.



Continue with *OK*.

Click in the previous window the button "*Finish*".

Note: It is necessary to restart Outlook to use the directory service.

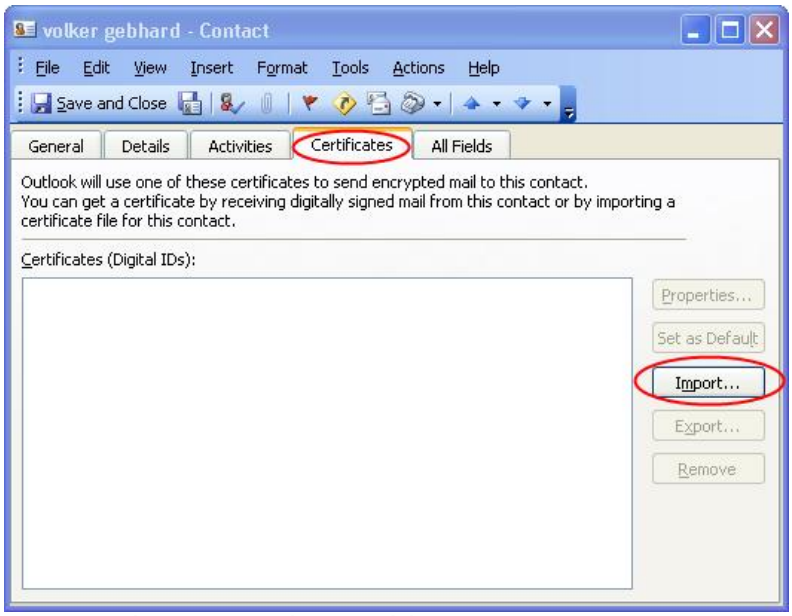
5.2 HTTP Directory Service

Siemens also offers an HTTP Directory Service. With this service, you can access the certificates of your Siemens partner also with your normal web browser. The service is available at http://cl.siemens.com/.

To find a certificate, enter the complete e-mail address of your partner and save the certificate to your hard drive.

To make Outlook use the downloaded certificates, you need to add them to an Outlook contact. Follow these instructions to add a certificate to a contact:

- Change the extension of the downloaded certificates from xxx.crt to xxx.cer.
- Open your Outlook contacts and the contact of the Siemens employee with whom 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*".
- Repeat this for all Siemens employees you want to securely communicate with.



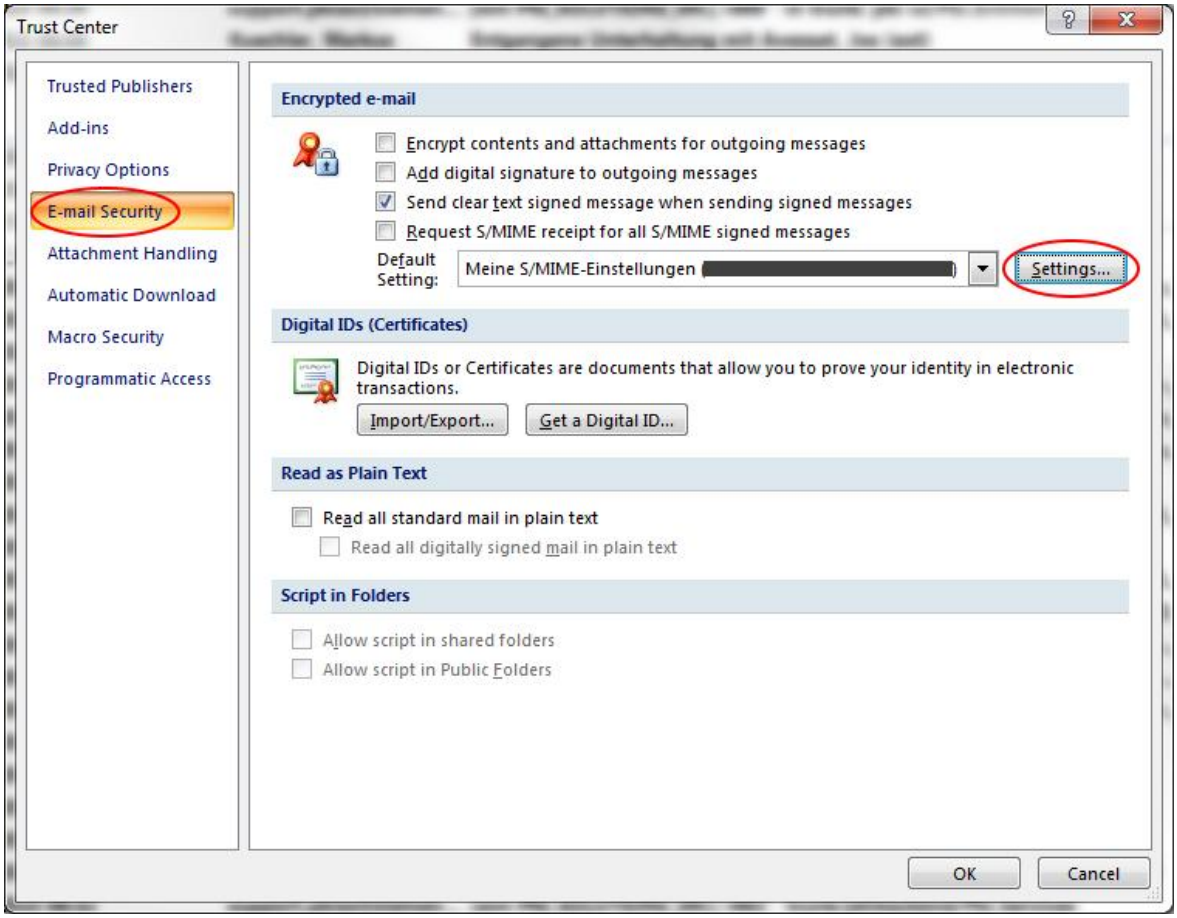
6. Final Settings for the Use in Outlook

To use the email encryption the certificate and the suitable encryption mode have to be chosen. Please note that you can ignore this chapter if you have already installed and used email encryption on your system.

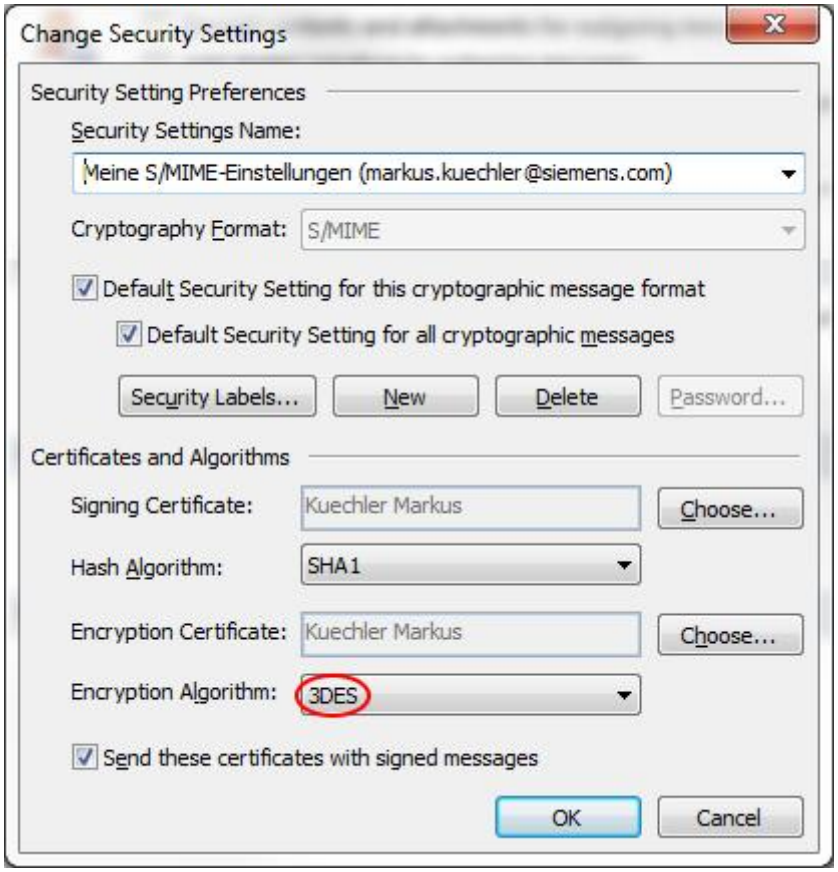
Please follow these steps:

Start Outlook.

- Select "*Tools*" → "*Trust Center*"



- Tab “E-mail Security”
- Click the button "*Settings*" to define the "*Default Setting*".



Under "*Certificates and Algorithms*" select "*Choose*" right next to the field ”*Signing Certificate*“ and select the suggested certificate.

Then choose an encryption algorithm. Select "3DES". Confirm your selections with "OK".

Note: If “3DES” is not available it could happen that a lower encryption method will be used. In this case the email cannot be read by the Siemens employee. To solve this problem, please contact your IT Support.

Close and restart Outlook for the changes to take effect.

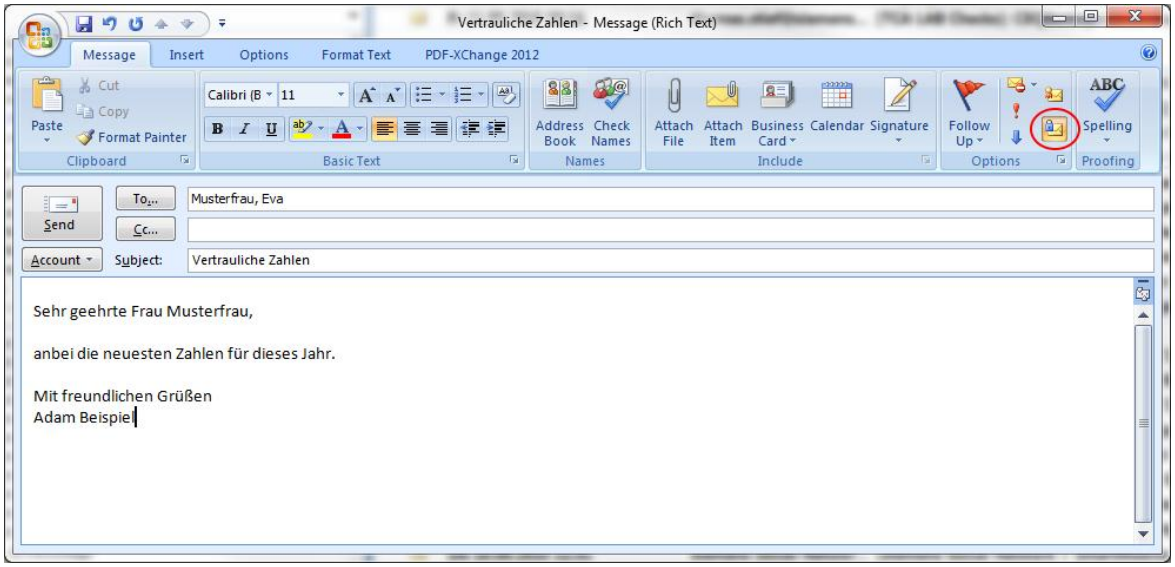
7. Sending and Reading Encrypted E-mails

7.1 Encrypting and Sending E-mails

Create and write a new e-mail as usual.

To encrypt the mail click the encryption symbol  .

Send the mail clicking the button "Send"  .



7.2 Reading Encrypted E-mails

Reading an encrypting e-mail is similar to reading an unencrypted e-mail:

Open the e-mail as usual.

Enter the password you assigned to the key during the import.

Now you can read the e-mail as usual.

8. Possible Problems Caused by an Insufficient Encryption Mode Used by the Business Partner

Siemens has defined internally that at least a 128bit-encryption has to be used for email encryption with Siemens employees.

Because of technical issues, emails may have been sent with a lower encryption than 128bit. These emails cannot be read by Siemens employees.

To solve the problem the business partner has to change his encryption method to 128bit/3DES (see chapter 6 Final Settings for the Use in Outlook).

Otherwise contact your IT Support.