E-Mail-Verschlüsselung mit S/MIME und Microsoft Outlook

Für die Verschlüsselung mit S/MIME wird ein Schlüsselpaar benötigt, das von einer Stammzertifizierungsstelle[1] 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 StartSSL[2] 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 CAcert[3].

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

S/MIME-Zertifkat / Free Secure Email Certificate von Comodo[4]

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

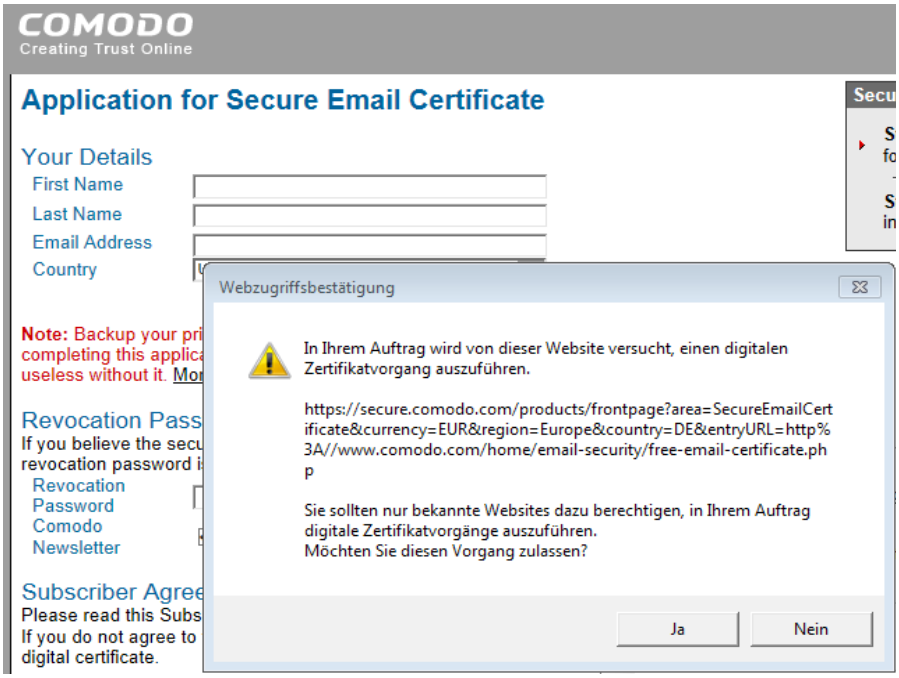
Starten Sie also die Anwendung Microsoft Internet Explorer und verwenden Sie diesen auch weiter unten um das Zertifikat bei Comodo, nach dessen Ausstellung, abzuholen.

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 Verschlüsselungs-zertifikate betreffen. Der Internet Explorer zeigt deshalb sofort eine Warnung und möchte von Ihnen die Erlaubnis für diese Vorgänge.

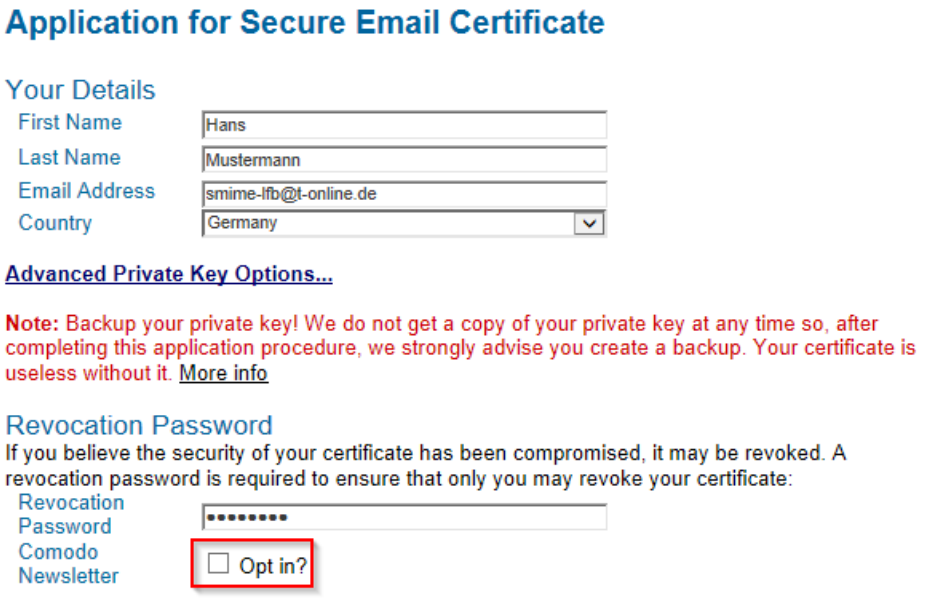
Bestätigen Sie den Vorgang durch einen Klick auf die Schaltfläche „Ja“.



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.

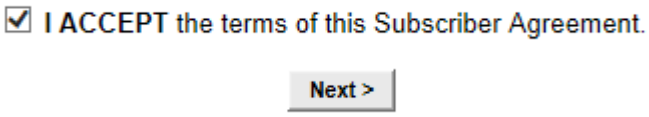
Merken Sie sich dieses Revocation-Passwort, Sie benötigen es bei Verlust oder Kompromittierung Ihres Zertifikats!



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.

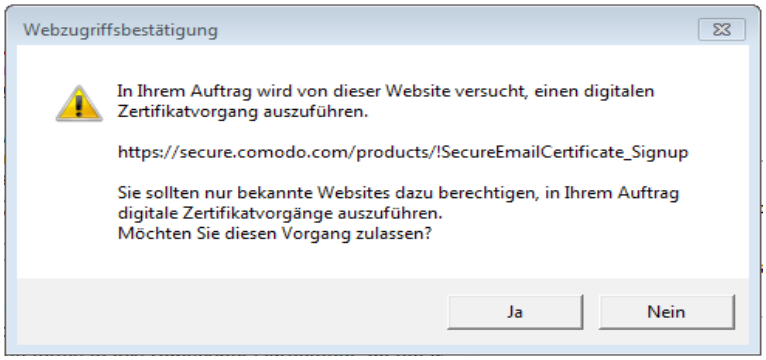
Diese Vereinbarung muss über das Setzen der ACCEPT-Option akzeptiert werden.



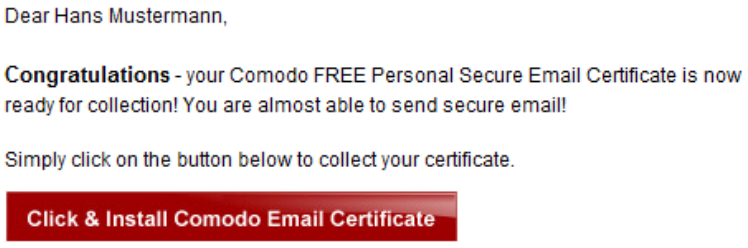
Nach dem **Anklicken der Schaltfläche „Next >“** sendet Comodo einen Funktionsaufruf an Ihren Browser, damit dieser über eine eingebaute Cryptofunktion ein Schlüsselpaar erzeugt.

Insbesondere der geheime Schlüssel (einer der beiden Schlüssel des Schlüsselpaars) 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.



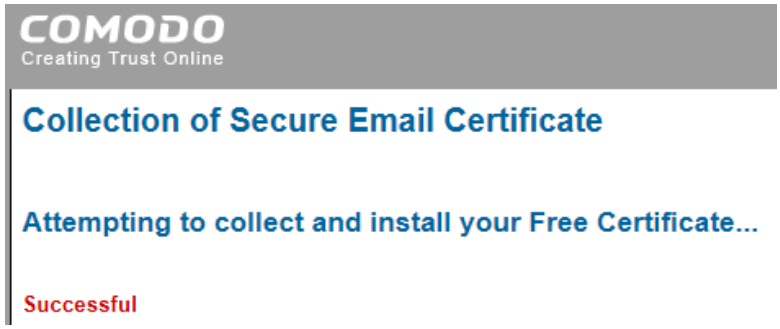
Mit dieser Mail, die Sie nach kurzer Zeit im Maileingang finden sollten, überprüft Comodo in einem Schritt, ob Sie das zugehörige Mailkonto abrufen können und teilt Ihnen mit, wo Sie die Beglaubigung abrufen können.

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.

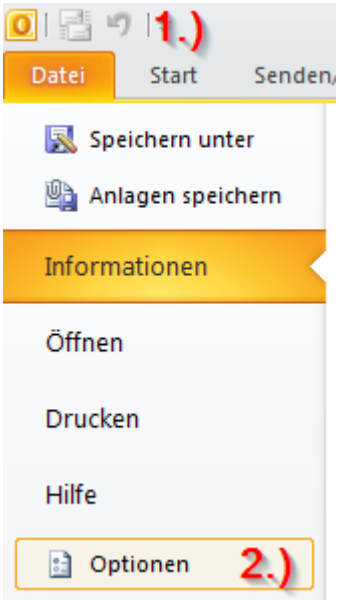
Erneut wird dabei auf den Zertifikatsspeicher zugegriffen und erneut möchte der Internet Explorer für diesen Vorgang eine Bestätigung von Ihnen haben. Erlauben Sie also auch diesen letzten Zugriff durch einen Klicke auf „Ja“.

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 „Microsoft Outlook“



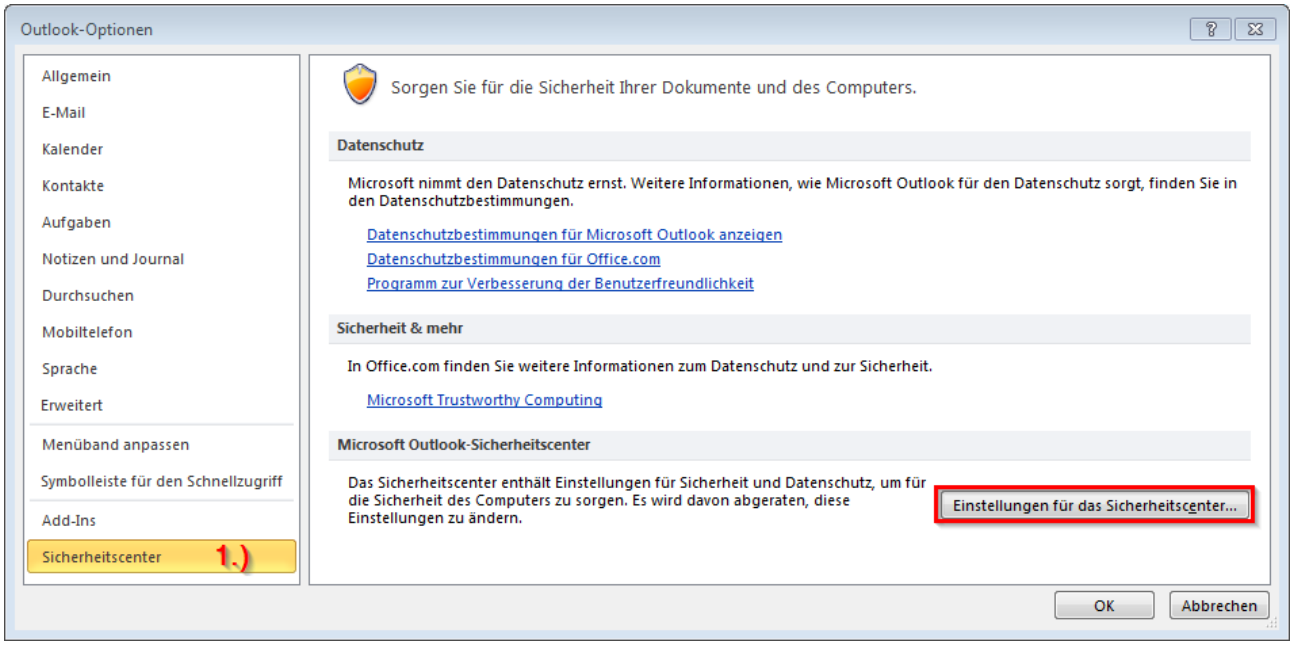
Starten Sie das bereits vorab mit Ihrem Mailkonto verknüpfte *Microsoft Outlook* und wechseln Sie dort im Hauptfenster von der Registerkart „Start“ (Default nach dem Programmstart) auf den Reiter „Datei“

→ Nebenstehend durch 1.) gekennzeichnet

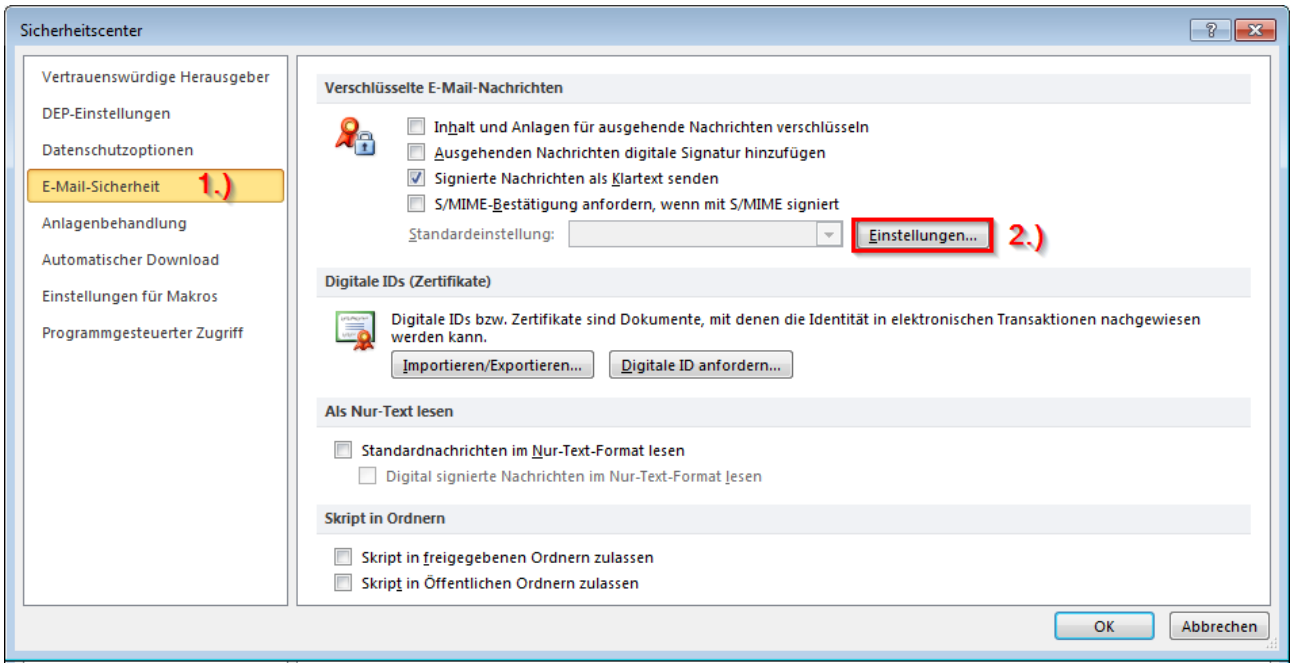
Klicken Sie anschließend auf „Optionen“

→ Nebenstehend durch 2.) gekennzeichnet

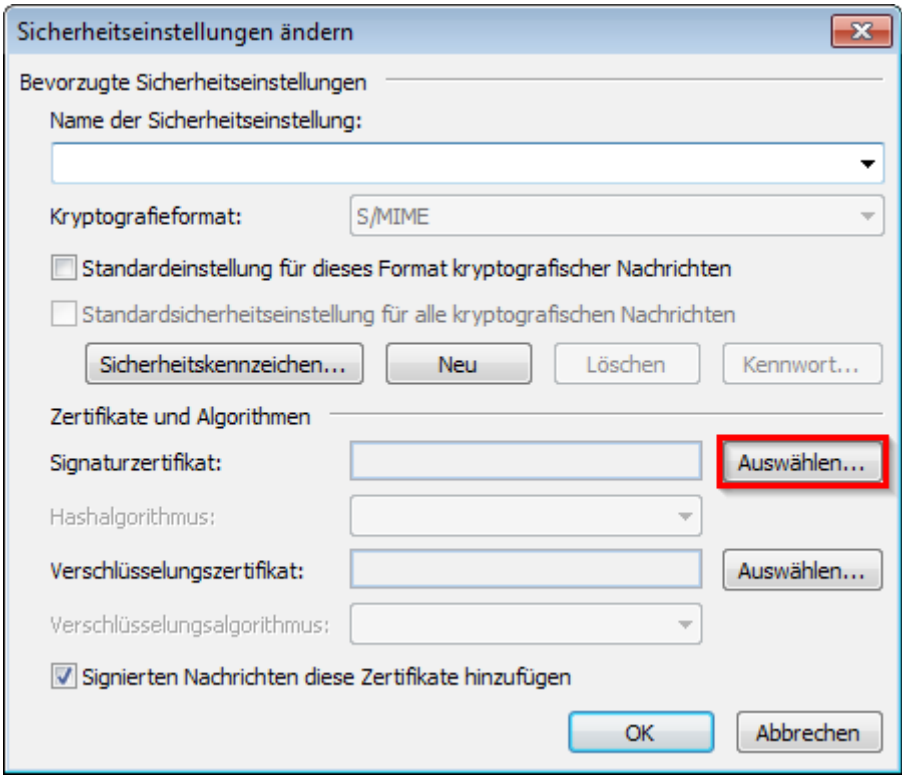
Ein Pop-Up-Fenster mit den Outlook-Optionen wird angezeigt. Wählen Sie hier auf der linken Seite zuerst „Sicherheitscenter“ aus um anschließend auf der rechten Seite die Schaltfläche „Einstellungen für das Sicherheitscenter ...“ anzuklicken.



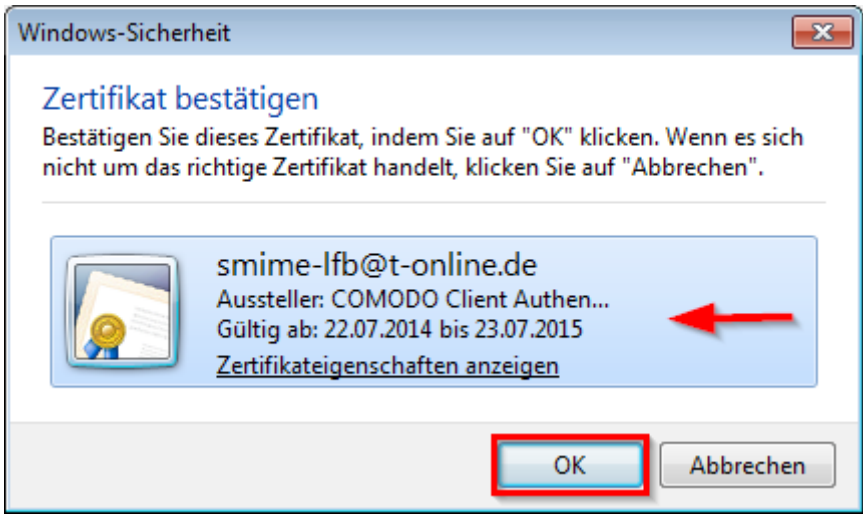
Im Sicherheitscenter auf der linken Seite „E-Mail-Sicherheit“ auswählen und dann rechts die Schaltfläche „Einstellungen“ anklicken.



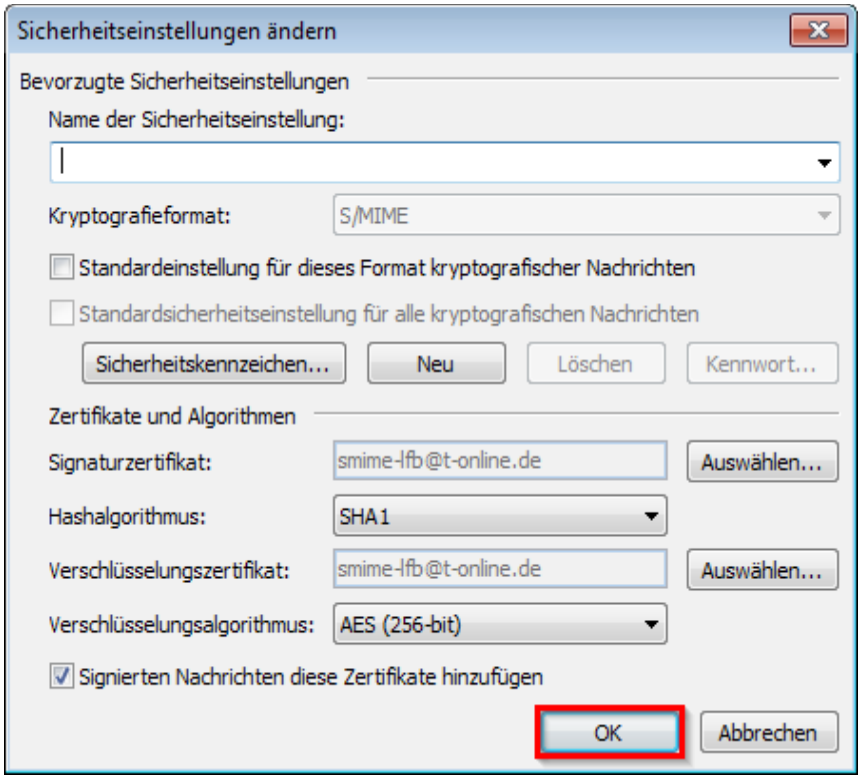
Der Dialog „Sicherheitseinstellungen ändern“ wird nun als Pop-Up-Fenster angezeigt. Klicken Sie hier, wie im Screeshot gezeigt, bei „Signaturzertifikat“ auf die Schaltfläche „Auswählen“.



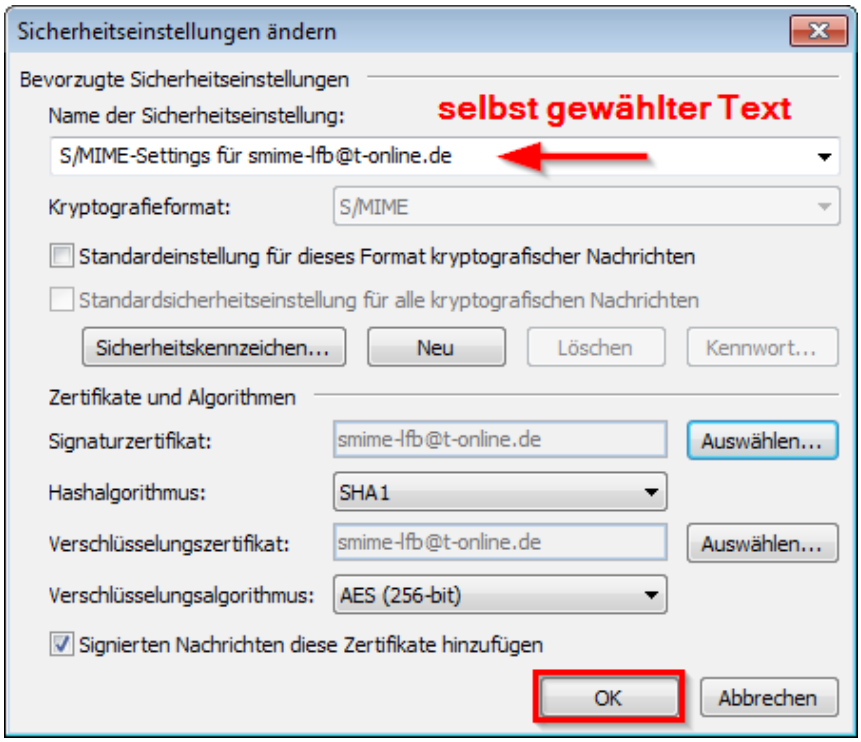
Das weiter oben mit dem Internet Explorer für Ihre Mailadresse installierte Zertifikat sollte nun automatisch angezeigt werden. Klicken Sie hier auf „OK“.



Die Sicherheitseinstellungen wurden nun, wie gezeigt geändert. Im Bereich des Signaturzertifikats sehen Sie als Eintrag Ihre im Zertifikat hinterlegte Mailadresse.

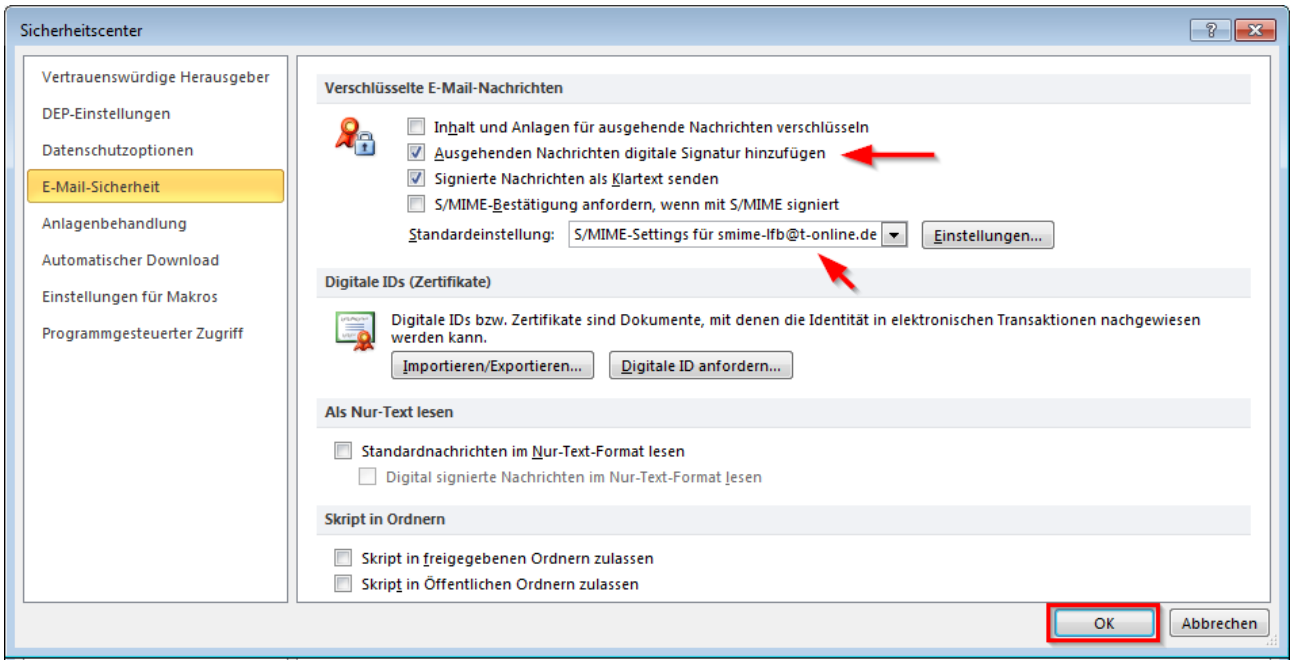


Vergeben Sie für diese Sicherheitseinstellung noch einen selbst gewählten Namen (siehe Beispiel im Screenshot) und klicken Sie dann auf „OK“.



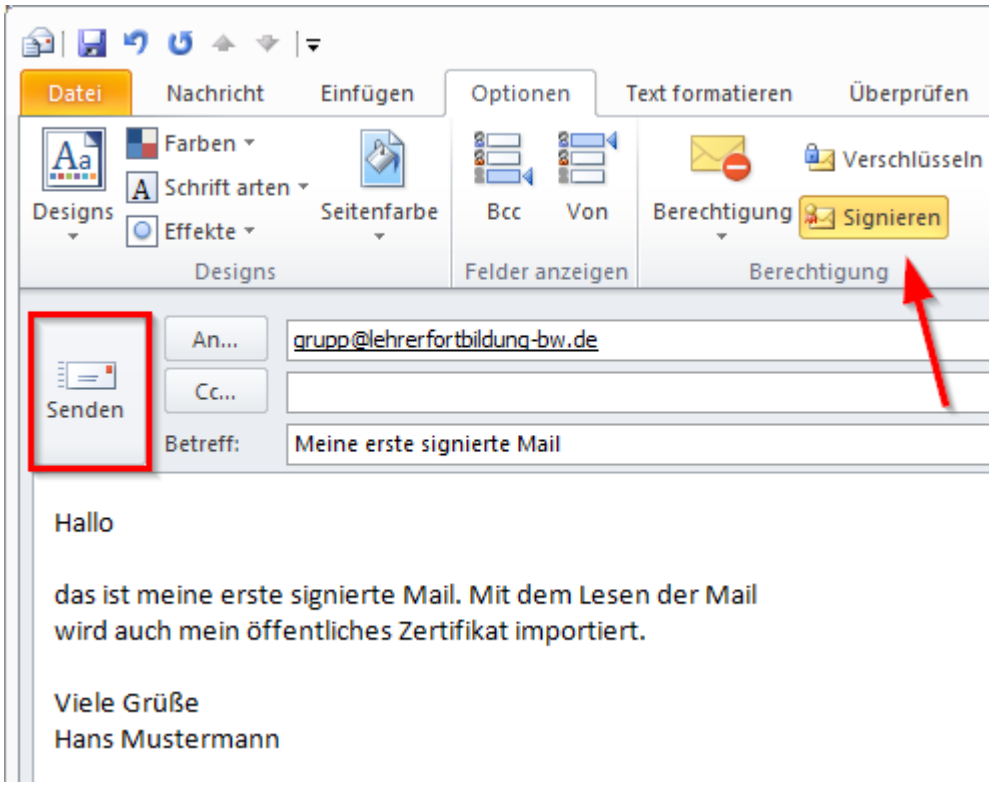
Sie befinden sich nun wieder im „Sicherheitscenter“. Um ausgehende Nachrichten standardmäßig mit einer digitalen Unterschrift zu versehen, dabei den Mailtext aber lesbar zu belassen, setzen Sie wie gezeigt die beiden Optionen

- Ausgehende Nachrichten digitale Signatur hinzufügen
- Signierte Nachrichten im Klartext senden



Damit haben Sie die S/MIME-Einstellungen Ihres Kontos erfolgreich durchgeführt und können das Sicherheitscenter mit „OK“ schließen.

Praktische S/MIME-Anwendung



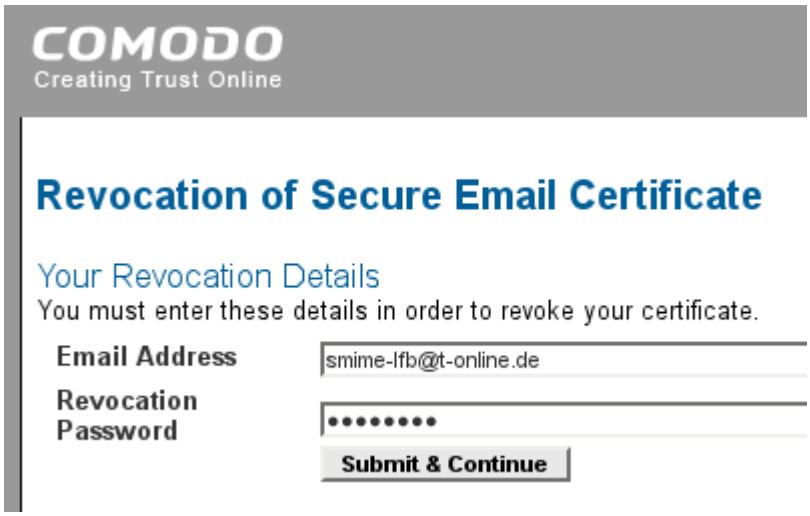
Anhang A – Comodo-Zertifikate für ungültig erklären

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.

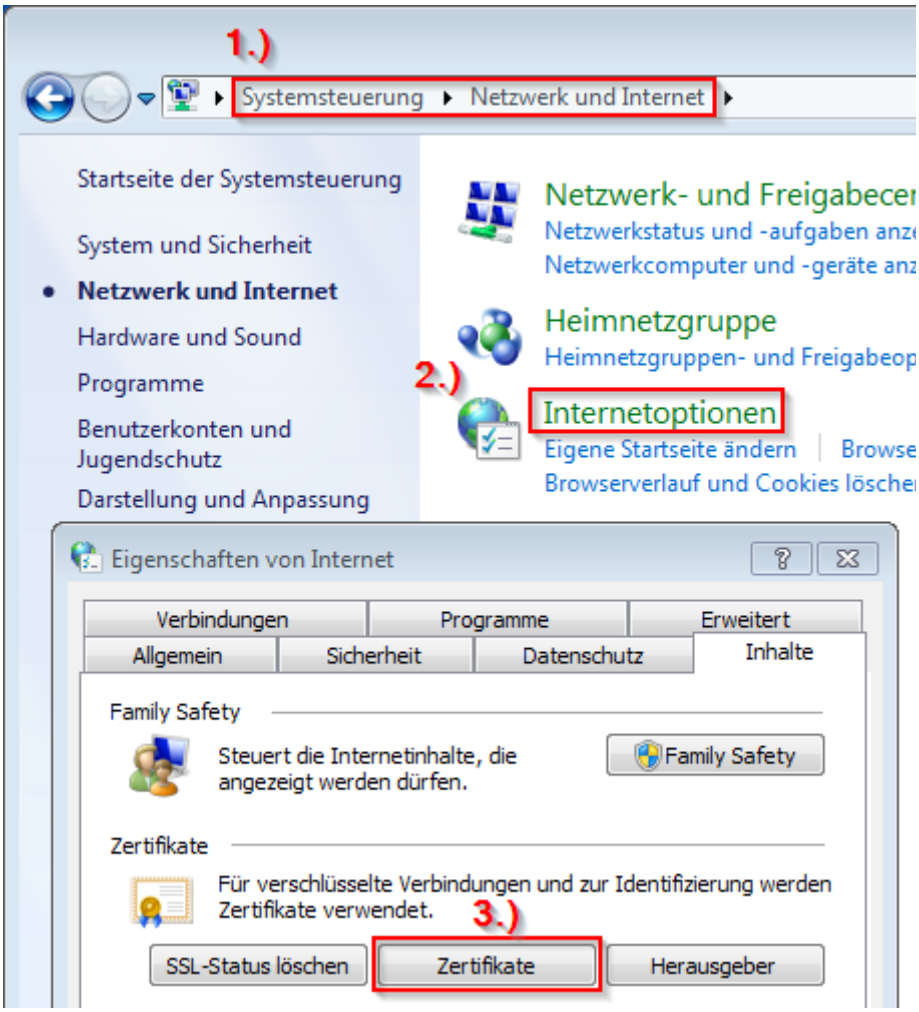


Betätigen Sie dann die Schaltfläche „Submit & Continue“. Bei korrekter Angabe des Revocation Passworts erhalten Sie die nachfolgende Rückbestätigung.

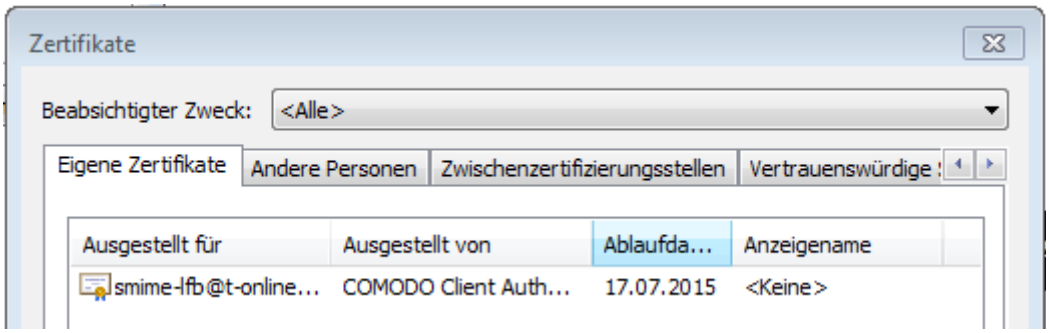
Anhang B – Kontrolle des Zertifikatsspeichers

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.