



E-Mail-Verschlüsselung mit Geschäftspartnern

(Anleitung für Siemens Mitarbeiter)

Datum: 13.07.2011
Dokumentenart: Anwenderbeschreibung
Version: 3.0
Autor: Redaktionsteam PKI

Inhaltsverzeichnis

1.	Zweck des Dokumentes:	3
2.	Voraussetzungen beim Geschäftspartner	4
2.1	Zertifikate und Standards:	4
2.2	Anforderungen an die Software:	4
3.	Anleitungen für Siemens Mitarbeiter.....	5
3.1	Übermittlung von Siemens-Zertifikaten an den Geschäftspartner.....	5
3.2	Übermittlung der Geschäftspartner-Zertifikate an Siemens	5
3.2.1	Siemens Directory Broker.....	5
3.2.2	Manueller Austausch mittels signierter E-Mail	6
3.3	Beantragung von Siemens Zertifikate für Geschäftspartner	7
4.	Mögliche Probleme durch ungenügende Verschlüsselung beim Geschäftspartner	8

1. Zweck des Dokumentes:

Diese Anleitung richtet sich an Siemens Mitarbeiter, die mit ihren externen Geschäftspartner verschlüsselte E-Mails austauschen 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.

Für den Geschäftspartner steht eine komplementäre Anleitung zur Verfügung, die an den ihm übergeben werden kann.

Bei Problemen wenden Sie sich bitte an Ihren Helpdesk. Eine Übersicht der Helpdesks bei Siemens finden Sie [hier](#)¹.

¹ https://cio.siemens.com/cms/ca/de/cs/sec/pki/pages/helpdesks_germany.aspx.

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.

2.2 Anforderungen an die Software:

Um mit X.509 Zertifikaten verschlüsseln zu können, muss das Mailprogramm des Geschäftspartners 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.

Bitte klären Sie mit Ihrem Geschäftspartner, ob die oben beschriebenen Voraussetzungen erfüllt sind.

3. Anleitungen:

3.1 Übermittlung von Siemens-Zertifikaten an den Geschäftspartner

In diesem Abschnitt wird beschrieben, wie ein Siemens Mitarbeiter seine Zertifikate Geschäftspartnern zur Verfügung stellen kann.

- Bei Verwendung des External Repositories oder einem Einzelaustausch über den HTTP-Verzeichnisdienst der European Bridge CA sind keine Aktionen notwendig, da der Geschäftspartner über beide Dienste direkt auf alle User-Zertifikate von Siemens zugreifen kann.
- Ist die Verwendung des External Repositories oder der Einzelaustausch über den HTTP-Verzeichnisdienst der European Bridge CA nicht möglich, schicken Sie Ihrem Geschäftspartner bitte eine signierte E-Mail. Damit dieser, durch diese E-Mail, auf Ihre Zertifikate zugreifen kann, überprüfen Sie bitte die folgenden Einstellungen:
 - Öffnen Sie in Outlook das Menü Extras→Optionen und klicken Sie in der Lasche Sicherheit im Bereich „*Verschlüsselte Nachrichten*“ auf Einstellungen.
 - 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 Geschäftspartner. In einer solchen E-Mail sind jetzt automatisch alle Zertifikate, die zur sicheren Kommunikation mit Siemens benötigt werden, enthalten.

3.2 Übermittlung der Geschäftspartner-Zertifikate an Siemens

3.2.1 Siemens Directory Broker

Der Directory Broker ist ein Proxy für spezielle Zertifikats-Suchanfragen, die auf dem Lightweight Directory Access Protocol (LDAP) basiert. Damit bildet der Directory Broker die Funktionalität eines „Outlook Adressbuches“ ab.

Überprüfen Sie, ob der Directory Broker bei Ihnen gesetzt ist. Gehen Sie hierzu in Outlook auf Extras→E-Mail-Konten→Vorhandene Verzeichnisse oder Adressbücher anzeigen oder bearbeiten. Wenn Sie im folgenden Fenster den Eintrag „*directorybroker.pki-services.siemens.com*“ sehen, ist der Directory Broker bei Ihnen konfiguriert.

Sollte dies nicht der Fall sein, so folgen Sie bitte dieser [Anleitung](#)² zur manuellen Einrichtung.

Bei Verwendung des Directory Brokers werden automatisch die Schlüssel Ihrer Geschäftspartner gefunden und zur Verschlüsselung verwendet, genau so, wie Sie dies im internen Mailverkehr über das SCD gewohnt sind. Dies ist jedoch nur möglich wenn

² https://cio.siemens.com/cms/cio/de/infosec/pki/Documents/directorybroker_oab.pdf

die Root-Zertifikate des Geschäftspartners bereits in der Siemens IT Infrastruktur gelistet sind.

Weitere Informationen zum Siemens Directory Broker, den angeschlossenen Geschäftspartnern und zum Meldeprozess für weitere Teilnehmer finden Sie auf der [CIT Web-Site](#)³.

3.2.2 Manueller Austausch mittels signierter E-Mail

Kann der Directory Broker nicht verwendet werden, so bitten Sie den Geschäftspartner, eine von ihm signierte E-Mail zu schicken, in der seine Zertifikate enthalten sind. Die notwendigen Einstellungen sind in der Anleitung für Geschäftspartner am Beispiel Outlook Native Verschlüsselung beschrieben.

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. Bitte überprüfen und bestätigen Sie diesen.



- 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.

³ https://cio.siemens.com/cms/cio/de/infosec/pki/Pages/pki_extcom_dirbroker.aspx

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

3.3 Beantragung von Siemens Zertifikate für Geschäftspartner

Falls ein Geschäftspartner über keine eigenen Zertifikate verfügt, besteht die Möglichkeit, dass er Siemens Zertifikate ausgestellt bekommen. Das muss der Siemens Mitarbeiter jedoch über „FIONA“ beantragen. Eine ausführliche [Anleitung](#)⁴ hierzu finden Sie im Siemens Intranet.

⁴https://workspace.cio.siemens.com/content/10002378/pki/FiOnA/docs/General%20Business%20Partner%20Certificates/GBP_guideline_applicant_en.pdf

4. Mögliche Probleme durch ungenügende Verschlüsselung beim Geschäftspartner

Siemens hat intern festgelegt, dass für die E-Mail Verschlüsselung mindestens eine 128Bit-Verschlüsselung genutzt werden muss.

Durch technische Schwierigkeiten kann es vorkommen, dass E-Mails, die mit einer schwächeren Verschlüsselung als 128Bit gesendet werden, von Siemens Mitarbeitern nicht gelesen werden können.

Dieses Problem kann nicht von Siemens gelöst werden. Zur Behebung ist es notwendig, dass der Geschäftspartner seine Verschlüsselung auf 128Bit umstellt.

Bitte wenden Sie sich dazu an Ihren IT Support. Nähere Informationen hierzu finden Sie [hier](#)⁵.

⁵https://pkisupport.siemens.com/imps_en/service/managed_pki_services/e_mail_verschlueselung/knowledge_base/verschlueselte_rc2_40bit_s_mime_x_509_emails_sind_nicht_lesbar.html