Verwendung von S/MIME zur Verschlüsselung und Signatur von E-Mails

GINDAT GmbH

Wetterauer Str. 6
42897 Remscheid

Version: **1.3**
Status: **in Ablage**
Stand: **01.02.2017**
Autor: **Tobias Grünewald**

1 Inhaltsverzeichnis

2 Hinweise zu Nutzungsrechten

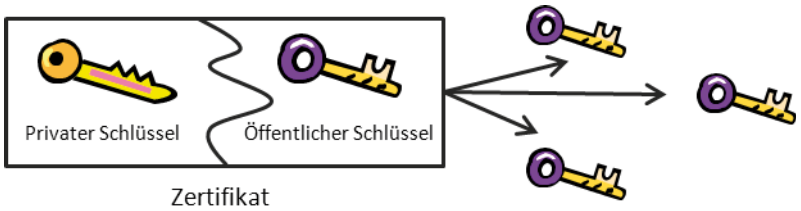
Verweise in diesem Dokument auf Websites Dritter werden nur gefälligkeitshalber zur Verfügung gestellt. Die Nutzung eines solchen Links erfolgt auf Ihre eigene Verantwortung. Die GINDAT GmbH hat nicht alle Websites Dritter kontrolliert und übernimmt für die dort vorgefundenen Inhalte keinerlei Haftung. Dies gilt ebenso für alle Ergebnisse, die durch die Benutzung von Websites Dritter erlangt werden können.

Alle verwendeten Warenzeichen, Produkt- oder Markenbezeichnungen, die hier dargestellt oder erwähnt sind, werden ohne Gewährleistung der freien Verwendbarkeit benutzt und sind möglicherweise eingetragene Warenzeichen.

3 S/MIME

Bei dem Begriff S/MIME handelt es sich um einen Standard für die Versendung verschlüsselter und signierter E-Mails. Fast alle gängigen E-Mail-Clients (z.B. Microsoft Outlook, Mozilla Thunderbird, Lotus Notes) unterstützen dieses Format in den aktuellen Versionen.

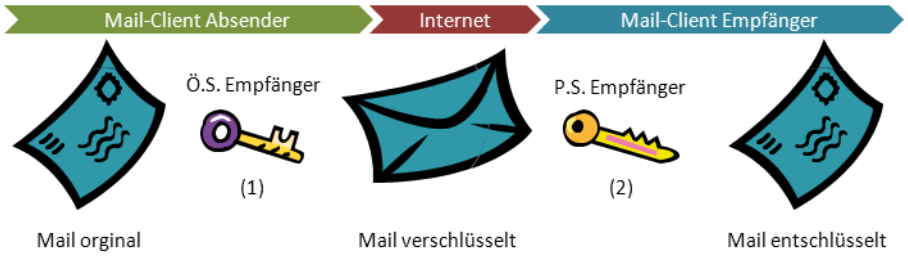
Sowohl die Verschlüsselung als auch die Signatur einer E-Mail werden mittels eines Public-Key-Verfahrens durchgeführt. Bei diesem asymmetrischen Verfahren werden immer zwei zueinander gehörende digitale Schlüssel verwendet (sogenannte Schlüsselpaare oder Zertifikate), ein „öffentlicher " und ein „privater" Schlüssel.



Der öffentliche Schlüssel wird an alle Kommunikationspartner verbreitet, der private Schlüssel verbleibt ausschließlich beim Besitzer der E-Mail-Adresse.

3.1 Verschlüsselte E-Mail

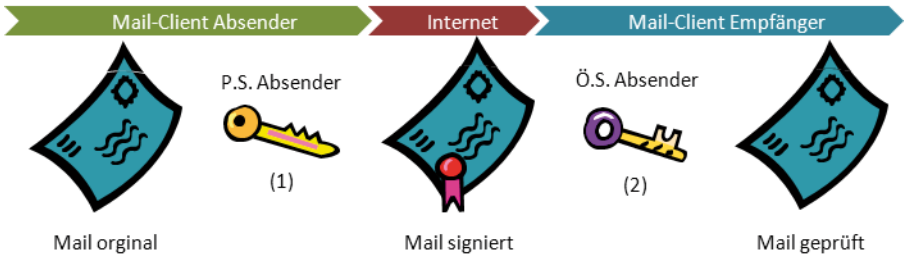
Der Inhalt einer Nachricht wird vom Absender mittels des öffentlichen Schlüssels der Empfänger-Adresse verschlüsselt und anschließend verschickt (1). Die Entschlüsselung der Mail ist dann nur noch mithilfe des privaten Schlüssels des Empfängers möglich (2). Dadurch ist sichergestellt, dass die Nachricht nur vom korrekten Empfänger gelesen werden kann und Unbefugte, die die Mail eventuell abfangen, diese nicht lesen können.



Der Empfänger benötigt also ein Zertifikat für seine E-Mail-Adresse, und muss dem Sender den öffentlichen Schlüssel dieses Paares zur Verfügung stellen.

3.2 Signierte E-Mail

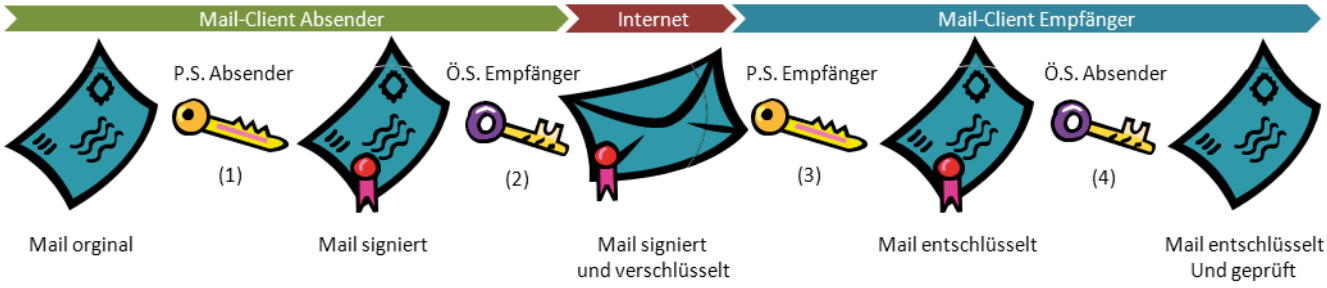
Hier wird der Inhalt der Mail im Klartext belassen, an die Mail wird aber eine digitale Signatur angehängt. Diese wird aus dem Inhalt der Nachricht sowie dem privaten Schlüssel des Absenders erzeugt (1). Der Empfänger kann dann mittels des öffentlichen Schlüssels des Senders verifizieren, dass die E-Mail auf dem Weg nicht verändert wurde und vom korrekten Absender stammt (2).



Der Absender einer signierten E-Mail benötigt also ein Zertifikat für seine E-Mail-Adresse und muss dem Empfänger seinen öffentlichen Schlüssel zur Verfügung stellen. Dies geschieht aber automatisch, da mit jeder signierten E-Mail eine Kopie des öffentlichen Schlüssels verschickt wird.

3.3 Signierte und verschlüsselte Mail

Die beiden genannten Verfahren können auch kombiniert werden. Hierbei wird die Mail zuerst mit dem privaten Schlüssel des Absenders signiert (1) und danach mit dem öffentlichen Schlüssel des Empfängers verschlüsselt (2). Der Empfänger nutzt seinen privaten Schlüssel zur Entschlüsselung (3) und anschließend den öffentlichen Schlüssel des Absenders, um die Mail zu prüfen (4).



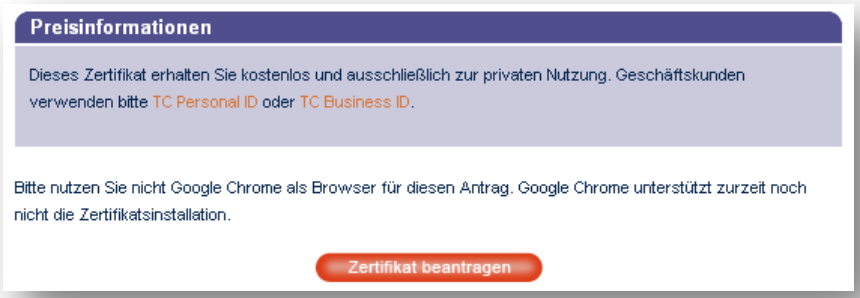
4 Eigenes Zertifikat beantragen und exportieren

Ein eigenes Zertifikat für Ihre E-Mail-Adresse müssen Sie dann beantragen, wenn Sie:
- signierte E-Mails verschicken wollen
- verschlüsselte E-Mails empfangen wollen

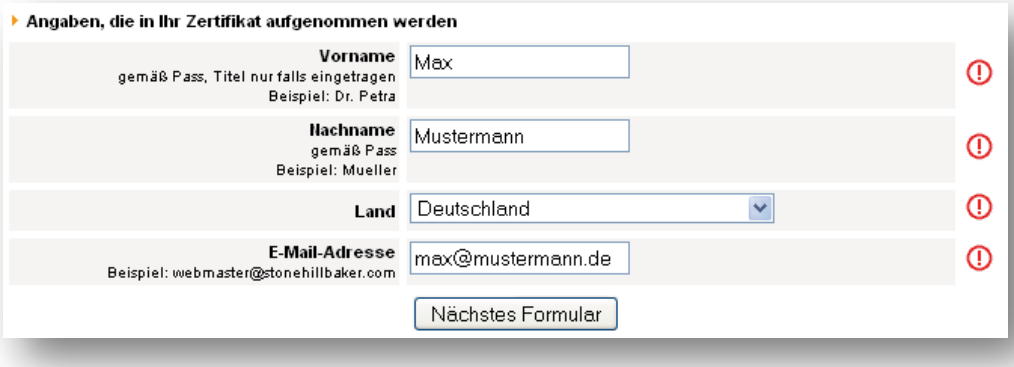
Im Folgenden wird beispielhaft die Vorgehensweise für die Beantragung eines Zertifikates bei Trustcenter beschrieben. Es gibt aber etliche weitere Aussteller von S/MIME Zertifikaten im Internet.

4.1 Kostenloses Zertifikat für den Privatgebrauch:

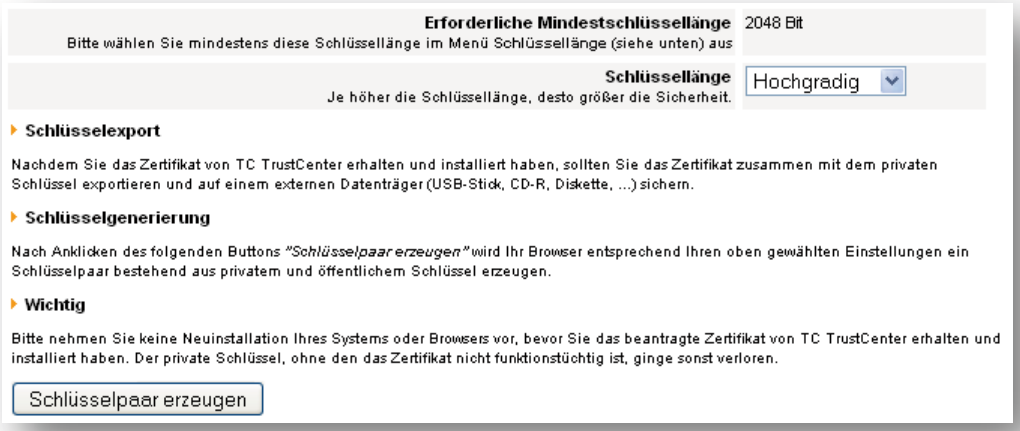
Begeben Sie sich auf http://www.trustcenter.de/products/tc_internet_id.htm und wählen Sie „Zertifikat beantragen“



Füllen Sie die folgenden Felder aus. Diese Informationen sind nachher für den Kommunikationspartner sichtbar.

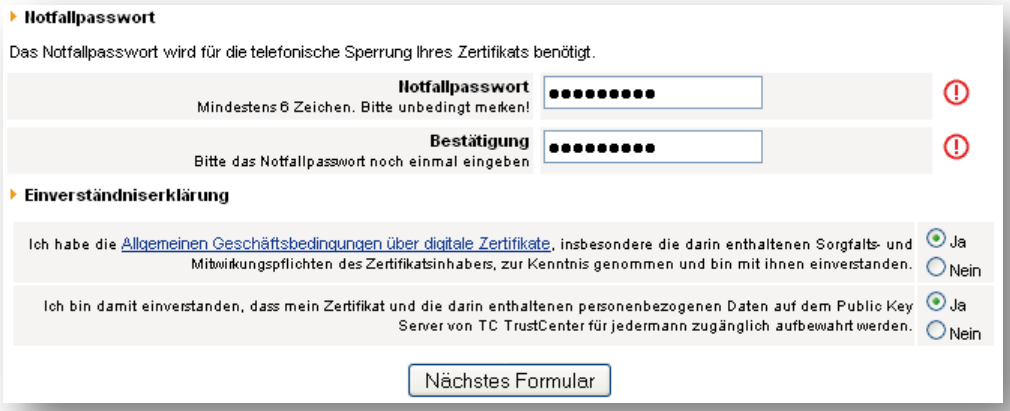


Wählen Sie als Schlüssellänge „Hochgradig“ aus und klicken Sie auf „Schlüsselpaar erzeugen“.



Die privaten Informationen für das Schlüsselpaar werden im Browser gespeichert. Aus diesem Grund dürfen Sie bis zum Abschluss des Vorganges Browser und Betriebssystem nicht neu installieren und müssen den Vorgang auch am gleichen Rechner und mit dem gleichen Browser abschließen, mit dem Sie ihn gestartet haben. Google Chrome wird momentan nicht unterstützt.

Im nächsten Dialog müssen Sie die AGBs akzeptieren und ein Notfallpasswort auswählen. Mit diesem können Sie Ihr Schlüsselzertifikat als ungültig kennzeichnen, wenn Ihr privater Schlüssel abhandenkommt.



Im nächsten Schritt erhalten Sie von Trustcenter eine E-Mail an die angegebene Adresse geschickt. Diese dient dazu, festzustellen, dass Sie auch tatsächlich unter der angegebenen E-Mail-Adresse erreichbar sind und nicht versuchen, Schlüssel für eine fremde Adresse zu erzeugen.

Die E-Mail enthält die weiteren Anweisungen. Sie müssen zur Bestätigung eine Antwortmail versenden, die die Auftrags-Nr. und eine Kontroll-Nr. enthält. Im Normalfall lässt sich dies direkt durch einen Klick auf den in der Mail enthaltenen Link ausführen.

Nach dem Versand der Bestätigung erhalten Sie eine zweite Mail, die den Auftrag abschließt. Diese enthält einen Link zu einer Webseite, welchen Sie im gleichen Browser aufrufen müssen, in dem Sie die Beantragung durchgeführt haben.

Mit einem Klick auf „Zertifikat installieren“ wird das Zertifikat im Zertifikatsspeicher Ihres Browsers installiert.

4.2 Kostenpflichtiges Zertifikat für geschäftliche Zwecke

Begeben Sie sich auf http://www.trustcenter.de/products/tc_personal_id.htm oder http://www.trustcenter.de/products/tc_business_id.htm und wählen Sie „Zertifikat kaufen“.

Die „Personal ID“ entspricht vom Inhalt her dem kostenfreien Zertifikat. Für die „Business ID“ werden zusätzliche Informationen über Ihr Unternehmen mit ins Zertifikat aufgenommen. Diese werden anhand von Dokumenten wie z.B. einem Handelsregisterauszug überprüft. Für die „Business ID“ gibt es zusätzlich die Option „Class 3“, bei der sich der Inhaber der E-Mail-Adresse mittels PostIdent-Verfahren ausweisen muss.

Für die Verschlüsselungsstärke ist es unerheblich, welches Zertifikat Sie verwenden. Die Zertifikate unterscheiden sich ausschließlich in den im Zertifikat enthaltenen Informationen. Das ausstellende Unternehmen Trustcenter bestätigt bei der „Business ID“ nicht nur die Echtheit der E-Mail-Adresse sondern auch die Zugehörigkeit zu Ihrem Unternehmen.

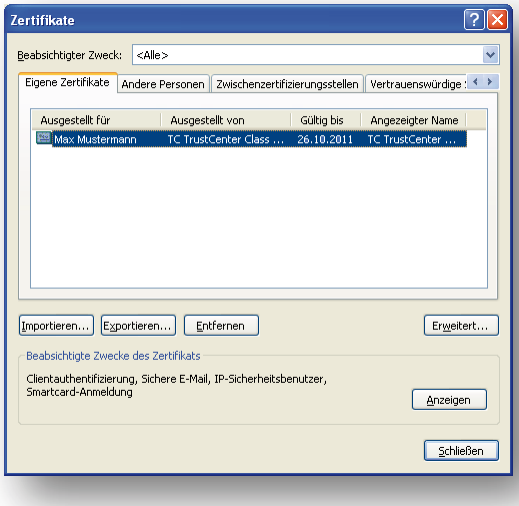
Die Beantragung verläuft analog wie die „Internet ID“ (Abschnitt 4.1), es müssen zusätzlich Zahlungsinformationen angegeben werden.

4.3 Zertifikat exportieren

Zur Verwendung in Ihrer E-Mail-Software muss das Zertifikat in eine Datei exportiert werden. Dies wird beispielhaft für die Browser „Internet Explorer“ und „Mozilla Firefox“ beschrieben.

4.3.1 Zertifikatsexport Internet Explorer

Wählen Sie im Internet Explorer im Menü „Extras“ den Punkt „Internetoptionen“. Unter dem Reiter „Inhalte“ findet sich der Punkt „Zertifikate“.



Markieren Sie Ihr Zertifikat und verwenden Sie den Button “Exportieren”, um es in eine Datei zu speichern. Dabei ist zu beachten, dass der private Schlüssel mit exportiert wird. Weiterhin ist es sinnvoll, alle Zertifikate im Zertifizierungspfad mit einzubeziehen. Die exportierte Datei sollte mit einem Passwort versehen werden, um den Zugriff Unbefugter auf Ihr Zertifikat zu verhindern.