SIEMENS

E-Mail-Encryption requirements

Date:	13.07.2011
Document type:	User description
Version:	2.0
Author:	Editor team PKI

Table of contents

1. Intention of this document

This guide is for all Siemens Employees and their business partners who want to get an overview about which different requirements for a secure communication (encrypted and/or signed E-Mails) between them exist. This document distinguishes, if there is already a foundation of trust or it has to be established first.

After you found out in which situation you are, you can get an overview about the possibilities for the exchange of the certificates.

This document is only an overview about the possibilities for a secure communication. You can find a detailed description for Siemens Employees here[1] and for business partners here[2].

Detailed information to the topic PKI can be found on the internet on this site www.siemens.com/pki.

[1] https://cio.siemens.com/cms/cio/en/infosec/pki/Documents/E-Mail_encryption_Siemens_en.pdf
[2] https://cio.siemens.com/cms/cio/en/infosec/pki/Documents/E-Mail_encryption_GP_en.pdf

2. Requirements

The requirements for secure communication are separated in different fields:

- At first it should be cleared, if certificates are available or have to be ordered
- After this it has to be checked, if there is a trust between the PKIs
- At last the method how the certificates will be exchanged has to be defined

For the secure PKI-based communication between Companies/Organizations both PKIs have to trust each other and the Root-CA-certificates must be distributed on both sides IT-infrastructure.
Siemens is using the so-called “Trusted Store” for this. The Trusted Store is a list of Root-Certificates which we trust and which are/will be distributed on the Standard-Clients or rather in the Active Directory.

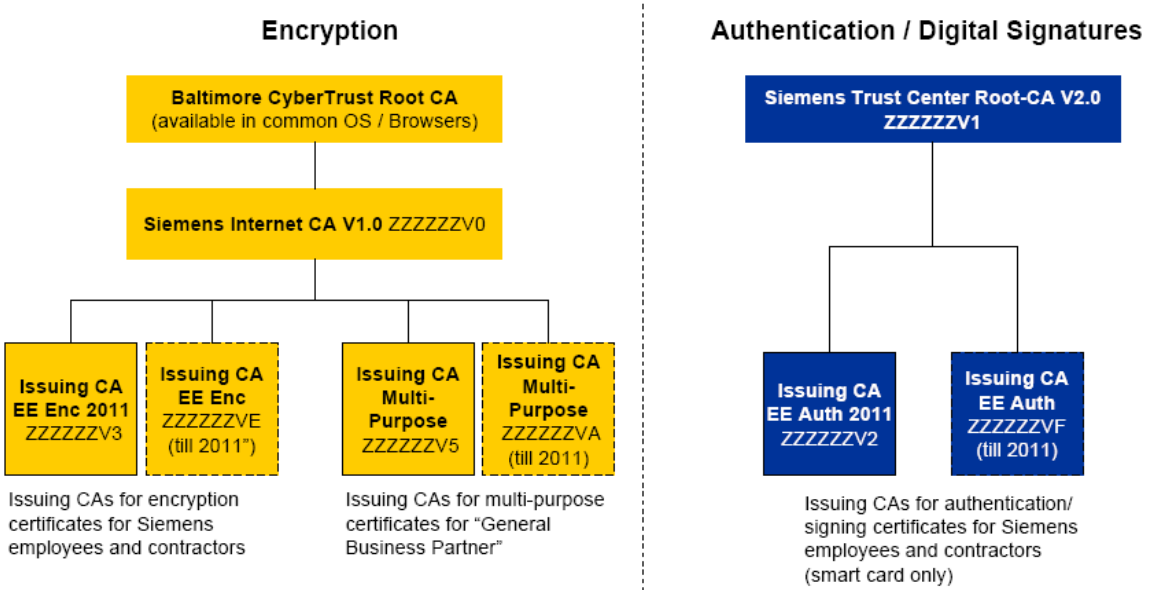
3. Properties of the Siemens PKI

3.1 External Trust – Baltimore Cyber Trust Root

Siemens has placed all relevant pieces of the Siemens PKI for the secure communication under the public "Baltimore CyberTrust Root[3]" of Verizon Business, to simplify the process of establishing trust.

The Root-CA-certificate of the Baltimore CyberTrust Root is contained in all major operating systems and browsers. Therefore external partner have automatically a Trust to the Siemens PKI. The explicit installation of the Siemens Root is not necessary. Underneath the public Baltimore CyberTrust Root, Siemens is exhibiting the following certificate types:

- Encryption-certificates for employees and business partner
- Server-certificates for (Web-)Server on the internet
- External code-signing-certificates



A secure e-mail exchange between Siemens employees and business partner is normally without any further installation possible, like it is shown on the yellow hierarchy. In case of problems the intermediate Siemens Internet CA has to be installed on the client of the business partners besides the Baltimore CyberTrust.

If the business partner wants to check digital signatures, he must explicitly trust the Siemens Trust Center Root CA, i.e. the blue hierarchy will be needed. Further information can be found here[4].

[3] http://cacert.omniroot.com/bc2025.crt
[4] https://cio.siemens.com/cms/cio/en/infosec/pki/Documents/certificate_authority_hierarchy.pdf

3.2 Siemens is a member of European Bridge CA

Siemens is a member of the European Bridge CA (EBCA). This supports a secure and authentic communication between companies and organizations. Thereby the Public Key Infrastructures (PKI) of the organizations is linked together.

Is the business partner also member of the EBCA a communication is easily possible.

The Root-Certificates of the Bridge CA members are already integrated in the Siemens-IT-Infrastructure, which means they are already in the trusted store. In this case the Siemens side has nothing else to consider.

However the partner has to check, if the Siemens-Root-Certificates (or at least the Baltimore Cyber Trust Root) are also already listed in the IT-Infrastructure or if they have to be populated first.

4. Properties of the business partner PKI

If the business partner is commanding about own certificates, the next thing to do is to check if there is already a trust relationship to Siemens or it has to set up first. Normally over the Baltimore CyberTrust Root this should already exist.

4.1 The business partner receives certificates from a public trust center in the Siemens trusted Store

There are a lot of public trust centers, which Root-Certificates are already listed in the Siemens Trusted Store.

Should the business partner own certificates from such Trust centers, than is a secure communication with Siemens Employees without any bigger effort possible.

The business partner has again to check if the Siemens-Root-Certificates are listed in his IT infrastructure.

This hyperlink[5] shows you the Trusted Store in the Siemens intranet.

4.2 Business partner owns certificates from a Trust Center without a trust relationship to Siemens.

Should the business partner use certificates from a trust center, which aren't listed in the Siemens trusted store, there are different possibilities.

For companies with a big (Siemens wide) demand for a secure communication it is possible, that the trust center will be listed in the Siemens trusted Store. Please contact Siemens CIT G ISEC for this.

For all other partners there is also the possibility to exchange (user) certificates in individually basis with communication partner.

4.3 Business partner owns no certificates

4.3.1 Receiving certificates from Siemens Trust Center

It is possible, if the business partner owns no certificates (and his company is also not disposal one) to get so called "general business partner" certificates over the Siemens Trust Center. Therefore the communication partner from Siemens has to request a certificate for the business partner over the "Fiona" procedure.

[5] https://cio.siemens.com/cms/cio/en/infosec/pki/Documents/DirBrokerList.pdf

4.3.2 Obtaining of certificates from a public Trust center

It is possible to obtain certificates from public trust centers, too.

Several known trust center, which are already listed in the Trusted Store, are for example:

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

For detailed information please contact the respective provider.
The business partner has to attend, that the Siemens-Root-Certificates has also to be listed in the own certificate store.

5. Possibilities for the certificate exchange

There are several possibilities fort the exchange of certificates.

5.1 Access for the business partner to Siemens certificates

Siemens offers different possibilities to get access of the Siemens certificates

The certificates are

- external accessible over the web, the Siemens External Repository or
- can be exchanged manually.

The easiest way is the usage of the Siemens external Repository. There a two ways to get access. Either you can use the automatic way over LDAP or the manually way over the web.

For the automatically invocation over LDAP calls, a unique establishment for the external Repository on the e-mail encryption client or the e-mail encryption gateway, from the business partner is necessary. After this a separate key exchange isn't needful.

In problematic cases it should be cleared with the network administrator, if such a LDAP request from the network of the business partner is possible.

As an alternative the external repository allows a certificate retrieval over a website[6]. This method needs more effort, because the certificates have to be populated manually.

If the business partner isn't able to access the External repository it is also an individual exchange of certificates via signed e-mails possible. For this the Siemens Employee has to send a onetime signed e-mail and the business partner can import the certificates out of this e-mail into his system.

5.2 Access from Siemens Employees to business partner certificates

If the trust center from the business partner publishes the certificates (as Siemens) in a trusted store at the web, Siemens Employees can automatically and/ or manually recall the certificates.

For the automatic exchange the repository of the business partner has to be listed in the Siemens directory broker and the link has to be registered on the client.

The most important public repositories for certificates are already available on the Siemens directory broker. Should the business partner use a repository, which isn't listed in the directory broker, an entry over CIT G ISEC is possible.

As alternative the certificates can be exchanged manually. This is an easy and fast possibility to tether individually business partners without an own directory service.

[6] http://cl.siemens.com

Other possibilities to disposal keys from business partners to Siemens are the deposit in the Active directory or to create an offline address book for Outlook. Both of these possibilities are related with high-maintenance and should only be used in very few instances.

6. Usage scenarios

In this chapter a few usage examples can be found.

- An EON Employee got certificates from his company and he wants to exchange signed e-mails with a Siemens Employee. Since EON is a member of the European Bridge CA this is without any bigger effort possible and the both companies have listed their Root-certificates in their trusted store. The retrieval of the certificates is on both sides over a repository possible
- A customer from a Siemens owns no certificates but he has to exchange e-mails with Siemens Employees. The Siemens Employee orders over “FIONA” a general business partner certificate. The customer installed the Siemens-root-certificates on his system and the external repository.
- An encrypted communication between a single Siemens Employee and a business partner is necessary. The business partner already owns certificates. His trust center is not listed in the Siemens trusted store and has no repository on the internet. The two communication partners decided to exchange the keys manually.