SIEMENS

E-Mail-Verschlüsselung mit Geschäftspartnern

(Anleitung für Geschäftspartner)

Datum:	15.07.2013
Dokumentenart:	Anwenderbeschreibung
Version:	3.2
Autor:	Redaktionsteam PKI

Inhaltsverzeichnis

1. Zweck des Dokumentes:

Diese Anleitung richtet sich an Siemens Geschäftspartner, die mit ihren Partnern bei Siemens per verschlüsselter E-Mail sicher kommunizieren möchten. Es wird beschrieben, welche Systemvoraussetzungen erfüllt sein müssen und welche Konfigurationseinstellungen (Outlook und Windows) nötig sind, um eine sichere Kommunikation (signierte und / oder verschlüsselte E-Mails) zu ermöglichen. Insbesondere wird gezeigt, auf welche Arten der Schlüsselaustausch erfolgen kann und wann welche Möglichkeit am sinnvollsten ist.

Bei Problemen wenden Sie sich bitte an Ihren Siemens Partner.

2. Voraussetzungen beim Geschäftspartner

2.1 Zertifikate:

Um E-Mails verschlüsselt versenden zu können, braucht der Geschäftspartner Zertifikate.

Es gibt unterschiedliche Standards bei Zertifikaten. Microsoft Outlook und viele andere Programme unterstützen X.509 (S/MIME), deshalb sollte dieser Standard zur sicheren Kommunikation verwendet werden. Aus diesem Grund verfügen alle Siemens-Mitarbeiter über X.509 Zertifikate. PGP wird nur als Sideline unterstützt und steht den Siemens-Mitarbeitern nur auf Antrag zur Verfügung.

Verfügt die Organisation des Geschäftspartners wie Siemens über ein eigenes Trust Center oder verwendet Ihre Firma ein öffentliches Trust Center so sollte dieses zum Bezug der Zertifikate verwendet werden.

Ein paar bekannte öffentliche Trustcenter, die bereits in der Siemens IT Infrastruktur gelistet sind, sind:

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

2.2 Anforderungen an die Software:

Um mit X.509 Zertifikaten verschlüsseln zu können, muss das verwendete Mailprogramm diesen Standard unterstützen. Außerdem muss es das Feld „*Schlüsselverwendung*“ im Zertifikat auswerten. Outlook ab Version 2003 enthält bereits eine Verschlüsselungsfunktionalität, die zur Siemens PKI kompatibel ist und ohne weitere Installationen genutzt werden kann.

Die nachfolgenden Benutzeranleitungen beschreibt am Beispiel von Outlook 2003, welche Schritte unternommen werden müssen, damit Geschäftspartner und Siemens-Mitarbeiter verschlüsselte oder signierte E-Mails austauschen können. Hierzu ist es notwendig, dass der Geschäftspartner seine Zertifikate in seinem Mailprogramm installiert hat.

3. Möglichkeiten des Zertifikatsaustauschs

Abhängig von der Anzahl der Kommunikationspartner sind unterschiedliche Möglichkeiten des Zertifikatsaustauschs sinnvoll.

Diese Alternativen können zur Anwendung kommen:

- Grundsätzlich wird die Verwendung des Siemens External Repositories empfohlen. Dies ist ein Verzeichnisdienst für PKI Schlüssel im Internet, über den mit jedem Siemens Mitarbeiter sicher kommuniziert werden kann. Es wird dabei direkt auf die aktuellen Zertifikate der Siemens Mitarbeiter zugegriffen. Nach der einmaligen Einrichtung ist kein gesonderter Schlüsselaustausch notwendig. Allerdings muss es möglich sein, sogenannte LDAP-Anfragen über an das Internet zu senden. Ist dies nicht möglich, entfällt diese Alternative. Bei Problemen mit LDAP-Anfragen wenden Sie sich bitte an Ihre Netzwerkadministration.

- Ist die Verwendung des Siemens External Repository nicht möglich oder verfügt der Geschäftspartner nicht über ein Repository im Internet, müssen Zertifikate einzeln ausgetauscht werden.

4. Anleitungen: „Outlook Native Verschlüsselung“

4.1 Übermittlung von eigenen Zertifikaten an den Siemens-Partner

In diesem Abschnitt wird beschrieben, wie Sie einem Siemens Mitarbeiter eigene Zertifikate zur Verfügung stellen können.
Testen Sie bitte, ob der Siemens Mitarbeiter Ihnen eine verschlüsselte E-Mail schicken kann. Ist dies der Fall, so sind hier keine weiteren Aktionen notwendig, da dann direkt auf einen Verzeichnisdienst Ihrer Organisation zugegriffen werden kann.

Ist dies nicht der Fall, schicken Sie Ihrem Siemens-Partner bitte eine signierte E-Mail. Damit dieser aus dieser E-Mail auf Ihre Zertifikate zugreifen kann, überprüfen Sie bitte die folgenden Einstellungen:

- Öffnen Sie in Outlook das Menü Extras → Optionen und in der Lasche Sicherheit klicken Sie unter *„Verschlüsselte Nachrichten“* auf Einstellungen. (Ab Outlook 2007: Extras → Vertrauenseinstellungscenter→ E-Mail-Sicherheit)
- Im folgenden Fenster „*Sicherheitseinstellungen ändern*“ aktivieren Sie die Option „*Signierten Nachrichten diese Zertifikate hinzufügen*“.
- Schließen Sie alle Fenster durch Bestätigung mit OK.
- Schicken Sie dann eine signierte E-Mail an Ihren Siemens-Partner. In einer solchen E-Mail sind jetzt automatisch alle Zertifikate, die zur sicheren Kommunikation mit Ihnen benötigt werden, enthalten.

4.2 Übermittlung von Siemens-Zertifikaten an den Geschäftspartner

4.2.1 Verwendung des Siemens Externen Repositories oder des HTTP-Verzeichnisdienstes der European Bridge-CA

4.2.1.1 Siemens Root Signing

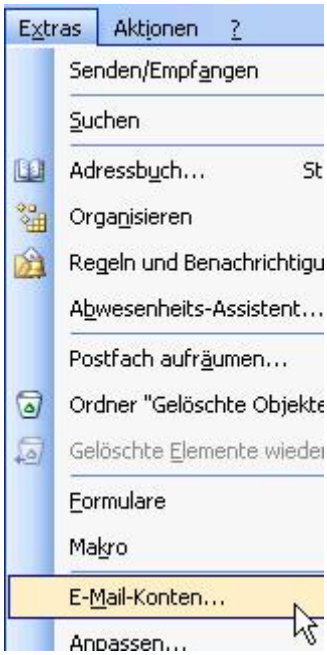
Root Signing Zertifikate sind Zertifikate die genutzt werden können um andere Zertifikate zu signieren, welche zu einem vertrauenswertem Root Zertifikate verknüpft sind. Da Siemens seine eigene Certification Authority besitzt, sind im normallfall die Zertifikate von Siemens Mitarbeitern bei Geschäftspartnern gültig.

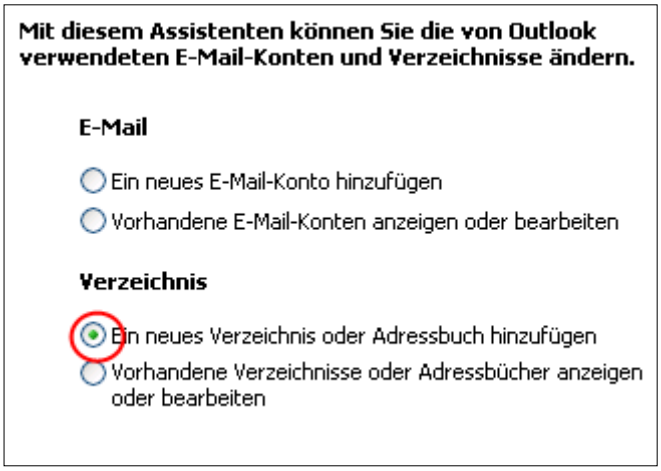
4.2.1.2 Einbinden des Siemens External Repository

Die Verwendung des Siemens External Repository wird grundsätzlich für die sichere Kommunikation mit Siemens empfohlen. Dadurch kann direkt auf die aktuellen Zertifikate aller Siemens Mitarbeiter von außen zugegriffen werden. Auch ist nach der einmaligen Einrichtung kein weiterer Schlüsselaustausch notwendig. Die Einbindung des Repositories muss durch Ihre Firewall erlaubt sein.

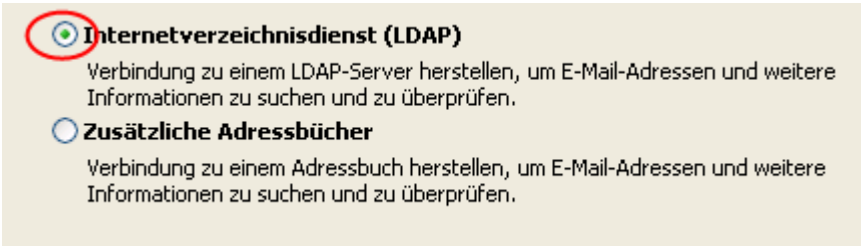
Zur Einbindung gehen Sie bitte folgendermaßen vor:

- Öffnen Sie in Outlook Extras → E-Mail Konten.
  (Ab Outlook 2007: Extras→Kontoeinstellungen der Reiter *Adressbücher*)
- Wählen Sie den Radio-Button *„Ein neues Verzeichnis oder Adressbuch hinzufügen“*.
  (Ab Outlook 2007: „*Neu*...“)

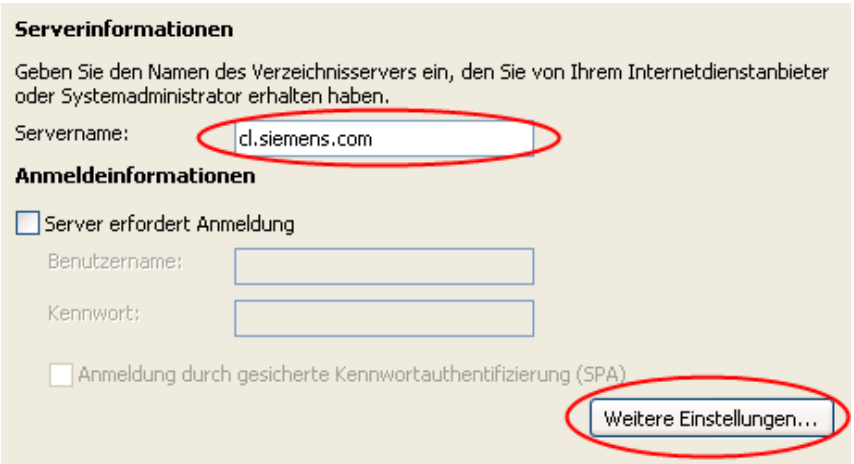




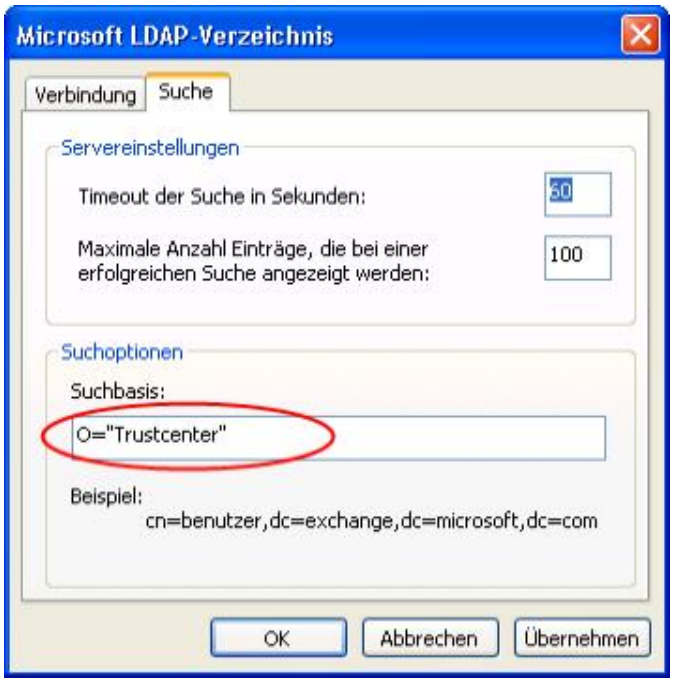
- Wählen Sie *„Internetverzeichnisdienst (LDAP)“.*



- Als Servername geben Sie *„cl.siemens.com“* ein. Klicken Sie dann auf *„Weitere Einstellungen...“*

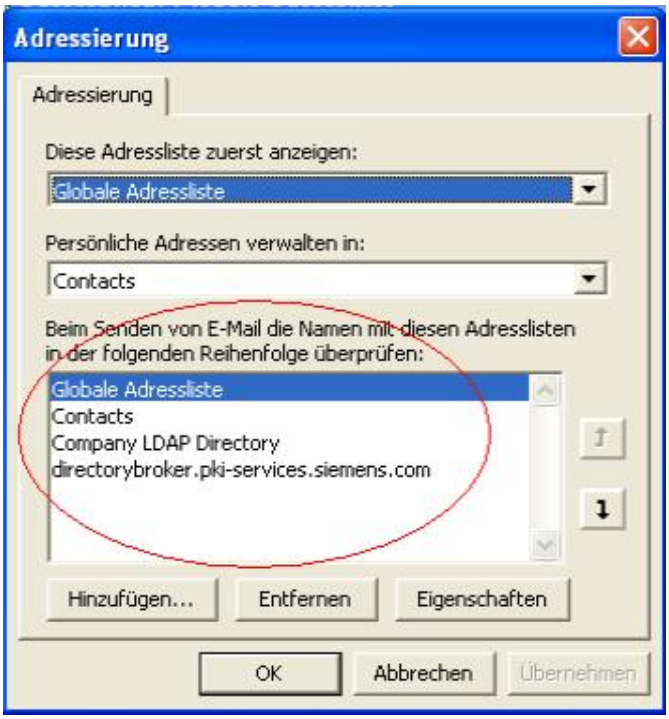


- Unter *„Suchoptionen“* im Reiter *„Suche“* geben Sie als Suchbasis: *O="Trustcenter"* ein.
- Weiter mit *OK*.
- Klicken Sie im vorherigen Fenster auf *Fertigstellen*.
  Hinweis: Es ist ein Neustart von Outlook notwendig, um den Verzeichnisdienst zu nutzen.



- Zum Schluss ist es notwendig, dass die Verzeichnisdienste in der richtigen Reihenfolge im Adressbuch eingetragen sind. Bitte öffnen Sie ihr Adressbuch
- Klicken Sie auf „Extras“ und dann auf „Optionen“
  (Ab Outlook 2007: Extras →Kontoeinstellungen im Reiter *Adressbücher*)

- Vergewissern Sie sich dass die Dienste in der richtigen Reihenfolge sind



4.2.1.3 HTTP Verzeichnis oder European Bridge CA

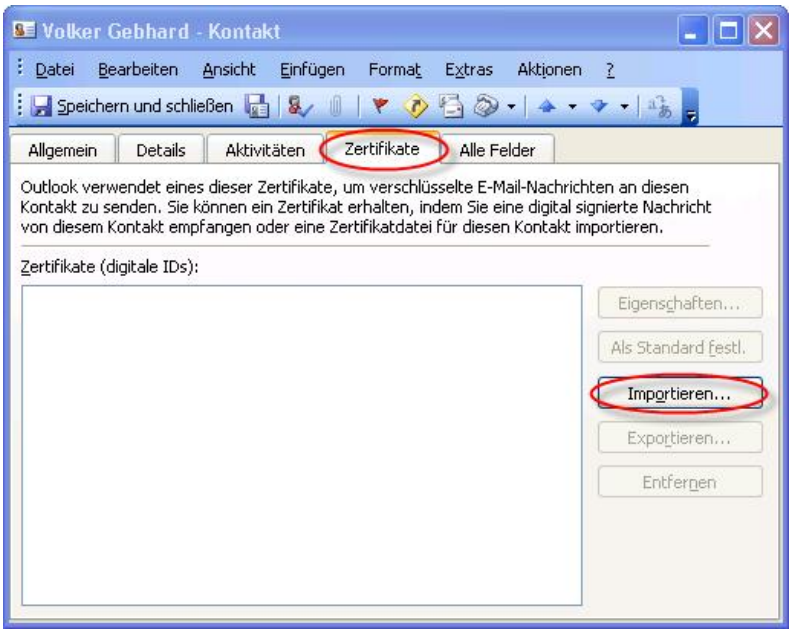
Alle Zertifikate von Siemens Mitarbeitern können unter folgendem Link heruntergeladen werden: http://cl.siemens.com

Darüber hinaus ist Siemens Mitglied der European Bridge CA. Daher können die Zertifikate aller Siemens Mitarbeiter auch über den HTTP-Verzeichnisdienst der Bridge CA heruntergeladen werden.
Der HTTP-Verzeichnisdienst der Bridge CA ist unter https://www.ebca.de/tools/zertifikate-finden/ erreichbar.

Suchen Sie dort nach der E-Mailadresse des gewünschten Siemens-Mitarbeiters und speichern Sie die angebotenen Zertifikate an einem beliebigen Ort auf Ihrem Computer. Es ist dabei notwendig, alle angebotenen Zertifikate zu speichern.

Falls die gespeicherten Zertifikate .crt-Dateien sind, ist es wichtig die sie in .cer-Dateien umzubenennen, da sie sonst nicht von unterstützt werden.

Damit Outlook die im vorherigen Schritt abgespeicherten Zertifikate verwenden kann, müssen diese einem Outlook-Kontakt zugeordnet sein. Gehen Sie dazu wie folgt vor:



- Öffnen Sie in Ihren Outlook-Kontakten den entsprechenden Kontakt des Siemens-Partners, mit dem Sie sicher kommunizieren wollen.
- Wählen Sie den Reiter *„Zertifikate“* und klicken sie auf Importieren.
- Wechseln Sie in das Verzeichnis, in dem Sie das Zertifikat des Siemens-Partners gespeichert haben und markieren Sie dieses zum Importieren.
- Verlassen Sie den Kontakt über *Speichern* und *Schließen*.
- Wiederholen Sie dies für alle Siemens-Partner, mit denen Sie sicher kommunizieren möchten.

4.2.2 Manueller Austausch mittels signierter E-Mail

Kann die European Bridge CA nicht verwendet werden, so bitten Sie Ihren Partner bei Siemens, eine von ihm signierte E-Mail zu schicken, in der seine Zertifikate enthalten sind.

Nachdem sie die signierte E-Mail bekommen haben, sollten Sie verschlüsselt mit dem Siemens Mitarbeiter kommunizieren können. Im Normallfall sind keine weiteren Schritte nötig. Falls eine Meldung „Digitale Signatur: Ungültig“ erscheinen sollte, folgen Sie bitte folgender Beschreibung.

Gehen Sie nach Erhalt der signierten E-Mail folgendermaßen vor:

- Beim Öffnen einer signierten E-Mail, deren Root-CA-Zertifikate noch nicht importiert wurden, öffnet sich dieses Fenster:

- Um die in der E-Mail übermittelten CA-Zertifikate zu importieren, klicken sie auf *Vertrauen*. Es erscheint eine *„Sicherheitswarnung“* die Sie auffordert, den Fingerprint des Zertifikats zu überprüfen.

- Klicken Sie auf *Ja*, um das Zertifikat in den Windows Certificate Store zu kopieren.
- Klicken Sie mit der rechten Maustaste auf den Absender der E-Mail.

- Wählen Sie den Menüpunkt *„Zu Outlook-Kontakten hinzufügen“*. Daraufhin öffnet sich die Kontakt-Maske mit den Daten des Senders. Überprüfen Sie, ob in der Lasche *„Zertifikate“* das Zertifikat des Senders importiert worden ist.
- Verlassen Sie den Kontakt über *Speichern* und *Schließen*.
- Wiederholen Sie dies für alle Geschäftspartner, mit denen Sie sicher kommunizieren möchten.

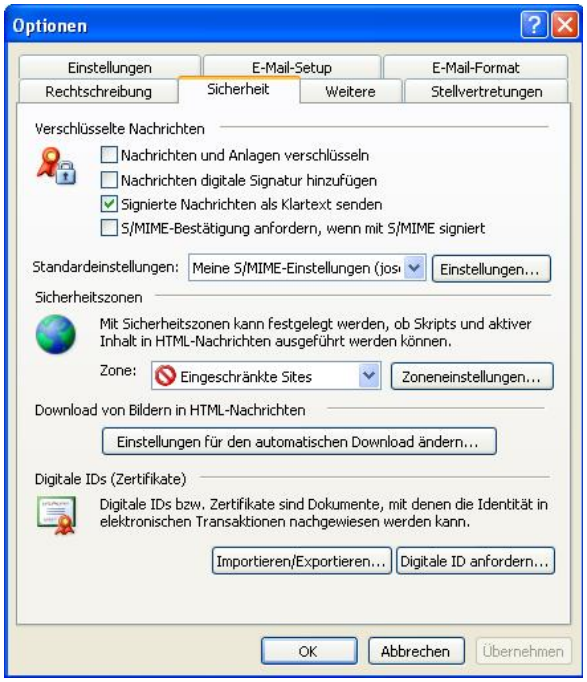
Hinweis: Die Signaturen der Geschäftspartner werden erst nach erneutem Öffnen der E-Mail als gültig angezeigt.

5. Abschließende Einstellungen in Outlook bei Erstbenutzung

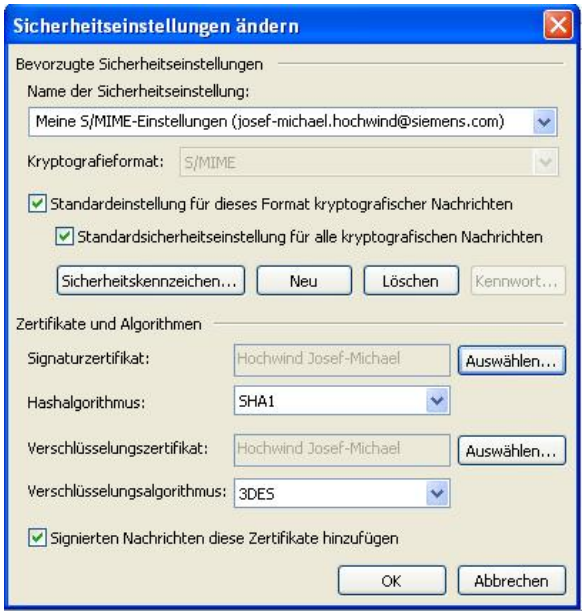
Um die E-Mail Verschlüsselung jetzt nutzen zu können, muss noch das richtige Zertifikat und das geeignete Verschlüsselungsverfahren ausgewählt werden. Bitte beachten Sie, dass Sie dieses Kapitel ignorieren können, wenn Sie schon E-Mail-Verschlüsselung auf Ihrem System eingerichtet haben und nutzen.

Bitte gehen Sie folgendermaßen vor:

- Starten Sie Outlook
- Unter Extras → Optionen finden Sie unter dem Reiter „*Sicherheit*“ Informationen für das Senden verschlüsselter Nachrichten. Klicken Sie auf „*Einstellungen*“ das neben „*Meine S/MIME-Einstellungen*“ zu finden ist. (Ab Outlook 2007: Extras → Vertrauenseinstellungscenter im Reiter „*E-Mail-Sicherheit*“)



- Wählen Sie neben „*Signaturzertifikat*“ das Ihnen vorgeschlagene Zertifikat aus. Danach wählen Sie einen Verschlüsselungsalgorithmus. Von Siemens wird hier der Algorithmus „*3DES*“ vorgeschrieben. Bestätigen Sie Ihre Eingaben mit „*OK*“
  Falls „*3DES*“ nicht ausgewählt werden kann, kann es sein, dass eine schwächere Verschlüsselung als 128Bit gewählt wird. In diesem Fall kann die E-Mail von Siemens Mitarbeiter nicht geöffnet werden. Um dieses Problem zu lösen sollte sich Ihr IT Support an den Siemens IT Support wenden.



- Schließen Sie Outlook und starten es erneut, damit die Änderungen übernommen werden.