E-Mail-Verschlüsselung mit S/MIME

17. November 2015

Inhaltsverzeichnis

1	Zertifikat erstellen	1
2	Zertifikat speichern	4
3	Zertifikat in Thunderbird importieren	6
4	Verschlüsselte Mail senden	8
5	Verschlüsselte Mail empfangen	8

In diesem Dokument wollen wir euch zeigen, wie ihr – am Beispiel von Firefox und Thunderbrid – ein S/MIME-Zertifikat erstellen könnt, mit dess Hilfe ihr und eure Freunde bequem verschlüsselte E-Mails austauschen könnt. Dazu sind drei Schritte notwendig:

- 1. Das Zertifikat erstellen.
- 2. Das Zertifikat aus Firefox exportieren.
- 3. Das Zertifikat in Thunderbrid importieren.

1 Zertifikat erstellen

Als erstes: Das Erstellen eines Zertifikates. Dabei wird ein privater und ein öffentlicher Schlüssel im Browser erzeugt. Der öffentliche Schlüssel wird zusammen mit einer E-Mail-Adresse, für die das Zertifikat gelten soll, an den Aussteller gesendet, der nun sicherstellen möchte, dass die E-Mail-Adresse auch der Person gehört, die die Anfrage stellt. Danach signiert der Aussteller – in unserem Beispiel Comodo – die Kombination aus E-Mail-Adresse und öffentlichem Schlüssel. Der private Schlüssel verlässt den Rechner nicht. Das Zertifikat von Comodo ist in der kostenlosen Variante ein Jahr gültig. Danach, kann ein neues, wiederum ein Jahr gültiges, erstellt werden.

Zum Erstellen dieses Zertifikats sind drei Schritte notwendig:

1. Besuchen Sie die Webseite

https://www.comodo.com/home/email-security/free-email-certificate.php

und klicken Sie auf $Sign\ up\ now:$

Internet Security Softwares PC Support & Maintenance	Free Secure Email Certificate 😝 Print Vie Email Certificate (SMIME) protects your emails with encrypting and digitally signing.
Email Security Free Email Certificate Antispam Gateway Personal Authentication Certificate	Want to keep your messages secure and private? Start protecting your digital communications with Comodo secure certificate • Digital signature ensures confidentiality • Secure message encryption • Protection against identity theft • Integrates with Microsofte Office and major applications
	Free Email Certificate Sign up now!

2. Das Formularfeld muss mit Name, Nachname und E-Mail-Adresse ausgefüllt werden. Das Zertifikat wird für die hier eingetragene E-Mail-Adresse erstellt. In dem Feld Key Size ist es empfehlenswert, den höchstmöglichen Wert auszuwählen. Je länger der Schlüssel ist, desto sicherer ist die Verschlüsselung.

			Secure Email Certificates
Application for §	Secure Email Certificate		Step 1: Provide details
Your Details			ior your certificate
First Name			Step 2: Collect and
Last Name			install your certificate
Email Address			
Country	Germany		
Private Key Options			
Key Size (bits):	Hochgradig 💌		
Note: Backup your private completing this application useless without it. <u>More infr</u> Revocation Passwo If you believe the security of passwort is required to an	key! We do not get a copy of your private key at any time so, aft procedure, we strongly advise you create a backup. Your certific a rd of your certificate has been compromised, it may be revoked. A re	er ate is evocation	
Revocation Password			
Comodo Newsletter	Opt in?		
you do not agree to the ter digital certificate.	ms of this Subscriber Agreement, do not apply for, accept, or use	e the	
Email Certificate	Subscriber Agreement	-	
THIS AGREEMEN THE AGREEMEN CONDITIONS.	IT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE READ T CAREFULLY BEFORE ACCEPTING THE TERMS AND		
IMPORTANT - PLI BEFORE APPLVI BY USING, APPLVI ACCEPTING THE ACKNOWLEDGE UNDERSTAND T BE BOUND BY IT CONDITIONS OF OR USE A COMO	EASE READ THESE TERMS AND CONDITIONS CAREFULLY IG FOR, ACCEPTING, OR USING A COMODO EMAIL CERTIFICATE (ING FOR, OR ACCEPTING A COMODO EMAIL CERTIFICATE OR BY SAGREEMENT BY CLICKING ON TACCEPT BELOW, YOU THAT YOU HAVE READ THIS LICENSE AGREEMENT, THAT YOU THAT YOU ACCEPT THE TERMS AS PESSITED, AND AGREE TO S TERMS. IF YOU DO NOT AGREE TO THE TERMS AND THIS SUBSCRIBER AGREEMENT, DO NOT APPLY FOR, ACCEPT, DO EMAIL CERTIFICATE AND CLICK "DECLINE" BELOW. ams		
1. Application of I	enne	-	
	ACCEPT the terms of this Subscriber Agreement.		

Das *Revocation Password* dient dem Widerruf des Zertifikats, wenn der geheime Schlüssel beispielsweise durch einen Virus / Trojaner in die falschen Hände geraten sein sollte oder die Zertifikatserstellung fehlgeschlagen ist. Hier möglichst eine ausreichend lange zufällige Zeichenfolge angeben und für den Verlustfall des Zertifikats aufheben. Wir empfehlen für das Speichern einen Passwordmanager wie zum Beispiel *KeePass*. Widerrufen werden kann das Zertifikat unter der folgenden Adresse:

```
https://secure.comodo.com/products/!SecureEmailCertificate_Revoke
```

Alle Eingaben mit Next > bestätigen

3. Daraufhin schickt COMODO eine E-Mail an die in Schritt zwei angegebene Adresse. Im Zweifelsfall könnte diese im Spamordner gelandet sein. Die E-Mail enthält einen Button zum bestätigen, dass die angegebene tatsächlich Ihnen gehört.

Congratulations - your Comodo FREE Personal Secure Email Certificate is now ready for collection! You are almost able to send secure email!

Simply click on the button below to collect your certificate.

Click & Install Comodo Email Certificate

Note:- If the above button does not work, please navigate to <u>https://secure.comodo.com</u> /<u>products/ISecureEmailCertificate_Collec2</u> Enter your email address and the Collection Password which is: 6Q8plrZtisFZehB7

Alternativ kann die unter dem Button stehende Webseite besucht werden. Durch Eingabe der E-Mailadresse und des *Collection Password* kann die Erstellung des Zertifikats ebenfalls abgeschlossen werden:

COMODO Creating Trust Online	
Collection of Secure Email Certificate Your Collection Details Your must enter these details to be authorized to collect your certificate. Email Address Collection Password Submit & Continue	Secure Email Certificates Step 1: Provide details for your certificate Step 2: Collect and install your certificate
© Copyright 2015. All rights reserved.	Monday June 29, 2015

2 Zertifikat speichern

Das jetzt fertig erstellte Zertifikat ist in Ihrem Browser gespeichert. Von dort muss es so gespeichert werden, dass es in Thunderbird importiert werden kann:

1. In Firefox (oben rechts) die Einstellungen öffnen:



2. Erweitert \rightarrow Zertifikate \rightarrow Zertifikate anzeigen

C Prierox aboucpren	een es-advanceu
0 Allgemein	Erweitert
Q Suche	Allasmain Dataniiharmittiung Natauark Hadata Zertifikata
📄 Inhalt	
🛕 Anwendungen	Wenn eine Website nach dem persönlichen Sicherheitszertifikat verlangt:
🗢 Datenschutz	O Automatisch eins wählen
🖴 Sicherheit	Jedes Mal fragen
🗘 Sync	✓ Aktuelle <u>G</u> ültigkeit von Zertifikaten durch Anfrage bei OCSP-Server bestätigen lassen
💩 Erweitert	Zertifikate anzeigen B Kryptographie-Module

3. In das Register *Ihre Zertifikate* wechseln, das COMODO-Zertifikat auswählen und auf *Sichern...* klicken:

ore haben Zertifikate dieser C Zertifikatsname	Kryptographie-Modul	en: Seriennummer	Läuft ab am	E
COMODO CA Limited				
COMODO CA Limited	das Software-Sicherheitsmodul	00:B3:61:1A:70:3F:6A:37:0	29.06.2016	

4. Im Speicherdialog den gewünschten Speicherort (z.B. in *Dokumente*) und Dateinamen (z.B. *E-Mail-Zertifikat-2015.p12*) wählen.

Dateiname für Backup				×
Computer •		• + ,	200	q
Organisieren 👻 Neuer Ordner			855	• •
👉 Eavoriten	A Name	^	Änderungsdatum	Тур
E Desktop				Privater
Downloads				Privater
Suletzt besucht				
	E			
🥽 Bibliotheken				
📔 Bilder				
Dokumente				
🚽 Musik				
🚼 Videos				
🐺 Computer				
Kokaler Datenträger (C:)				
🕞 Volume (D:)	+ K	ш		
Dateiname:	Zertifikiat_2015.p12			-
Dateityp: PKCS12-Dateien (*.	.p12)			-
 Ordner ausblenden 			Speichern Abb	rechen

5. Ein Passwort vergeben, mit dem das Zertifikat verschlüsselt werden soll, damit der private Schlüssel nicht im Klartext auf der Festplatte liegt. Dieses Passwort wird später wieder beim Importieren in Thunderbird benötigt.



6. Nun sollte das Zertifikat aus dem Browser gelöscht werden, da es hier unverschlüsselt abgelegt ist.

3 Zertifikat in Thunderbird importieren

Das in Firefox exportierte (gesicherte) Zertifikat muss nun in Thunderbird importiert werden.

1. Konto-Einstellungen öffnen (in der Windows-Version im Menü Extras zu finden):

ſ	
Server-Einstellungen Kopien & Ordner Verfassen & Adressieren Junk-Filter Synchronisation & Speicherplatz Empfangsbestätigungen (MDN) S/MIME-Sicherheit Lokale Ordner Junk-Filter Speicherplatz JacR Speicherplatz Postausgang-Server (SMTP)	S/MIME-Sicherheit Um verschlüsselte Nachrichten zu senden und zu empfangen, sollten Sie sowohl ein Zertifikat für Verschlüsselung als auch eines für digitale Unterschrift angeben. Digitale Unterschrift Folgendes Zertifikat verwenden, um Nachrichten digital zu unterschreiben: ✓ Nachrichten gigital unterschreiben (als Standard) Verschlüsselung Folgendes Zertifikat verwenden, um Nachrichten zu ver- und entschlüsseln: Standard-Verschlüsselungseinstellung beim Senden von Nachrichten: ④ Nie (keine Verschlüsselung verwenden) ● Ngtwendig (Senden nur möglich, wenn alle Empfänger ein Zertifikat besitzen) Zertifikate Zertifikate verwalten Kryptographie-Module verwalten
Konten-Aktionen •	OK Abbrehen

Hier das entsprechende Konto (linke Spalte) und darin den Unterpunkt S/MINME-Sicherheit auswählen. Auf der rechten Seite Zertifikate verwalten... klicken

2. In dem sich öffnenden Dialogfeld den Reiter *Ihre Zertifikate* wählen und *Importieren...* anklicken und anschließend die Datei auf der Festplatte aussuchen, die in Schritt 4 beim Speichern des Zertifikats erstellt wurde:

3. Wenn die Passwörter für die E-Mailkonten mit einem zentralen Master-Passwort verschlüsselt sind, muss dieses nun evtl. eingegeben werden. Sonst kommt direkt das nächste Dialogfeld.



In das Dialogfeld *Passworteingabe-Dialog* muss das Passwort eingegeben werden, das beim sichern aus Firefox vergeben wurde (Siehe Zertifikat speichern, Schritt 5).



4. Das Zertifikat taucht nun unter Ihre Zertifikate auf.

Kryptographie-Modul	Seriennummer La	iuft ab am 🛤
Software-Sicherheitsmodul	00:B3:61:1A:70 29	.06.2016
chen		
		ОК
	Kryptographie-Modul Software-Sicherheitumodul	Kryptographie-Modul Seriennummer Li Software-Sicherheitsmodul 0083611470 29

5. Um E-Mails signieren und entschlüsseln zu können, muss das Zertifikat noch für diese Nutzung ausgewählt werden. Sowohl bei *Digitale Unterschrift* als auch bei *Verschlüsselung* über den Button *Auswählen...*

A	S/MIME-Sicherheit		
Server-Einstellungen Kopien & Ordner Verfassen & Adressieren Junk-Filter Synchronisation & Speicherplatz	Um verschlüsselte Nachrichten zu senden und zu empfangen, sollten Sie sowohl ein Zertifi für Verschlüsselung als auch eines für digitale Unterschrift angeben. Digitale Unterschrift Folgendes Zertifikat verwenden, um Nachrichten digital zu unterschreiben: Auswählen		
S/MIME-Sicherheit			
Junk-Filter Speicherplatz JACR Speicherplatz Postausgang-Server (SMTP)	Verschlüsselung Folgendes Zertifikat verwenden, um Nachrichten zu ver- und entschlüsseln: Ausgehlen Lgeren Standard-Verschlüsselungseinstellung beim Senden von Nachrichten:		
	<u>Mie</u> (keine Verschlüsselung verwenden) <u>Ng</u> twendig (Senden nur möglich, wenn alle Empfänger ein Zertifikat besitzen) Zertifikate		
	Zertifikate verwalten Kryptographie-Module verwalten		
Konten-Aktionen *			

und das darauf hin erscheinende Dialogfeld

Zertifikat wäl	hlen		— ×
Zertifikat:	COMODO CA Limited ID von		-
Details des	gewählten Zertifikats:		
	(ОК	Abbrechen

das COMODO-Zertifikat auswählen.

4 Verschlüsselte Mail senden

Ob eine Mail signiert und / oder verschlüsselt werden soll, kann nun beim Erstellen der Mail ausgewählt werden.

合 Verfassen: (kein Betreff)	
<u>D</u> atei <u>B</u> earbeiten <u>A</u> nsicht <u>O</u> ptionen <u>Ex</u> tras <u>H</u> ilfe	
🎬 Später senden 🛛 🖋 Rechtschr. 🔻 関 Anhang 🔻	S/MIME 🔻 🖬 Speichern 🔻
Von:	✓ Nachricht <u>v</u> erschlüsseln
Antwort an:	✓ Nachricht <u>u</u> nterschreiben
- An:	Sicherheitsinformationen anzeigen
D	
Betrett:	

Nur an Empfänger, zu denen der private Schlüssel bekannt ist, können Mails auch verschlüsselt werden. Der einfachste Weg den eigenen privaten Schlüssel zu übertragen ist dem Kommunikationspartner eine signierte E-Mail zu schicken.

5 Verschlüsselte Mail empfangen

Ob eine Mail nun signiert und / oder verschlüsselt wurde, können Sie den Symbolen entnehmen die im Kopf der E-Mail angezeigt werden: $\fbox{}$ Um die Nachricht lesen zu können, müssen Sie nichts weiter tun. Thunderbird zeigt ihnen die Mail automatisch entschlüsselt an.