Net at Work
Building IT-Excellence.

Auswahl von Zertifikaten für E-Mail Verschlüsselung

Author: Stefan Cink

Das E-Mail Gateway NoSpamProxy Encryption bietet die automatisierte Signatur und Verschlüsselung für E-Mails auf Basis der Standards S/MIME und PGP an. In diesem Whitepaper wird die Auswahl der richtigen Zertifikate beschrieben, die für die S/MIME basierte Signatur und Verschlüsselung benötigt werden.

Was sind Zertifikate?

Für das Signieren und Verschlüsseln werden sogenannte „Zertifikate“ benötigt. Mit dem Begriff „Zertifikat“ wird hier ein Schlüsselpaar beschrieben, welches aus einem privatem und einem öffentlichen Schlüssel besteht. Der private Schlüssel wird für das Signieren und Entschlüsseln von E-Mails verwendet. Der öffentliche Schlüssel hingegen wird von Kommunikationspartnern verwendet, um E-Mail Signaturen auf ihre Gültigkeit zu prüfen und um Nachrichten zu verschlüsseln.

Die beiden Schlüssel bilden eine mathematische Einheit, und stellen die passenden Umkehroperationen für einander dar. Der private Schlüssel rechnet beispielsweise immer +1, während der öffentliche Schlüssel grundsätzlich -1 rechnet. Das „Zertifikat“ als solches beinhaltet weiterhin Informationen über seinen Eigentümer, den Verwendungszweck und die Vertrauenswürdigkeit des Zertifikates.

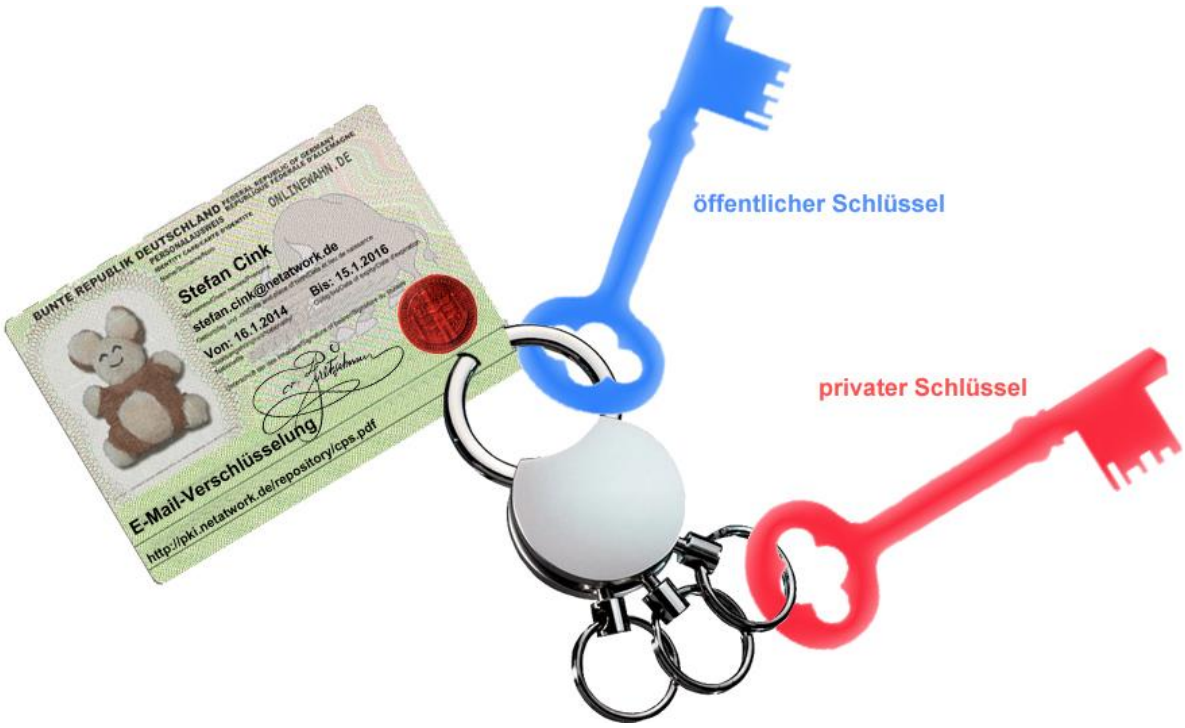

Abbildung 1:Beispielhafte Darstellung eines Zertifikats

Die Rolle der Trustcenter

Üblicherweise werden die Schlüssel auf dem Computer generiert, der sie später auch verwenden wird. NoSpamProxy Encryption hat einen entsprechenden Schlüsselgenerator bereits integriert. Die erzeugten Schlüssel müssen nun noch von einer Zertifizierungsstelle signiert werden. Dies entspricht

der Ausstellung eines Personalausweises in Ihrem zuständigen Einwohnermeldeamt. Das Amt bestätigt Ihre Identität. Bei Zertifikaten übernehmen dies Zertifizierungsstellen oder auch Trustcenter genannt. Das Trustcenter bestätigt mit seiner Unterschrift, dass das Zertifikat einer bestimmten Person oder Organisation gehört. Die Angaben des Antragstellers werden mittels verschiedener Verfahren überprüft. Je nachdem wie streng diese Prüfung ausfällt, werden Zertifikate der Klasse 1, 2 oder 3 ausgegeben.

Bei Zertifikaten der Klasse 1 wird nur eine E-Mail an den Antragsteller verschickt, die dann bestätigt werden muss. Für ein Klasse 2 Zertifikat, hat der Antragsteller eine Kopie eines Lichtbildausweises an die Zertifizierungsstelle geschickt. Die strengste Prüfung erfolgt bei Klasse 3 Zertifikaten. Hier wird in Deutschland zur Identifizierung des Antragstellers unter anderem das POSTIDENT-Verfahren eingesetzt. Der Antragsteller war demzufolge persönlich vor Ort.

Damit Kommunikationspartner einer E-Mail Signatur sofort vertrauen, sollte diese mit einem „offiziellen“ Zertifikat signiert werden. „Offiziell“ bedeutet hierbei, dass der E-Mail Empfänger dem ausstellenden Trustcenter vertraut, d.h. sich darauf verlassen kann, dass die Identität des Zertifikats-Eigentümers genau geprüft wurde. Dieses „Vertrauen“ wird erreicht, indem auf dem PC des Empfängers vertrauenswürdige Trustcenter durch Ihre sogenannten Root-Zertifikate hinterlegt sind. Mit dem Betriebssystem Windows werden solche Root-Zertifikate für einige Trustcenter bereits standardmäßig ausgeliefert.

Dies ist z.B. für SwissSign, GlobalSign oder D-Trust gegeben. Natürlich kann ein Kommunikationspartner auch anderen Trustcentern vertrauen und diese in seinem PC hinterlegen. Dies kann aber nur über die persönliche Absprache erfolgen.

Gateway- oder Personenzertifikat

E-Mail Zertifikate werden immer für eine konkrete E-Mail Adresse ausgestellt, d.h. genau genommen benötigt jeder Anwender ein eigenes Zertifikat. Eine Besonderheit stellen Gateway-Zertifikate bzw. Domain-Zertifikate dar, die z.B. auf die Adresse gate@netatwork.de ausgestellt werden. Diese Gateway-Zertifikate können für die Signatur aller E-Mails einer E-Mail Domäne (z.B. netatwork.de) verwendet werden.

Obwohl der Einsatz von Gateway-Zertifikaten international standardisiert ist, können einige E-Mail Clients diese nicht richtig verarbeiten (z.B. Webmailer von web.de etc.) und erklären die damit erstellten Signaturen für ungültig. Ebenso können diese E-Mail Clients nicht auf Basis von Gateway-Zertifikaten verschlüsseln. Beispielsweise melden Outlook Express und Windows Live Mail Signaturen auf Basis eines Gateway-Zertifikates als ungültig. Microsoft Outlook stellt die Signatur als gültig dar, kann auf Basis eines Gateway-Zertifikates aber dennoch nicht verschlüsseln.

Eine weitere Besonderheit sind Team-Zertifikate. Diese sind auf E-Mail Adressen ausgestellt, die nicht direkt einer Person zugeordnet sind, z.B. vertrieb@netatwork.de. Wie bei den Gateway-Zertifikaten handelt es sich vor allem um eine kaufmännische Gestaltung der Trustcenter. Technisch gleichen diese Zertifikate Personenzertifikaten und können auch von den meisten E-Mail Clients korrekt verarbeitet werden, da in diesem Falle ja auch meist mit der gleichen Absender-Adresse, wie im Zertifikate versandt wird.

Folgende Tabelle stellt dar, welche Möglichkeiten sich dem Sender einer E-Mail bieten, abhängig von der beim Empfänger eingesetzten Software. „Signatur“ bedeutet dabei, ob der Empfänger die Gültigkeit der Signatur der E-Mail korrekt angezeigt bekommt (grün=ja, rot=nein). „Verschlüsselung“ kennzeichnet, ob der Empfänger in der Lage ist, auf Basis der erhaltenen Signatur verschlüsselt zu antworten.

Empfänger / Sender	Outlook Express Live Mail	Microsoft Outlook	S/MIME Gateway
Personen-Zertifikat	⇨Signatur ⇦Verschlüsselung	⇨Signatur ⇦Verschlüsselung	⇨Signatur ⇦Verschlüsselung
Team-Zertifikat	⇨Signatur ⇦Verschlüsselung	⇨Signatur ⇦Verschlüsselung	⇨Signatur ⇦Verschlüsselung
Gateway-Zertifikat	⇨Signatur ⇦Verschlüsselung	⇨Signatur ⇦Verschlüsselung	⇨Signatur ⇦Verschlüsselung

Abbildung 2:Übersicht E-Mail-Clients und Domain-Zertifikate

Die folgende Tabelle führt beispielhaft Anbieter von E-Mail Zertifikaten auf:

Anbieter	Typ	Klassen	
SwissSign	Person	2,3	Zertifikatsanforderung integriert in NoSpamProxy Encryption
GlobalSign	Person, Team, Gateway	1,2,3	Zertifikatsanforderung integriert in NoSpamProxy Encryption
D-Trust	Person, Gateway	2	Zertifikatsanforderung integriert in NoSpamProxy Encryption (demnächst)
StartSSL	Person (kostenfrei)	1	https://www.startssl.com/

Abbildung 3:Übersicht einiger Trustcenter

Die Kosten für ein Zertifikatspaket mit 25 bzw. 50 Zertifikaten mit einem Jahr Laufzeit stellen sich wie folgt dar:

Anbieter	25 Zertifikate	50 Zertifikate
SwissSign	Ab 651,00 €	Ab 779,00 €
GlobalSign	1.485€	2.790€
D-Trust	Noch nicht verfügbar	Noch nicht verfügbar

Abbildung 4:Preisbeispiel für Zertifikatspakete

Fazit

In der Praxis sind Gateway-Zertifikate kostengünstiger und einfacher zu verwalten und funktionieren gut mit Partnern, die auch eine Gateway-Verschlüsselungslösung einsetzen. In Einzelfällen wird es bei Kommunikationspartnern jedoch immer wieder zu Warnungen bei der Signaturprüfung kommen. Wird in der Regel viel mit Einzelpersonen oder Kleinunternehmen kommuniziert, bzw. wird die Vermeidung von Warnungen beim Partner angestrebt, sind Personenzertifikate vorzuziehen.

Wird mit sogenannten Sammel-E-Mail-Adressen gearbeitet, können Team-Zertifikate sinnvoll oder notwendig sein.

Alle Zertifikatstypen können mit NoSpamProxy Encryption auch gemischt eingesetzt werden. Die Software wird grundsätzlich das passende Zertifikat verwenden.