Andreas Köcher  
 Berlin, 12.06.2014

# Informationen zu S/MIME und CA

Dieses Dokument soll den aktuellen Stand der Überlegungen zum Einsatz von E-Mail Verschlüsselung bei der enadCo Media AG dokumentieren.

## Einsatz von S/MIME

Grundsätzlich gibt es 2 Standards, wenn E-Mailverschlüsselung eingesetzt werden soll, S/MIME und PGP. Die Verschlüsselungstechniken sind nicht kompatibel, theoretisch kann ein E-Mail mit S/MIME und PGP verschlüsselt werden, dann braucht es aber auch S/MIME und PGP zum Entschlüsseln.

Was die Sicherheit der Verschlüsselung angeht sind beide Standards absolut ebenbürtig. Die Unterschiede liegen primär in der Organisation und Verwaltung der Schlüsselzertifikate. Während PGP hier den Anwender selbst in der Verantwortung sieht und Austausch, Prüfung und Pflege durch den Anwender selber fordert, gibt es für S/MIME ein System von zentralisierter Schlüsselerstellung, Beglaubigung und Verwaltung. Dies wird als Trust-Center oder Certificate Authority (CA) bezeichnet.

Für S/MIME spricht die etwas einfachere Handhabung der Schlüsselzertifikate für den Anwender und die allgemeine Verbreitung in den E-Mail Clients. PGP wird allgemein als etwas sicherer eingestuft, da es keine öffentlichen Trust-Center benötigt, deren Sicherheit und Integrität immer wieder Gesprächsstoff bietet. Diese Kritik betrifft aber nur die Unterschriftsfunktion, die Verschlüsselung ist bei beiden Systemen gleich sicher.

In Unternehmen wird häufig S/MIME eingesetzt, da die erforderliche Verwaltung zentralisiert werden kann und weniger Kenntnisse bei jedem einzelnen Anwender erfordert. Zudem wird für die Verwendung des privaten Schlüssels standardmäßig kein weiteres Passwort verlangt.

## Privates CA vs. Öffentliches CA

S/MIME erfordert es, dass jeder Schlüssel durch ein CA bestätigt wird, bevor er als eingesetzt werden kann. Zur Bestätigung von Schlüsseln hat sich eine Reihe von Unternehmen etabliert, die diese Dienste kommerziell anbieten und deren Root-Zertifikate standardmäßig in allen Betriebssystemen bzw. E-Mail Client Software registriert sind. Beispiele für diese Unternehmen sind VeriSign oder Deutsche Post SignTrust. Diese Unternehmen bieten Schlüssel-Zertifikate in unterschiedlichen Klassen, üblicherweise

* Class 1: nur die Existenz der E-Mail Adresse ist geprüft.
* Class 2: Die Person hat sich durch einen Ausweis o.ä. identifiziert.
* Class 3: Eine vollständige Identitätsprüfung, in Deutschland z. B. durch POSTIDENT hat stattgefunden.
* Class 4: Ein persönlicher Kontakt mit Vorlage aller Dokumente ist erforderlich (wird wegen des Aufwands von keinem Provider angeboten).

Die Preise liegen etwa bei € 10,-- für Class 1 bis € 100,-- für Class 3 – Zertifikate pro Person und Jahr. Es gibt einen Anbieter für kostenlose Class 1 – Zertifikate (StartCom), der ist allerdings auch nicht auf allen Plattformen akkreditiert, d.h. dieses Root-Zertifikat muss ggf. nachinstalliert werden – dazu später.

Es gibt weiterhin eine nicht-kommerzielle, gemeinschaftsbetriebene Zertifizierungsstelle namens CAcert. Hier wird mit viel Aufwand die persönliche Authentifizierung bestätigt und dokumentiert, allerdings hat es dieser Ansatz bis heute nicht geschafft in die allgemeinen Listen der CA’s bei Microsoft oder Mozilla aufgenommen zu werden. Ein Schelm, wer vermutet, dass die Lobby sich nicht ein Millionengeschäft kaputt machen lassen wollen. Also auch dieses Root-Zertifikat muss nachinstalliert werden, wenn die Verwaltung über CAcert erfolgen soll.

Es bleibt die Möglichkeit, im Unternehmen ein eigenes CA für die E-Mail Verschlüsselung mit S/MIME aufzubauen. Die hierfür erforderliche Software gibt es auf jedem Linux-Rechner oder auch auf Windows-Enterprise-Servern. Dieses CA wird einmalig etabliert und kann dann beliebig viele Personen-Zertifikate für Mitarbeiter ausstellen, beglaubigen und auch verwalten.

Der Vorteil eines solchen Unternehmens-CA besteht darin, dass alle Aktivitäten direkt im Unternehmen durchgeführt werden können und eine hohe Authentifizierung gewährleistet wird, denn das Unternehmen kennt seine Mitarbeiter. Weiterhin entstehen keine laufenden Lizenzkosten und der Abwicklungsprozess kann einfach gehalten werden.

Der Nachteil eines Unternehmens-CA besteht darin, dass das Root-Zertifikat nicht in den Betriebssystemen bzw. E-Mail Client Software von Anbeginn an enthalten ist. Unternehmens-intern ist das kein wirkliches Problem, das Root-Zertifikat muss nur nachinstalliert werden, bzw. in die Installationsimages für neue Rechner aufgenommen werden. Etwas aufwändiger ist das Vorgehen bei Externen. Möchte man die E-Mail Verschlüsselung mit einem Externen Geschäftspartner einrichten, muss dieser zunächst das Root-Zertifikat unserer Unternehmens-CA in seinen Zertifikat-Speicher aufnehmen.

Das ist nicht kompliziert, ein Rechtsklick auf die Datei, die Auswahl „Zertifikat installieren“ und ein paar Bestätigungen installieren das Zertifikat beispielsweise unter Windows. Weder wir noch unserer Geschäftspartner geht damit ein Risiko ein, das Root-Zertifikat ist ein öffentlicher Schlüssel, den Jeder besitzen darf. Es bestätigt lediglich, dass die öffentlichen Zertifikate unserer Mitarbeiter tatsächlich aus unserem Unternehmen stammen, es sich also um unsere Mitarbeiter handelt.

Ein Beispiel für solch ein Unternehmens-CA ist bei Web.de zu finden. Web.de als großer E-Mail – Provider stellt für jede seiner Mail-Boxen ein S/MIME – Zertifikat zur Verfügung. Die Bestätigung dieser Zertifikate wird nur durch das CA von Web.de gewährleistet. Web.de tut das auf der Ebene eines Class 1 – Zertifikat, denn die Existenz der Mailbox und dessen Besitzers kann Web.de nachweisen.

Um das Root-Zertifikat von Web.de zu erhalten hat Web.de eine Web-Seite (<https://trust.web.de/>) installiert, von wo das Root-Zertifikat heruntergeladen werden kann. Diese Web-Seite ist natürlich SSL-geschützt, ansonsten aber relativ simpel.

## Zusätzliche Gedanken zur E-Mail Verschlüsselung mit S/MIME und Unternehmens-CA

### Outlook 2013 und S/MIME

Outlook verwendet als Speicher für die privaten S/MIME Zertifikate das Windows Zertifikate SnapIn certmgr.msc. Die Zuweisung der Zertifikate erfolgt in Outlook über „Datei – Optionen – TrustCenter – Einstellungen für das Trust Center“. Dort in E-Mail-Sicherheit wechseln und dann mittels „Importieren/Exportieren“ die .pfx-Datei importieren. Anschließend kann dieses Zertifikat in den Einstellungen dem E-Mail – Konto zugewiesen werden.

Sobald ein private Schlüssel zugewiesen ist, erscheinen in „Neuer E-Mail – Optionen – Berechtigung“ die Schalter für „Verschlüsseln“ und „Signieren“, es kann losgehen.

Outlook macht es seinen Anwendern etwas schwerer eine E-Mal Verschlüsselung mit S/MIME durchzuführen als andere E-Mail Clientsoftware. Grundsätzlich teilt man dem E-Mail-Partner seinen öffentlichen Schlüssel durch eine unterschriebene E-Mail mit. Das funktioniert in Outlook wie in allen anderen Clients. Das öffentliche Zertifikat der Unterschrift wird gespeichert und wenn dann noch das Root-Zertifikat des CA vorliegt auch als authentisch eingestuft.

In Outlook reicht das allerdings nicht aus, um dem Partner eine verschlüsselte E-Mail zurück zu schicken. Es muss zusätzlich für den Partner ein Kontakt erstellt werden und diesem Kontakt ebenfalls das öffentliche Zertifikat des Partners zugewiesen werden. Bis Outlook 2013 reichte es aus, hierfür mit Rechtsklick auf die E-Mailadresse in der Mail die Funktion „Kontakt erstellen“ bzw. bei einem bestehenden Kontakt „Kontakt ergänzen“ auszuführen.

Outlook 2013 übernimmt das S/MIME – Zertifikat nicht mehr bei der Kontakterstellung, stattdessen muss man umständlich in den Kontakt wechseln, Bei „Datenursprung anzeigen“ auf „Outlook (Kontakte)“ klicken und in diesem Formular unter „Anzeigen - Zertifikate“ das Zertifikat importieren.

Hierfür muss das Zertifikat als .cer-Datei vorliegen. Die folgenden Schritte sind also noch notwendig:

* In der unterschriebenen E-Mail auf das Unterschrifts-Symbol klicken –> digitale Signatur
* In digitaler Signatur auf Details klicken –> Eigenschaften der Nachrichtensicherheit
* In Eigenschaften der Nachrichtensicherheit den Signierer auswählen und Details anzeigen klicken 🡪 Signatur
* In Signatur auf Zertifikat anzeigen klicken🡪 Zertifikat anzeigen
* In Zertifikat anzeigen auf den Reiter Details wechseln und in Datei kopieren klicken 🡪 Zertifikat-Export-Assistent
* Weiter, DER-codiert-binär X509 (.CER) auswählen, weiter, Dateiname und Pfad bestimmen, weiter, fertigstellen

Und schon hat man das öffentliche Zertifikat, das dann dem Kontakt zugewiesen werden kann.

Ein weiteres Problem sind ist das Globale Adressbuch. Es sieht aber so aus, als wenn man Einem Eintrag aus dem Globalen Adressbuch auch einen lokalen Eintrag an die Seite stellen kann wo dann das Zertifikat hinterlegt wird. ***Muss noch getestet werden…***

Einen derartigen Umstand gibt es nur bei Outlook (2013). Alle anderen bekannten E-Mail Clients von Windows, Mac, Linux, I-OS oder Android sind wesentlich einfacher bei der Aufnahme neuer Partner Zertifikate bedienbar.

### Zugang des Unternehmens zu verschlüsselter E-Mail

Das Unternehmen braucht in jedem Fall einen Zugang zur Korrespondenz des Mitarbeiters. Anderenfalls könnten wichtige Informationen für das Unternehmen verloren gehen, wenn ein Mitarbeiter ausscheidet oder die Schlüsselinformationen verloren gehen.

Hier bietet da Unternehmens-CA einen weiteren Vorteil gegenüber der kommerziellen Lösung. Da die Schlüsselerstellung vollständig in der Hand des Unternehmens liegt, können Rohdaten gespeichert bleiben.

Die Schlüsselerstellung in einem CA wird in 3 Schritten vollzogen.

* Erzeugung des Schlüsselpaars als .pem-Dateien, mit vorläufigem Passcode
* Zertifizierung des Schlüssels mit Hilfe des privaten Root-Schlüssel
* Generierung des S/MIME Schlüsselpakets (.pfx-Datei) mit Hilfe des vorläufigen Passcodes und Erzeugung des Transport Passcode.

Das bedeutet, auch wenn die .pfx-Datei nicht gespeichert wird und der Transport Passcode nur beim Anwender bleibt, kann aus den .pem-Dateien und dem vorläufigen Passcode eine neue .pfx-Datei erzeugt werden. Das bedarf aber unbedingtem Vertrauen in die CA und höchstem Sicherheitsschutz der CA-Einrichtung. ***Muss noch getestet werden…***

### Änderung der Passcode

Für S/MIME wird der private Schlüssel in der .pfx-Datei mit einem Transport Passcode gesichert. Nach dem Import in den Certifikate Store ist kein Passwort zur Nutzung des privaten Schlüsseln mehr erforderlich. ***Zu Testen ist***, welches Passwort verlangt wird, wenn der S/MIME – Betrieb auf „Höchste Sicherheit“ geschaltet wird, oder ob dann ein individuelles Passwort vergeben werden kann.

Hier ist S/MIME deulich anders als PGP, wo immer ein Passphrase bei der Nutzung des privaten Schlüssels verlangt wird.

### Einbindung oder Einsatz von Windows-Server als CA

***Muss noch getestet werden…***