SIEMENS

E-mail encryption with business partners

(Guideline for Siemens employees)

Date:	2013-07-15
Document type:	User description
Version:	3.2
Author:	Editor team PKI

Table of contents

1. Intention of this document

This document is written for Siemens employees who need to exchange encrypted e-mails with external business partners. It describes the system requirements and the necessary configurations (Outlook and Windows) to enable a secure communication (signed and/or encrypted e-mails). It shows especially the possibilities for key exchange.

For business partners there is a complementary documentation which can be committed to him.

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.

2.2 Prerequisites for software:

To encrypt with X.509 certificates the mail program of the business partner has to support this standard. Especially it has to evaluate the field “key usage” in the certificate.

Outlook (since version 2003) is already using an encryption functionality compatible to the Siemens PKI and can be used without any further installation.

Please talk to your business partner if these prerequisites are fulfilled.

3. Manual for Siemens Employees

3.1 Transmission of Siemens certificates to the business partner

This paragraph describes how a Siemens Employee can transfer his certificates to a business partner.

- In case the Siemens External Repository (ldap or http) or the http directory service of the European Bridge CA is used, no other actions are necessary. The business partner will access all Siemens user certificates directly over both services
- In case the use of the Siemens External Repository or the directory service of the European Bridge CA is not possible, you can send a signed e-mail to your business partner. This e-mail will contain your certificates and the business partner can import them directly. Please check following Settings.
    - Open Outlook, click Tools->Options and click on the tab "*Security*", then in the area "*encrypted messages*" on "settings"
      (Since Outlook 2007: Tools->Trust Center in the Section "*E-mail Security*" on "*Settings...*")
    - In the next window „change security settings" activate the option „*Send these certificates with signed messages*"
    - Close all windows with "*OK*"
    - Send a signed e-mail to your business partner after these steps. In such an e-mail all your certificates which are necessary for a secure communication with Siemens are added automatically

3.2 Transmission of the business partner certificates to Siemens

3.2.1 Siemens directory broker

The directory broker is a proxy for special certificate search requests based on the Lightweight Directory Access Protocol (LDAP). Therewith the directory broker forms the functionality of an "outlook address book".

Please check if the directory broker is configured on your system. To do so, please open Outlook and go to Tools → e-mail accounts → show or edit existing directories or address books. (Since Outlookt 2007: Tools → Account Settings in the tab "*Adress Books*") If you see "*directorybroker.pki-services.siemens.com*" in this window, the directory broker is already configured. If this is not the case please follow this manual[1] for the manually set up.

With usage of the directory broker the keys of your business partners can be found automatically and used for encryption, as you know it from the internal usage of e-mail encryption with the SCD. This is only possible if the root-certificates of the business partner are already listed in the Siemens infrastructure.

[1] https://cio.siemens.com/cms/cio/de/infosec/pki/Documents/directorybroker_oab.pdf

Additional information to the Siemens directory Broker, the linked business partners and the report process for further participants can be found on CIT Web-Site[2].

3.2.2 Manual exchange via signed e-mails

If the directory broker cannot be used, please ask your business partner to send a signed e-mail to you. This e-mail must contain his certificates. The necessary settings are described in the manual for business partners, following the example of Outlook native encryption.

Perform the following steps after receiving a signed e-mail:

- After opening a signed e-mail whose Root-CA-Certificates are not yet imported this window will be shown:
- To import the received CA certificates, click on Trust. A pop up “Security warning” appears which asks you to verify the Fingerprint of the certificate. Please check and confirm this fingerprint.

- Click on Yes to copy the certificate into the Windows Certificate Store.
- Right-click onto the sender’s e-mail 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 e-mail for a second time.

[2] https://cio.siemens.com/cms/cio/de/infosec/pki/Pages/pki_extcom_dirbroker.aspx

3.3 Requesting for Siemens certificates for business partners

There is the possibility to order Siemens certificates for business partners if the business partner does not own certificates himself. These certificates must be ordered by the Siemens Employee over the "*FIONA*" system. In the Siemens intranet you can find a detailed manual[3].

3.4 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.

[3]https://workspace.cio.siemens.com/content/10002378/pki/FiOnA/docs/Multipurpose%20Business%20Partner%20Certificates/MPBP_guideline_applicant_en.pdf

4. Possible problems through insufficient encryption at the business partner

Siemens internally has defined that at least a 128bit-encryption has to be used for e-mail encryption.
Because of technical issues, it can appear that e-mails are sent with a weaker encryption than 128bit. These e-mails cannot be read by Siemens employees. The problem cannot be solved by Siemens. To solve the problem it is necessary that the business partner changes his encryption method to 128bit.
In this case please contact your IT Support. Detailed information can be found here[4].

[4]https://pkisupport.siemens.com/wppages/mail_kb_mails_are_not_readable.aspx