

E-Mail-Verschlüsselung mit S/MIME und Windows Live Mail



E-Mail-Verschlüsselung mit S/MIME und Windows Live Mail von Andreas Grupp ist lizenziert unter einer [Creative Commons Namensnennung - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz](#).

Für die Verschlüsselung mit S/MIME wird ein Schlüsselpaar benötigt, das von einer Stammzertifizierungsstelle¹ beglaubigt ist – der Beglaubigungsteil ist ein sogenanntes Zertifikat. Üblicherweise ist diese Beglaubigung kostenpflichtig. Einige wenige Stellen, bieten dies aber kostenfrei an. Für den **privaten Gebrauch** wird dies beispielsweise von Comodo angeboten. Unabhängig vom Einsatzgebiet bietet StartSSL² ebenfalls kostenfreie Zertifikate an.

U.a. bei diesen beiden Anbietern findet „nur“ eine sogenannte E-Mail-Validierung statt. Es wird also nur geprüft, ob der Antragssteller Zugriff auf das Mailkonto hat. Die Beglaubigung umfasst also auch nur diese Angabe.

Aufwändiger aber auch wesentlich vertrauenswürdiger, weil ein persönliches Treffen mit sogenannten Assuren erforderlich ist, ist CAcert³.

Da Comodo das vergleichsweise einfachste Verfahren anbietet, wird hier für die ersten „Gehversuche“ dieser Anbieter einführend verwendet.

S/MIME-Zertifikat / Free Secure Email Certificate von Comodo⁴

Windows Live Mail verwendet als Zertifikatsspeicher den in das Betriebssystem Microsoft Windows integrierten Zertifikatsspeicher. Das persönlich Zertifikat wird über einen Webbrower beantragt und muss, wenn es mit Windows Live Mail verwendet werden soll, in diesem betriebssysteminternen Zertifikatsspeicher installiert werden. Der einfachste Weg dies zu bewerkstelligen, ist die Nutzung des Microsoft Internet Explorers da auch dieses Produkt den gleichen Zertifikatsspeicher nutzt.

Starten Sie also die Anwendung Microsoft Internet Explorer und verwenden Sie diesen auch weiter unten um das Zertifikat bei Comodo, nach dessen Ausstellung, abzuholen.



Free Email Certificate
Sign up now!

Unter der in der [Fußnote angegebenen Adresse](#) beginnt der Beantragungsprozess durch einen Klick auf die nebenstehende dargestellte Schaltfläche.

1 Stammzertifizierungsstelle (engl. Certification Authority oder CA) ist so etwas wie ein Notar in der digitalen Welt. Die Stammzertifizierungsstelle, der digitale Notar, stellt Beglaubigungen aus.

2 <http://www.startssl.com/>

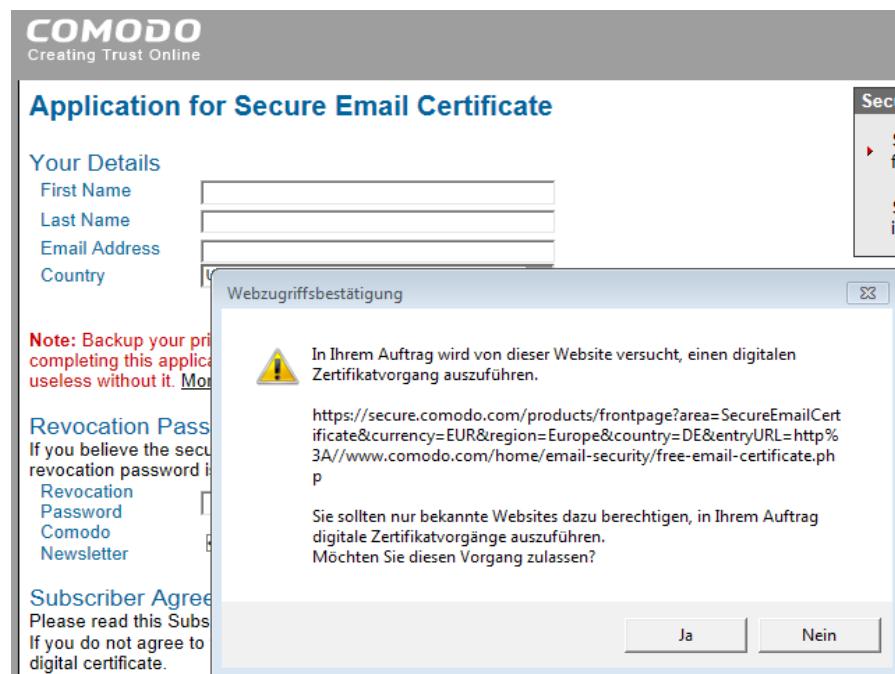
3 <http://www.cacert.org/>

4 <http://www.comodo.com/home/email-security/free-email-certificate.php> od. <http://tinyurl.com/freecert>



Die Website von Comodo wird nachfolgend Vorgänge auslösen, die Verschlüsselungszertifikate betreffen. Der Internet Explorer zeigt deshalb sofort eine Warnung und möchte von Ihnen die Erlaubnis für diese Vorgänge.

Bestätigen Sie den Vorgang durch einen Klick auf die Schaltfläche „Ja“.



Im nachfolgenden Formular füllen Sie die Felder „Vorname“, „Nachname“, „E-Mail-Adresse“ und „Land“ aus. Die Schlüsseloption belassen Sie auf „Hochgradig“ oder „2048 (High Grade)“ - je nach Browser.

Um ggf. das Zertifikat vorzeitig für ungültig zu erklären – eine Revocation – überlegen Sie sich für diesen Zweck ein Revocation-Passwort und tragen auch das ein.

Merken Sie sich dieses Revocation-Passwort, Sie benötigen es bei Verlust oder Kompromittierung Ihres Zertifikats!

Application for Secure Email Certificate

Your Details

First Name	Hans
Last Name	Mustermann
Email Address	smime-lfb@t-online.de
Country	Germany

Advanced Private Key Options...

Note: Backup your private key! We do not get a copy of your private key at any time so, after completing this application procedure, we strongly advise you create a backup. Your certificate is useless without it. [More info](#)

Revocation Password

If you believe the security of your certificate has been compromised, it may be revoked. A revocation password is required to ensure that only you may revoke your certificate:

Revocation Password	*****
Comodo Newsletter	<input type="checkbox"/> Opt in?

Wenn Sie den Comodo Newsletter nicht abonnieren möchten, entfernen Sie diese Option die standardmäßig gesetzt ist.

Im unteren Teil des Antragsformulars finden Sie den rechtlichen Teil des Antrags – eine Einverständniserklärung / Vereinbarung zwischen Ihnen und Comodo – der insbesondere hinsichtlich der Nutzung für Sie relevant ist. Die kostenfreien Zertifikate von Comodo dürfen nur für private Zwecke genutzt werden.

Diese Vereinbarung muss über das Setzen der ACCEPT-Option akzeptiert werden.

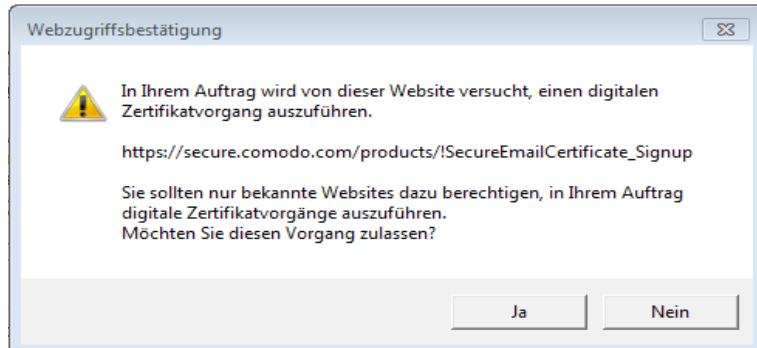
I ACCEPT the terms of this Subscriber Agreement.

Next >

Nach dem **Anklicken der Schaltfläche „Next >“** sendet Comodo einen Funktionsaufruf an Ihren Browser, damit dieser über eine eingebaute Cryptofunktion ein Schlüsselpaar erzeugt.

Insbesondere der geheime Schlüssel (einer der beiden Schlüssel des Schlüsselpaares) verlässt Ihren Rechner dabei nicht! Nur der öffentliche Schlüssel wird anschließend automatisch an Comodo zur Beglaubigung übermittelt.

Auch bei dieser Aktion wird auf den Zertifikatsspeicher zugegriffen. Die Warnmeldung bzw. die erbetene Bestätigung ist erneut mit „Ja“ zu bestätigen.



Nach erfolgreicher Durchführung dieser Aktion, teilt Ihnen die Comodo-Website mit, dass die Antragsstellung durchgeführt wurde und Sie nun eine E-Mail erhalten.



Dear Hans Mustermann,

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

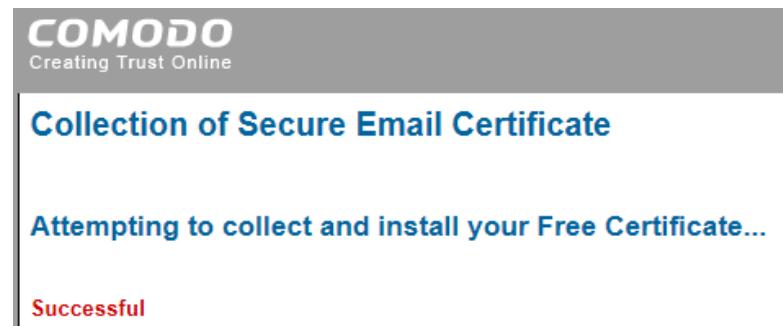
Mit dieser Mail, die Sie nach kurzer Zeit im Maileingang finden sollten, überprüft Comodo in einem Schritt, ob Sie das zugehörige Mailkonto abrufen können und teilt Ihnen mit, wo Sie die Beglaubigung abrufen können.

ACHTUNG: Es ist unbedingt erforderlich die nachfolgende Aktion mit dem gleichen Browser (hier war das der Microsoft Internet Explorer) durchzuführen, mit dem auch der vorige Schritt – die Beantragung des Zertifikats – durchgeführt wurde!!!

Klicken Sie zum Abruf des Zertifikats auf die Schaltfläche „Click & Install Comodo Email Certificate“. Die aufgerufene Seite auf der Comodo-Website übermittelt die Beglaubigung (das Zertifikat) und Ihr Browser fügt dies nun noch an Ihr bereits im Zertifikatsspeicher befindliches Schlüsselpaar an.

Erneut wird dabei auf den Zertifikatsspeicher zugegriffen und erneut möchte der Internet Explorer für diesen Vorgang eine Bestätigung von Ihnen haben. Erlauben Sie also auch diesen letzten Zugriff durch einen Klicke auf „Ja“.

Die erfolgreiche Transaktion wird Ihnen im Browser angezeigt. Fehlermeldungen dürfen dabei nicht auftreten.



Das Zertifikat ist nun im Zertifikatsspeicher des Betriebssystems Windows enthalten. Alle Anwendungen die ebenfalls diesen internen Speicher des Betriebssystems verwenden, haben nun ebenfalls Zugriff auf dieses Zertifikat. Die Anwendung *Windows Live Mail* ist, wie z.B. auch *Microsoft Outlook*, eine derartige Anwendung.

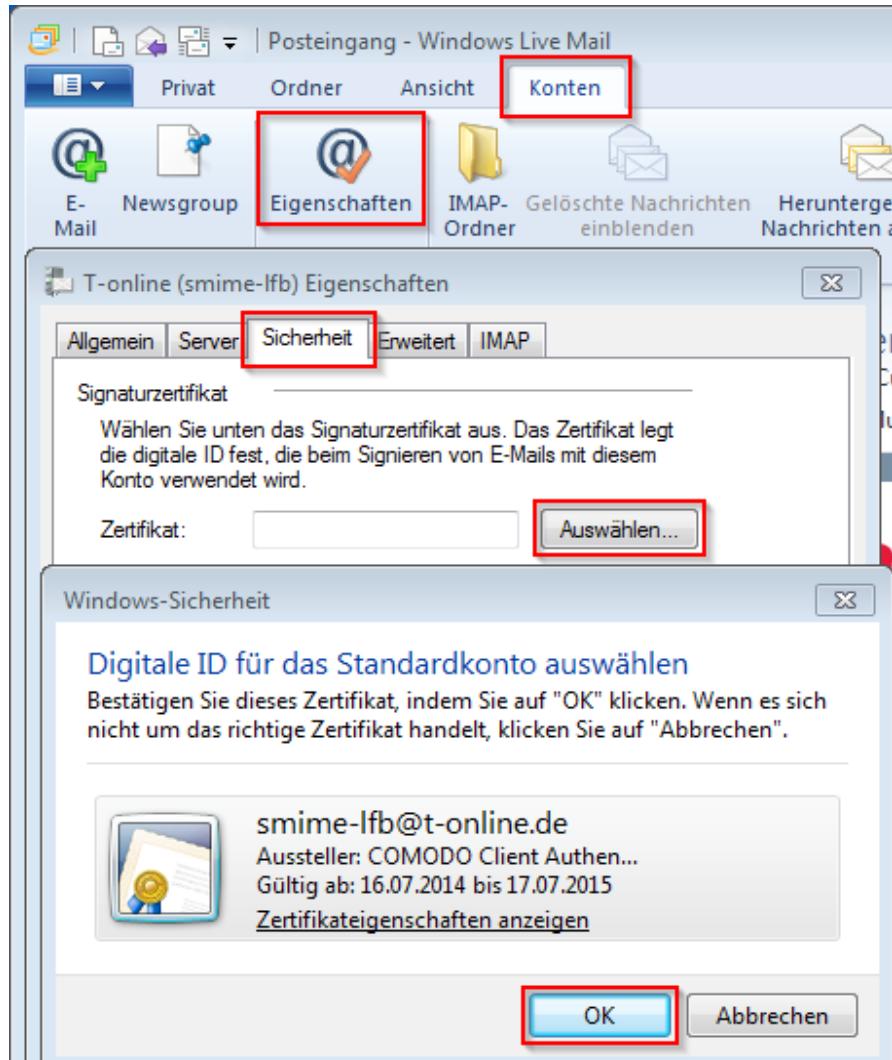
S/MIME-Konfiguration von „Windows Live Mail“

Starten Sie das bereits vorab mit Ihrem Mailkonto verknüpfte *Windows Live Mail* und wechseln Sie dort zu „Konten“.

Im Bereich „Konten“ wählen Sie „Eigenschaften“ um in die Konten-Eigenschaften ihres E-Mail-Kontos zu gelangen.

Unter der Registerkarte „Sicherheit“ klicken Sie beim Eingabefeld „Zertifikat“ auf die Schaltfläche „Auswählen“.

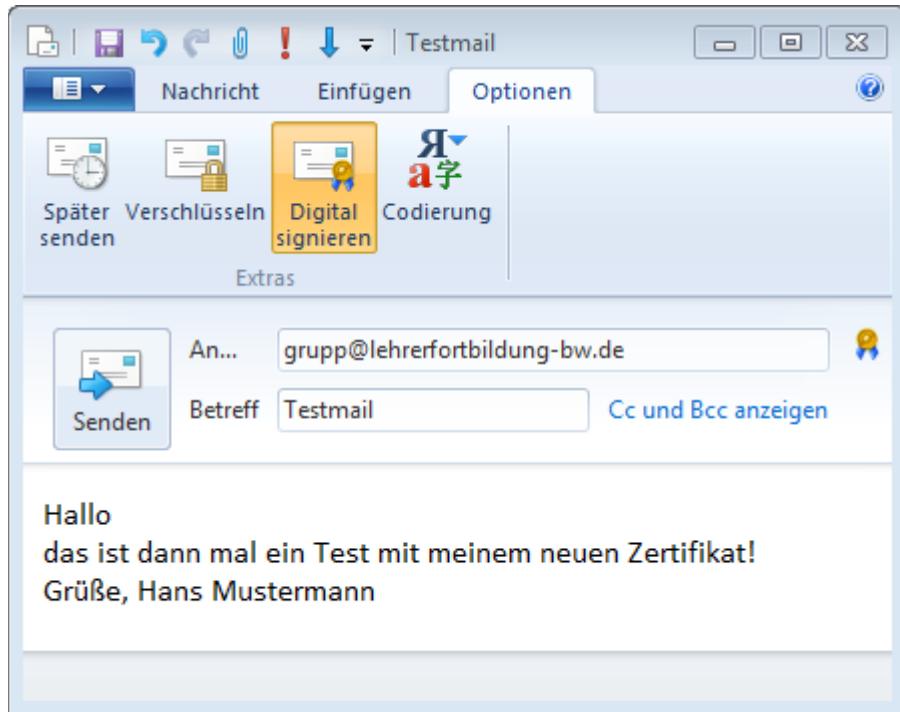
Es sollte nun automatisch das passende, im zentralen Zertifikatsspeicher befindliche S/MIME-Zertifikat angeboten werden. Wählen Sie dieses aus und bestätigen Sie die Verknüpfung zum Mailkonto mit „OK“.



Praktische S/MIME-Anwendung

Digital unterschriebene Mails

Verfassen Sie einfach erst einmal wie gewohnt eine neue Mail. Um die Mail digital zu signieren, wählen Sie zuerst die Registerkarte „Optionen“ und dort die Schaltfläche „Digital signieren“ aus.



Das war es schon – Sie können Ihre erste kryptographisch signierte Mail mittels der Schaltfläche „Senden“ absenden.



Ein Nebeneffekt von S/MIME ist übrigens, dass damit auch gleich das eigene Zertifikat (nur der für die Öffentlichkeit bestimmte Anteil) an den Empfänger übermittelt wird⁵.

Da ein Absender für den Versand verschlüsselter Mails das Zertifikat⁶ des Empfängers benötigt, haben Sie dies hiermit für diesen Empfänger schon mal erledigt.

Der Empfänger einer Mail mit gültiger Signatur, hier schon die ebenfalls signierte Rückantwort auf unsere obige Mail, sieht dies an einem kleinen Icon mit dem Text „Digital signiert und überprüft“.

Wurden von irgendjemanden Änderungen am Mailinhalt vorgenommen, ist die Unterschrift ungültig.

Re: Testmail

Andreas Grupp (grupp@lehrerfortbildung-bw.de) [Kontakt hinzufügen](#)

An: Hans Mustermann;

Digital signiert und überprüft

Hallo

die Mail kam mit gültiger Unterschrift an!

Grüße, Andreas Grupp

Alleine durch das Öffnen der signierten Rückantwort, wurde übrigens das Zertifikat des Absenders in den Zertifikatsspeicher von Windows übernommen. Grundsätzlich wäre damit bereits eine verschlüsselte Rückantwort von Ihrer Seite aus möglich. Hier zeigt sich aber eine kleine

⁵ Für die Profis: Der lästige Schlüsselaustausch bei GnuPG ist somit wesentlich eleganter gelöst.

⁶ Korrekt formuliert muss es „den öffentlichen Teil des Zertifikats / des öffentlichen Schlüssel“ lauten.

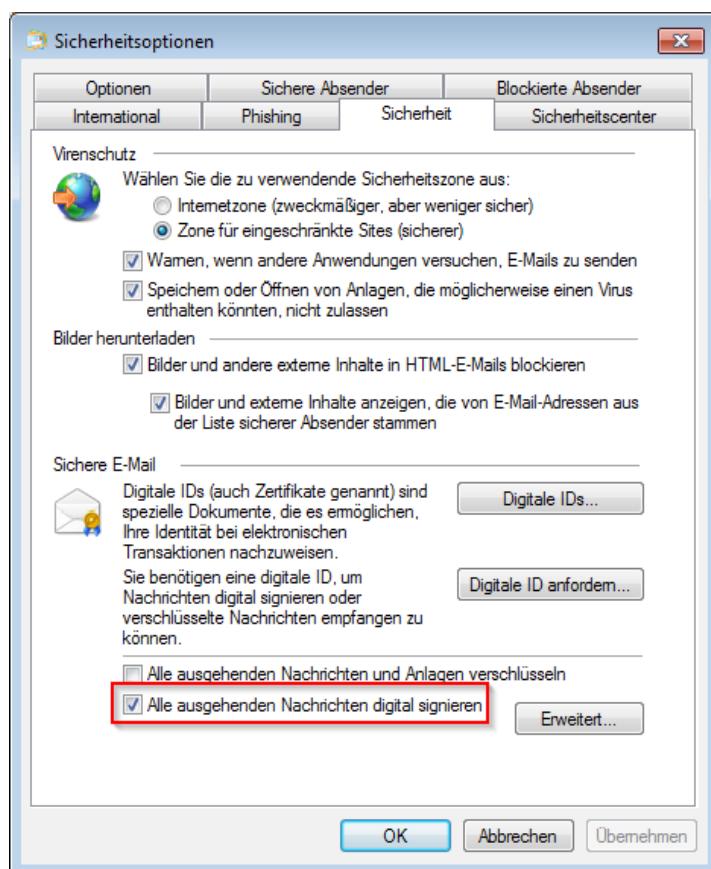
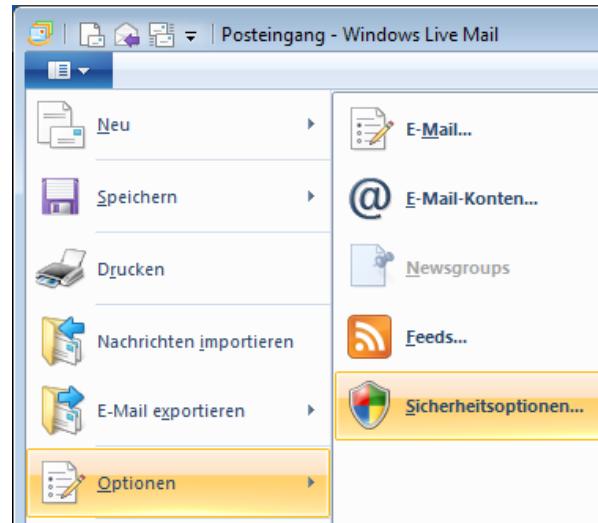
Unzulänglichkeit von Microsoft Live Essentials, die Anwendung muss dafür neu gestartet werden um den veränderten Zertifikatsspeicher neu einzulesen.

Standardmäßig signierte Mails

Grundsätzlich ist es eine gute Idee, die digitale Signatur Ihrer Mails als Standard⁷ einzustellen. Potentielle Absender vertraulicher Daten haben damit dann schon vorab Ihr Zertifikat in deren Zertifikatsspeicher und können Ihnen sofort verschlüsselte Mails senden.

Die entsprechende Einstellung finden Sie wie folgt:

- Lassen Sie sich, wie nebenstehend gezeigt, das Pull-Down-Menü von *Windows Live Mail* anzeigen
- Wählen Sie dort „*Optionen*“ und dann „*Sicherheitsoptionen ...*“ aus



Im nächsten Dialogfenster wählen Sie dann die Registerkarte „*Sicherheit*“ und setzen dort die Option:

„*Alle ausgehenden Nachrichten digital signieren*“

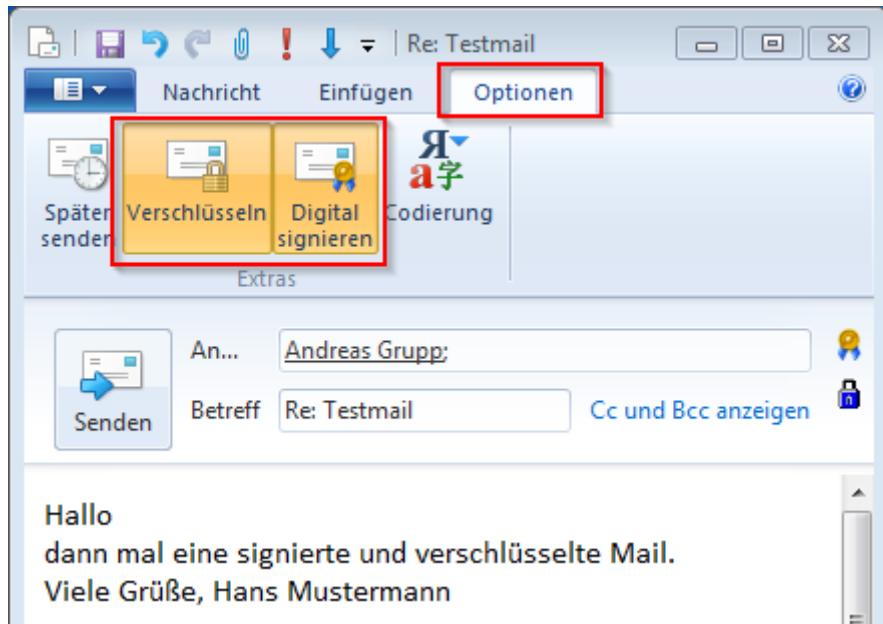
Nachteile hat diese Einstellung nicht!

⁷ Empfänger die nur einen Webmailer verwenden, sind bei signierten Mails allerdings gelegentlich verwirrt, da bei ihnen die digitale Signatur als Mailanhänger in einer P7-Datei erscheint.

Verschlüsselte Mails

Grundvoraussetzung für verschlüsselte Mails: Wie bereits erwähnt, muss Ihnen der Empfänger vorab sein öffentliches Zertifikat per Mail übermittelt haben. Dazu muss er, wie im vorigen Abschnitt beschrieben, einmal eine digital unterschriebene Mail an Sie gesandt haben.

Danach geht es ganz einfach: Neue Mail verfassen und nach Anwählen des „Optionen“-Registers die Schaltfläche „Verschlüsseln“ anklicken, das war's!



Eventuelle Dateianhänge werden dadurch auch automatisch verschlüsselt!

Das kann nicht so einfach sein ...

Oh doch ..., wenn Sie bis hierher gekommen sind, dann ist das ab jetzt soooooo einfach. Wenn Sie es nicht glauben, schauen Sie sich doch mal den Quellcode einer verschlüsselten Mail an – die Sie dazu einfach mal verschlüsselt an sich selbst mailen. Klicken Sie in der Mailübersicht die Mail mit der rechten Maustaste an und wählen Sie „Eigenschaften“. Im nächsten Fenster klicken Sie in der Registerkarte „Details“ auf „Sicherer Quelltext ...“.

```
Content-Type: application/pkcs7-mime; name="smime.p7m"; smime-type=enveloped-data
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7m"
Content-Description: S/MIME Encrypted Message
X-TOI-SPAM: n;1;2014-07-16T08:34:03Z
X-TOI-VIRUSSCAN: clean
X-TOI-EXPURGATEID: 149288::1405499639-0000153C-ABB03CED/0-0/0-0
X-TOI-SPAMCLASS: CLEAN, NORMAL
X-TOI-MSGID: 62c90dde-6e6e-4f7e-b0ec-af7ae5b83eb3
X-Seen: false
X-ENVELOPE-TO: <smime-lfb@t-online.de>

MIAGCSqGSIb3DQEHA6CAMIACAQAxggN2MIIBrQIBADCB1DCBjDELMAkGA1UEBhMCSUwxFjAU
BgNVBAoTDVNOYXJ0Q29tIE02C4xKzApBgNVBAstI1N1Y3VyZSBEaWdpdGFsIEN1cnRpZmlj
YXR1IFNpZ25pbmcxODA2BgNVBAMTL1N0YXJ0Q29tIENsYXNzIDEgUHJpbWFyeSBJbnR1cm1l
ZG1hdGUgQ2xpZW50IENBAgMJchUwDQYJKoZIhvcNAQEBBQAEggEAQCuGIZrfDjpniO8KFzw1
T0Rz+0A1w0i+0Tm15vR5Cn+T/H04TRl0F+8Vw3u+h41T0R5AvTHMWT17D0Z+Lw+TR7541+870
```

Dieser „Zeichensalat“ ist der verschlüsselte Mailinhalt, ggf. incl. Dateianhänge.

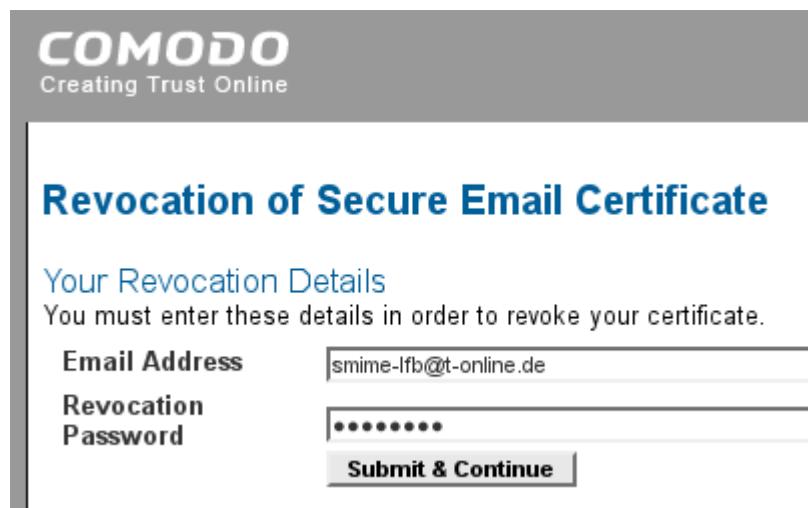
Anhang A – Comodo-Zertifikate für ungültig erklären

Gründe für das Zurückziehen eines Zertifikats / ein Zertifikat für ungültig erklären:

- Das Zertifikat / Teile des Zertifikats gingen verloren
- Es besteht der Verdacht, dass das Zertifikat in falsche Hände gelangt ist

In solchen Fällen benötigen Sie ein neues Zertifikat und müssen das bisherige Zertifikat möglichst für ungültig erklären / zurückziehen, oder im englischen Fachbegriff → eine Revocation durchführen.

Am Beispiel von Comodo-Zertifikaten gehen Sie dazu auf https://secure.comodo.com/products!/SecureEmailCertificate_Revoke, tragen die E-Mail-Adresse und das Revocation Passwort (wurde bei der Beantragung des Zertifikats festgelegt) des betroffenen Zertifikats ein.



Revocation of Secure Email Certificate

Your Revocation Details
You must enter these details in order to revoke your certificate.

Email Address

Revocation Password

Submit & Continue

Betätigen Sie dann die Schaltfläche „Submit & Continue“. Bei korrekter Angabe des Revocation Passworts erhalten Sie die nachfolgende Rückbestätigung.

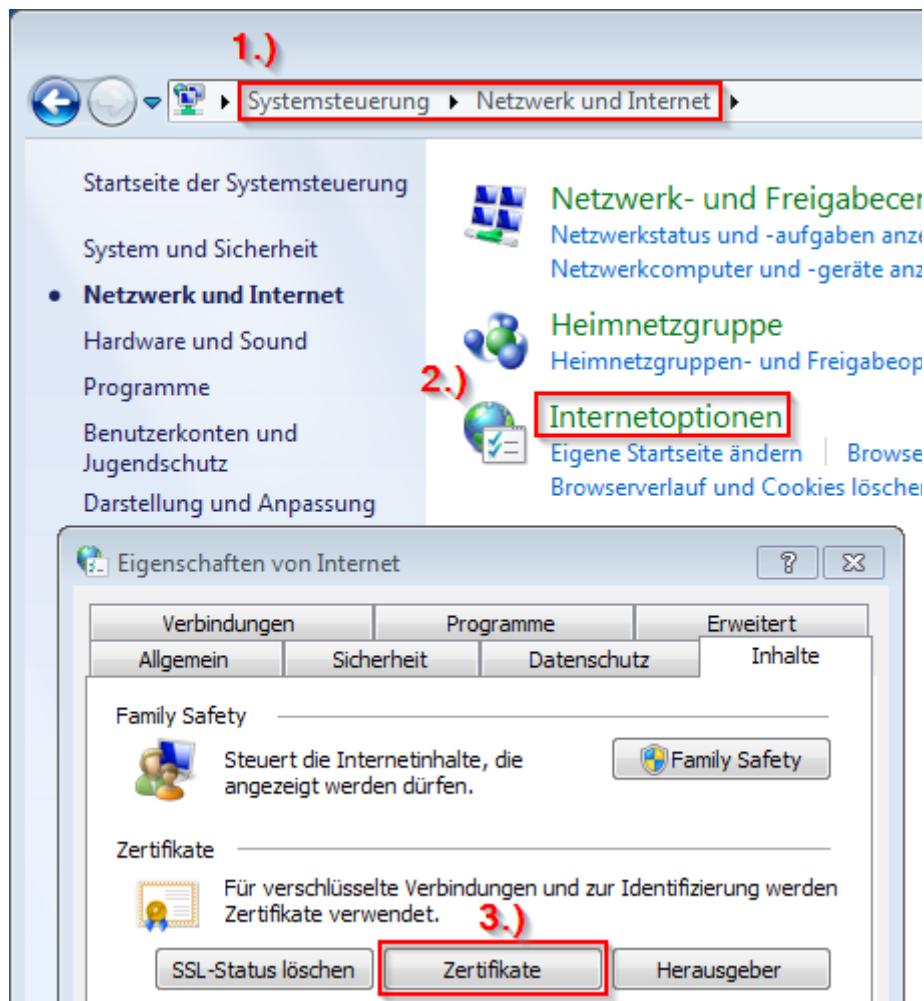


The Secure Email certificate for smime-lfb@t-online.de has been revoked

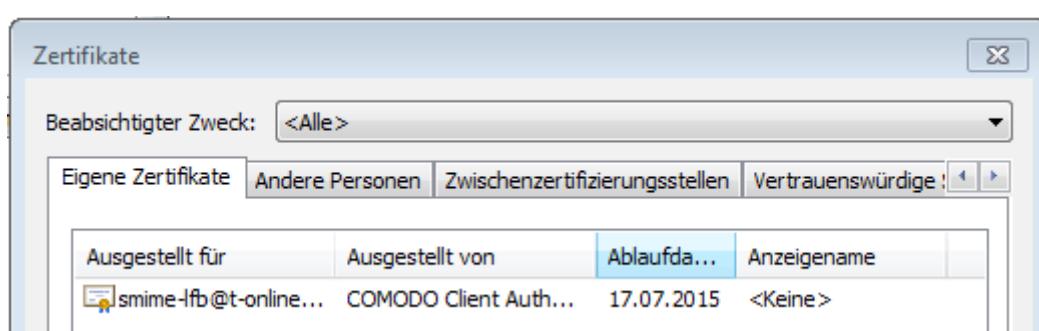
Anhang B – Kontrolle des Zertifikatsspeichers

Wenn Sie auf den Zertifikatsspeicher des Betriebssystems Windows zugreifen wollen, starten Sie die „Systemsteuerung“ und wählen Sie den Bereich „Netzwerk und Internet“.

In diesem Bereich der Systemsteuerung finden Sie die „Internetoptionen“ die in einem eigenen Fenster mit mehreren Registerkarten dargestellt werden. Wählen Sie hier die Registerkarte „Inhalte“ und klicken Sie auf die Schaltfläche „Zertifikate“.



Unter der Registerkarte „Eigene Zertifikate“ sieht man unser oben installiertes Zertifikat, während unter „Andere Personen“ die Zertifikate der Kommunikationspartner, so weit bereits erhalten, zu finden sind.



Anhang C – Sichern / Backup des persönlichen Zertifikats

Um das Zertifikat als eigenständige Datei sichern zu können, bzw. als normale Datei in einem Backup zu haben, muss das Zertifikat aus dem Zertifikatsspeicher exportiert werden.

Für Windows 7: Öffnen Sie dazu die Verwaltung von Zertifikaten wie im vorigen Anhang beschrieben. Anschließend gehen Sie folgendermaßen vor:

1. Wählen Sie die Registerkarte „*Eigene Zertifikate*“
2. Wählen Sie das zu exportierende Zertifikat aus
3. Klicken Sie auf die Schaltfläche „*Exportieren*“
4. Es wird der „*Zertifikatsexport Assistent*“ angezeigt. Im Start-Bildschirm des Assistenten erst einmal die Schaltfläche „*Weiter*“ anklicken.
5. „*Ja, privaten Schlüssel exportieren*“ auswählen und auf „*Weiter*“ klicken
6. Im nächsten Dialog kann der *Zertifizierungspfad* mit ausgewählt werden, muss aber nicht. Auf jeden Fall mit „*Weiter*“ fortfahren.
7. Das exportierte Zertifikat wird mit einem Kennwort geschützt. Hier also ein gutes Passwort angeben. Erneut mit „*Weiter*“ fortfahren.
8. Über die Schaltfläche „*Durchsuchen*“ einen geeigneten Speicherplatz im Dateisystem wählen und einen Dateinamen vergeben → z.B. „*smime-lfb-at-t-online-dot-de.pfx*“ und dann mit „*Weiter*“ fortfahren.
9. Zum Abschluss auf „*Fertig stellen*“ klicken.