SIEMENS

E-Mail-Verschlüsselung
Vorrausetzungen

Datum:	09.08.2011
Dokumentenart:	Anwenderbeschreibung
Version:	2.0
Autor:	Redaktionsteam PKI

Inhaltsverzeichnis

1. Zweck des Dokumentes:

Diese Anleitung richtet sich an Siemens Mitarbeiter und Ihre Geschäftspartner, die einen Überblick bekommen wollen, welche verschiedenen Vorraussetzungen für eine sichere Kommunikation (verschlüsselte und / oder signierte E-Mails) miteinander existieren. Das Dokument unterscheidet hier, ob bereits eine Vertrauensbasis besteht oder diese erst aufgebaut werden muss.

Nachdem Sie herausgefunden haben in welcher Situation Sie sich befinden, bekommen Sie einen Überblick über die einzelnen Möglichkeiten für den Zertifikat Austausch.

Das Dokument bietet nur einen Überblick zu den einzelnen Möglichkeiten die für eine sichere Kommunikation nötig sind. Eine genauere Beschreibung für Siemens Mitarbeiter finden Sie hier[1] und für Geschäftspartner hier[2].

Detaillierte Informationen zum Thema PKI finden Sie im Internet unter www.siemens.com/pki.

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

2. Voraussetzungen

Die Voraussetzungen sind in verschiedene Bereiche zu teilen:

- Als erstes ist zu klären ob bereits Zertifikate zur Verfügung stehen oder diese erst besorgt werden müssen.
- Danach muss überprüft werden ob ein Vertrauen zwischen den PKIs besteht, siehe unten.
- Als letztes muss gegebenenfalls noch geklärt werden, wie ein gegenseitiger Austausch der Zertifikate möglich ist.

Für die sichere PKI-gestützte Kommunikation zwischen Unternehmen/Organisation müssen sich die beiden PKI-en gegenseitig vertrauen und die Root-CA-Zertifikate müssen auf beiden Seiten in der IT-Infrastruktur verteilt sein.
Siemens pflegt dazu den sogenannten „Trusted Store“. Der Trusted Store ist eine Liste von Root-Zertifikaten denen wir vertrauen und die auf den Standard-Clients bzw. im Active Directory verteilt sind/werden.

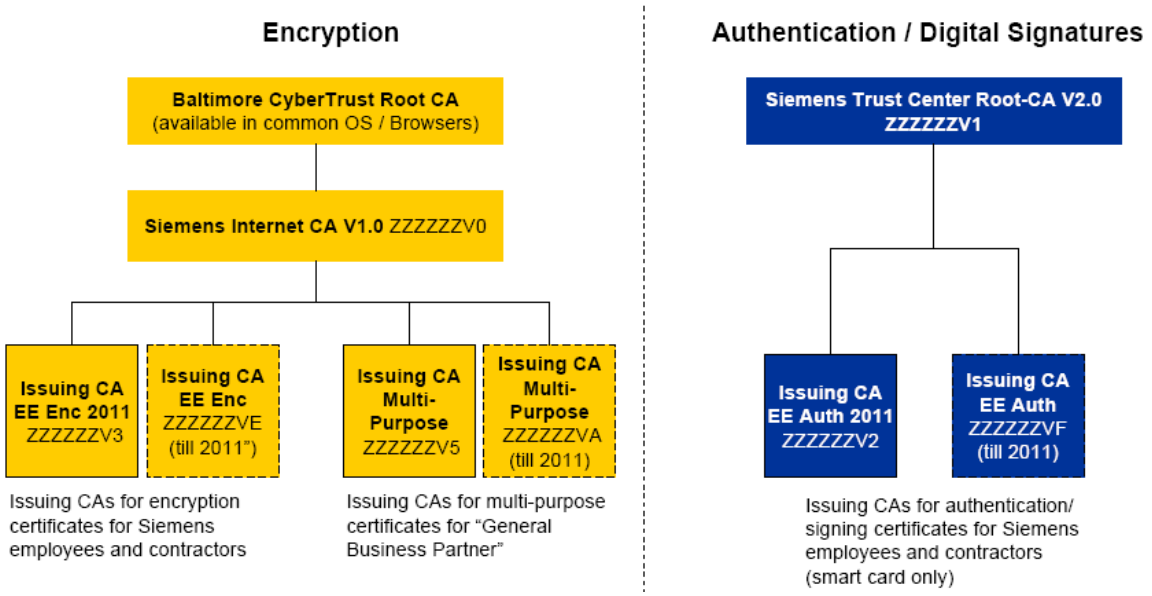
3. Eigenschaften der Siemens PKI

3.1 Baltimore CyberTrust Root

Um den Prozess des gegenseitigen Vertrauens zu vereinfachen, hat Siemens die für die externe Kommunikation relevanten Teile der Siemens PKI unter die öffentliche „Baltimore CyberTrust Root[3]“ von Verizon Business, gestellt.

Das Root-CA-Zertifikat der Baltimore CyberTrust Root ist in allen gängigen Betriebsystemen und Browsern enthalten. Externe Partner haben damit automatisch eine Vertrauensstellung (Trust) zur Siemens PKI. Die explizite Installation der Siemens Root kann damit (im Regelfall) entfallen. Unterhalb der öffentlichen Baltimore CyberTrust Root stellt Siemens die folgenden Zertifikatstypen aus:

- Verschlüsselungs-Zertifikate für Mitarbeiter und Geschäftspartner
- Server-Zertifikate für (Web-)Server im Internet
- Externe Code-Signing-Zertifikate



Ein sicherer E-Mail Austausch zwischen Siemens Mitarbeiter und Geschäftspartner ist im Normalfall ohne weitere Installation möglich, wie hier in der gelben Hierarchie gezeigt wird. Im Problemfall muss die Siemens Internet CA beim client des Geschäftspartners neben der Baltimore Cybertrust installiert sein.
Falls Geschäftspartner die Signatur prüfen und verifizieren will, muss er dazu die Siemens Trust Center Root CA installieren. Hierzu benötigt man die Hierarchie, die hier blau dargestellt wird. Weitere Informationen hier[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 ist Mitglied European Bridge CA

Siemens ist Mitglied der European Bridge CA (EBCA), diese ermöglicht eine sichere und authentische Kommunikation zwischen Unternehmen und Organisationen. Dabei werden die Public-Key-Infrastrukturen (PKI n) der einzelnen Organisationen miteinander verknüpft.

Ist das Trust Center des Geschäftspartners Mitglied der EBCA ist eine Kommunikation einfach möglich.

Die Root-Zertifikate der Bridge-CA Teilnehmer sind bereits in der Siemens-IT-Infrastruktur integriert, d. h. sie befinden sich im Trusted Store. In diesem Fall ist von der Siemens-Seite nichts weiteres mehr zu beachten.

Der Partner hingegen muss überprüfen, ob die Siemens-Root-Zertifikate (oder zumindest die Baltimore Cyber Trust Root) ebenso bereits in dessen IT-Infrastruktur verteilt sind oder sie noch eingepflegt werden müssen.

4. Eigenschaften Geschäftspartner PKI

Besitzt der Geschäftspartner eigene Zertifikate, ist als nächstes zu überprüfen ob hier bereits eine Vertrauensbeziehung zu Siemens besteht oder diese erst aufgebaut werden muss. Normalerweise sollte diese durch die Baltimore CyberTrust Root bereits bestehen.

4.1 Geschäftspartner bezieht Zertifikate von einem Öffentlichen Trust Center im Siemens Trusted Store

Es gibt eine Vielzahl öffentlicher Trust Center, deren Root-Zerifikate bereits im Siemens Trusted Store gelistet sind.

Sollte der Geschäftspartner Zertifikate eines solchen Trust Centers besitzen, ist auch hier eine Kommunikation mit Siemens Mitarbeitern ohne großen Aufwand möglich.

Wiederum muss hier der Geschäftspartner wieder überprüfen ob die Siemens-Root-Zertifikate in dessen IT-Infrastruktur sind.

Unter folgendem Link[5] finden Sie den Trusted Store im Siemens Intranet.

4.2 Geschäftspartner bezieht Zertifikate von Trust Center ohne Trust Beziehung zu Siemens

Sollte der Geschäftspartner Zertifikate von einem Trust Center beziehen, das nicht im Siemens Trusted Store gelistet ist, gibt es verschiedene Möglichkeiten.

Für Unternehmen mit einem großen (Siemens-weiten) Bedarf an sicherer Kommunikation ist es möglich, dass das Trust Center in den Siemens-Store mit aufgenommen wird. Bitte wenden Sie sich hierzu an Siemens CIT G ISEC.

Für alle weiteren Partner besteht dazu die Möglichkeit, (Nutzer-)Zertifikate auf individueller Basis mit Ihren Kommunikationspartnern auszutauschen.

4.3 Geschäftspartner besitzt keine eigenen Zertifikate

4.3.1 Bezug von Zertifikaten vom Siemens Trust Center

Wenn der Geschäftspartner keine eigenen Zertifikate besitzen sollten (und auch die Firma keine zur Verfügung stellt) ist es möglich, über das Siemens Trust Center sogenannte „General Business Partner“ Zertifikate zu beziehen. Dazu muss der Ansprechpartner von Siemens das Zertifikat für den Geschäftspartner über das Verfahren „FIONA“ bzw. die zuständigen Stellen beantragen lassen.

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

4.3.2 Bezug von Zertifikaten von einem öffentlichen Trust Center

Ebenso ist es möglich, Zertifikate über öffentliche Trust Center zu erwerben.
Einige bekannte Trust Center, die bereits im Trusted Store gelistet sind, sind zum Beispiel:

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

Bitte wenden Sie sich für genauere Informationen an die jeweiligen Anbieter.
Zu beachten ist, dass auch hier die Siemens-Root-Zertifikate in den eigenen Zertifikats-Store aufgenommen werden müssen.

5. Möglichkeiten zum Zertifikats Austausch

Zum Austausch von Zertifikaten gibt es verschiedene Möglichkeiten.

5.1 Zugriff der Geschäftspartner auf Siemens Zertifikate

Siemens bietet verschiedene Möglichkeiten, um auf Siemens Zertifikate zuzugreifen.

Die Zertifikate sind

- extern vom Internet zugänglich, über das Siemens External Repository oder
- können manuell ausgetauscht werden.

Der einfachste Weg hierbei ist die Verwendung des Siemens External Repositories. Der Zugriff ist über zwei Wege möglich entweder automatisiert per LDAP oder manuell per Web.

Für den automatischen Zertifikats Aufruf via LDAP-Anfragen. Ist eine einmalige Einrichtung des External Repositories beim E-Mail Verschlüsselungsclient oder E-Mail Verschlüsselungsgateway des Geschäftspartners erforderlich. Danach ist kein gesonderter Schlüsselaustausch mehr nötig.

Im Problemfall sollte mit dem zuständigen Netzwerkadministrator geklärt werden, ob eine solche LDP-Anfrage aus dem Netzwerk des Geschäftspartners möglich ist.

Alternativ erlaubt das External Repository Zertifikats Abrufe über eine Webseite[6]. Diese Methode ist aufwendiger, da die Zertifikate manuell eingepflegt werden müssen.

Falls der Geschäftspartner nicht auf den External Repository zugreifen kann ist auch ein individueller Austausch von Zertifikaten per signierter E-Mail möglich. Dazu muss der jeweilige Siemens Mitarbeiter dem Geschäftspartner einmalig eine signierte E-Mail senden und der Partner kann aus dieser Mail die Zertifikate in sein System importieren.

5.2 Zugriff von Siemens auf Geschäftspartner Zertifikate

Falls das Trust Center des Geschäftspartners die Zertifikate (wie Siemens) im Internet in einem Verzeichnisdienst veröffentlicht, können die Zertifikate dort von Siemens Mitarbeitern automatisiert und/oder manuell abgerufen werden.

Zum automatisierten Austausch muss das Repository vom Geschäftspartner in dem Siemens Directory Broker gelistet sein und der Link auf jedem Client eingetragen.

Die wichtigsten öffentlichen Repositories für Zertifikate werden bereits im Siemens Directory Broker zur Verfügung gestellt. Sollte der Geschäftspartner ein Repository nutzen, das nicht im Directory Broker gelistet ist, ist ein Eintrag über CIT G ISEC möglich.

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

Alternativ können Zertifikate immer manuell ausgetauscht werden. Dieses ist eine einfache und schnelle Möglichkeit einzelne Geschäftspartner ohne eigenen Verzeichnisdienst anzubinden.

Weitere Möglichkeiten Schlüssel von Geschäftspartnern bei Siemens zur Verfügung zu stellen, ist die Hinterlegung im Active Directory oder die Erzeugung eines Offline Adress Books für Outlook. Beide Möglichkeiten sind aber mit hohem Pflegeaufwand verbunden und sollten deswegen nur in Einzelfällen in Erwägung gezogen werden.

6. Anwendungsszenarien

In diesem Kapitel können verschiedene Anwendungsbeispiele gefunden werden.

- Einem Mitarbeiter der EON wurden Zertifikate von seiner Firma ausgestellt und er möchte jetzt mit einem Siemens Mitarbeiter verschlüsselte E-Mails austauschen. Hierbei ist dies ohne weiteren Aufwand möglich, da EON wie Siemens Mitglied der European Bridge CA ist und beide Unternehmen ihre Root-Zertifikate jeweils verteilt haben. Der Abruf der Zertifikate ist hier auf beiden Seiten über ein Repository möglich.
- Ein Kunde von Siemens besitzt noch keine Zertifikate, muss aber verschlüsselte E-Mails mit einem Siemens Mitarbeiter austauschen. Der Siemens Mitarbeiter bestellt daher über „FIONA“ ein General Business Partner Zertifikat. Der Kunde richtet auf seinem System die Siemens-Root-Zertifikate und das External Repository ein.
- Eine verschlüsselte Kommunikation zwischen einem einzelnen Siemens Mitarbeiter und einem Geschäftspartner wird benötigt. Der Geschäftspartner verfügt bereits über Zertifikate. Sein Trust Center ist nicht im Siemens Trusted Store gelistet und verfügt nicht über ein Repository im Internet. Daher entscheiden sich beide für den manuellen Schlüsselaustausch.