

Auswahl von Zertifikaten für E-Mail Verschlüsselung

Autor: Net at Work GmbH, Uwe Ulbrich, 05251-304-600, 2011, Version 23

Inhalt

Was sind Zertifikate?	1
Die Rolle der Trustcenter	1
Verschiedene Zertifikatstypen	2
Fazit	3

Das Gateway für E-Mail Verschlüsselung und –Signatur [enQsig®](#) bietet die automatisierte Signatur und Verschlüsselung für E-Mail auf Basis des Standards S/MIME an.

Was sind Zertifikate?

Für das Signieren und Verschlüsseln werden sogenannte „Zertifikate“ benötigt. Mit dem Begriff „Zertifikat“ wird hier ein Schlüsselpaar aus privatem und öffentlichem Schlüssel beschrieben. Das „Zertifikat“ beinhaltet weiterhin Informationen über seinen Eigentümer und die Vertrauenswürdigkeit des Zertifikates.

Das Schlüsselpaar wird einer Person oder Organisation zugeordnet. Der private Schlüssel wird für das Signieren und Entschlüsseln von E-Mails verwendet. Der öffentliche Schlüssel wird von Kommunikationspartnern verwendet, um E-Mail Signaturen auf ihre Gültigkeit zu prüfen und um Antworten zu verschlüsseln.

Die Rolle der Trustcenter

Das Zertifikat wird von einem Trustcenter - einer vertrauenswürdigen Organisation - ausgestellt und bestätigt, dass der öffentliche Schlüssel zu einer eindeutigen Person bzw. Organisation gehört. Das Trustcenter überprüft bei der Ausgabe, den Antragsteller auf seine Identität mittels verschiedener Verfahren. Je nachdem wie streng diese Prüfung ausfällt, werden Zertifikate der Klasse 1, 2 oder 3 ausgegeben. Bei der Klasse 1 wird nur eine E-Mail an den Antragsteller verschickt, die dann bestätigt werden muss. Bei Klasse 3 Zertifikaten wird in Deutschland zur Identifizierung des Antragstellers unter anderem das POSTIDENT-Verfahren eingesetzt.

Damit Kommunikationspartner einer E-Mail Signatur 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 ausgeliefert.

Dies ist z.B. für GlobalSign, SignTrust, TC Trustcenter oder D-Trust gegeben. Natürlich kann ein Kommunikationspartner auch anderen Trustcentern vertrauen und diese in seinem PC hinterlegen. Dies wird aber nur in Einzelfällen und über persönliche Absprachen sinnvoll sein.

Verschiedene Zertifikatstypen

E-Mail Zertifikate werden immer für eine konkrete E-Mail Adresse ausgestellt, d.h. genau genommen benötigt jeder Anwender ein eigenes Zertifikat. Eine Besonderheit sind Gateway-Zertifikate bzw. Domain-Zertifikate, die z.B. auf die Adresse gate@netatwork.de ausgestellt sind. 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 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 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. Hier 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, z.B. enQsig
Personen-Zertifikat	⇒ Signatur ⇐ Verschlüsselung	⇒ Signatur ⇐ Verschlüsselung	⇒ Signatur ⇐ Verschlüsselung
Team-Zertifikat	⇒ Signatur ⇐ Verschlüsselung	⇒ Signatur ⇐ Verschlüsselung	⇒ Signatur ⇐ Verschlüsselung
Gateway-Zertifikat	⇒ Signatur ⇐ Verschlüsselung	⇒ Signatur ⇐ Verschlüsselung	⇒ Signatur ⇐ Verschlüsselung

Folgende Anbieter stellen E-Mail Zertifikate aus:

Anbieter	Typen	Klassen	
GlobalSign	Person, Team, Gateway	1,2,3	GlobalSign bei Net at Work
SignTrust (Deutsche Post)	Person	2 (3)	Zertifikatsanforderung integriert in Gateway-Produkte
TC Trustcenter	Person, Team, Gateway	1, 2, 3	http://www.trustcenter.de
D-Trust	Person, Gateway	2	http://www.d-trust.de
Comodo CA Limited	Person		http://www.enterprisesssl.com
StartSSL	Person (kostenfrei)	1	https://www.startssl.com/?app=12

Die Kosten liegen beispielsweise für Zertifikate mit einem Jahr Laufzeit wie folgt:

Bezeichnung	Class	GlobalSign EUR pro Jahr
Personen-Zertifikat	1	12,--
Personen-Zertifikat	2 oder 3	69,--
Team/Gateway-Zertifikat	2 oder 3	196,--

GlobalSign Stand: 2/2011

Fazit

In der Praxis sind Gateway-Zertifikate kostengünstiger und einfacher zu verwalten und funktionieren gut mit Partnern, die auch eine Gateway-Verschlüsselungslösung einsetzen. Wird viel mit Einzelpersonen oder Kleinunternehmen kommuniziert, können zusätzlich Personenzertifikate notwendig sein.

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

Alle Zertifikatstypen können mit enQsig gemischt eingesetzt und über das Regelwerk für die entsprechende Verwendung konfiguriert werden.