E-Mail-Verschlüsselung mit S/MIME und Mail (Apple)

Anleitung basiert auf Vorab-Material von Andreas Grupp, grupp@lehrerfortbildung-bw.de

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.

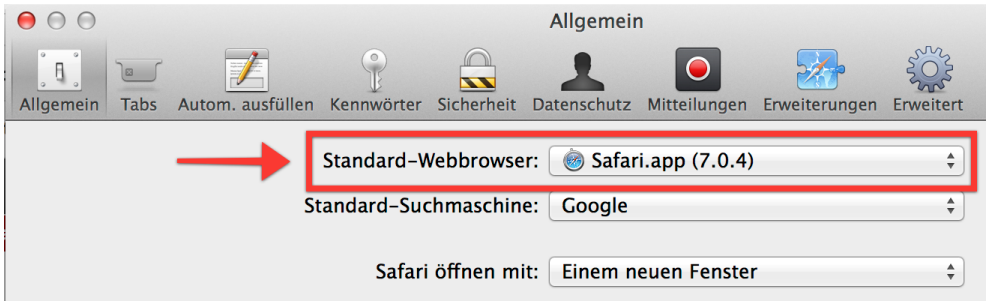
Wichtig: (nur falls Safari nicht Ihr Standardbrowser ist!)

Für das im Folgenden beschriebene Verfahren wird davon ausgegangen, dass auf Ihrem System Safari als Standardbrowser eingerichtet ist. Ist das nicht der Fall, weil Sie sich z.B. Firefox als Standardbrowser eingerichtet haben, müssen Sie zunächst Safari temporär als Standardbrowser einrichten, Sie können Firefox dann aber nach der Installation der Zertifikate selbstverständlich wieder als Standardbrowser einrichten.

So richten Sie Safari als Standardbrowser ein: Starten Sie Safari und wählen Sie im Menü „Safari“ den Punkt „Einstellungen“:

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/

Im nun folgenden Fenster wählen Sie unter „Standard – Webbrowser“ Safari aus:



Auf genau diesem Weg können Sie nach dem Installieren der Zertifikate auch wieder Ihren persönlichen Lieblingsbrowser als Standardbrowser einrichten. Nach diesen Vorarbeiten kann es losgehen!

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

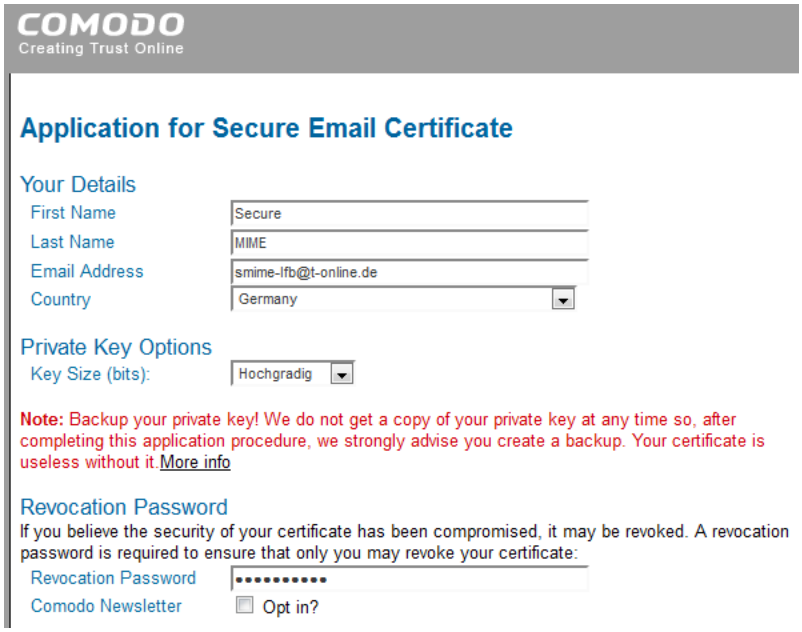
Unter der in der Fußnote angegebenen Adresse beginnt der Beantragungsprozess durch einen Klick auf die nebenstehende dargestellte Schaltfläche.

Im nachfolgenden Formular füllen Sie die Felder „Vorname“, „Nachname“, „E-Mail-Adresse“ und „Land“ aus.

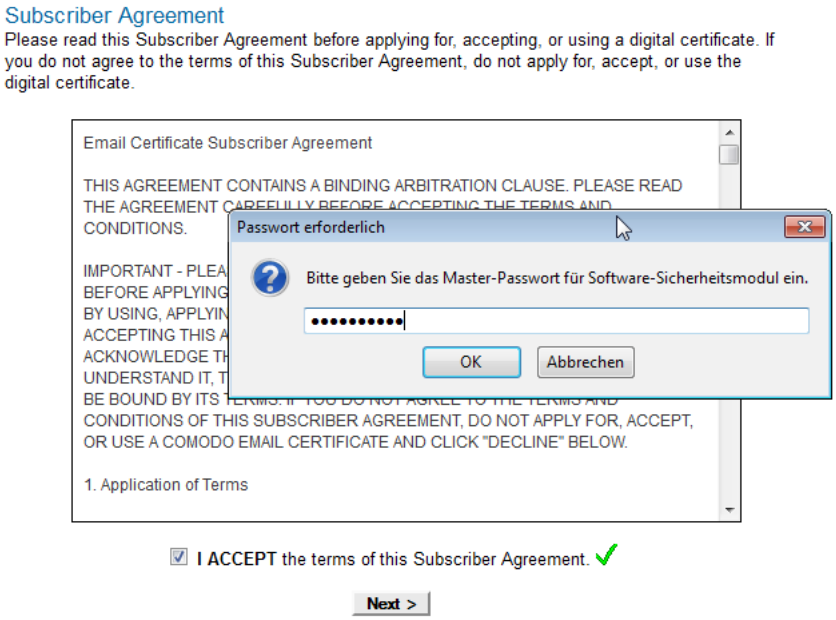
Die Schlüsseloption belassen Sie auf „Hochgradig“ oder „2048 (High Grade)“ - je nach Browser.

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.

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



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



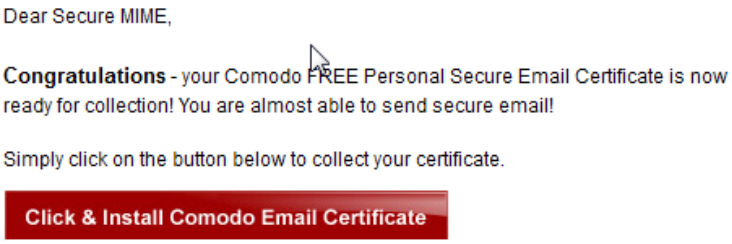
Im unteren Teil des Antragsformulars finden Sie den legalen Teil des Antrags – eine Einverständniserklärung / Vereinbarung zwischen Ihnen und Comodo. Diese Vereinbarung muss über das Setzen der ACCEPT-Option akzeptiert werden.

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.

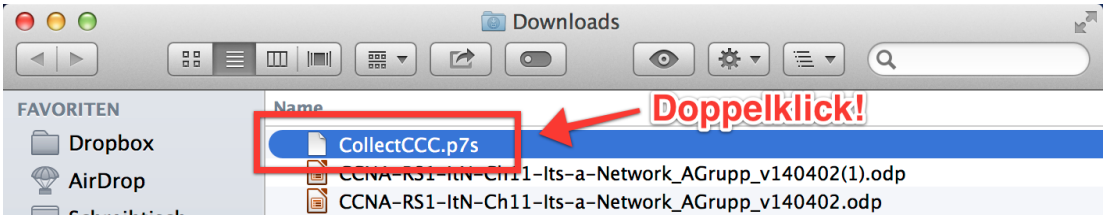
Da bei dieser Aktion das Schlüsselpaar in den Zertifikatsspeicher des Browsers geschrieben wird, müssen Sie diesen gegebenfalls über die Angabe des Master-Passworts freigeben. Sie haben doch hoffentlich ein Master-Passwort gesetzt? Falls nicht, machen Sie das unbedingt im Anschluss! Das Master-Passwort schützt unter anderem ihr persönliches Zertifikat und damit Ihre persönliche Identität.

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

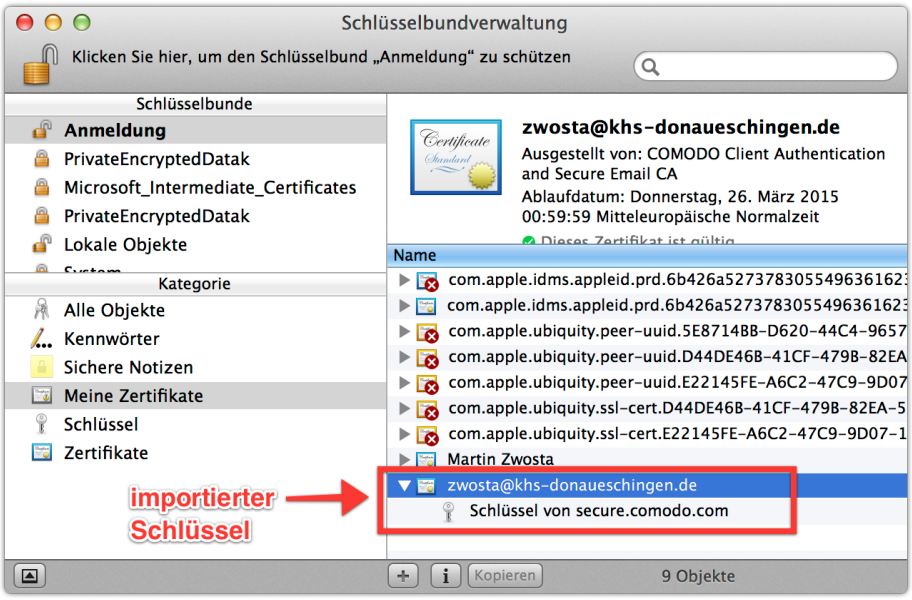


Mit dieser Mail, die Sie nach kurzer Zeit im Maileingang finden solllten, überprüft Comodo in einem Schritt, ob Sie das zugehörige Mailkonto abrufen können und teilt Ihnen mit, wo Sie die Beglaubigung abrufen können.

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 (Safari) lädt das Zertifikat in Ihren Download – Ordner. Das Zertifikat liegt nun als Datei („CollectCCC.p7s“) auf Ihrem Rechner und muss nun noch in die Schlüsselbundverwaltung Ihres Rechners integriert werden. Dazu machen Sie einfach einen Doppelklick auf das heruntergeladene Zertifikat:

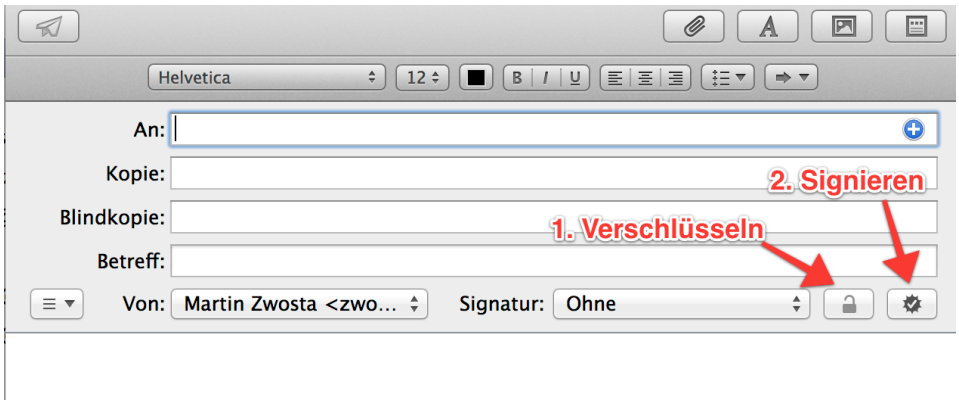


Im Regelfall wird Ihnen nun die Schlüsselbundverwaltung angezeigt und Sie können sehen, dass das Zertifikat erfolgreich importiert wurde:



Wichtig: Falls Ihr email – Programm während dieses Vorgangs geöffnet war, müssen Sie es jetzt einmal schießen und wieder neu öffnen, damit es die neuen Zertifikate einlesen kann.

Sobald Sie Ihr mail – Programm neu gestartet haben, sehen Sie 2 neue Symbole für das Verschlüsseln und Signieren von emails:



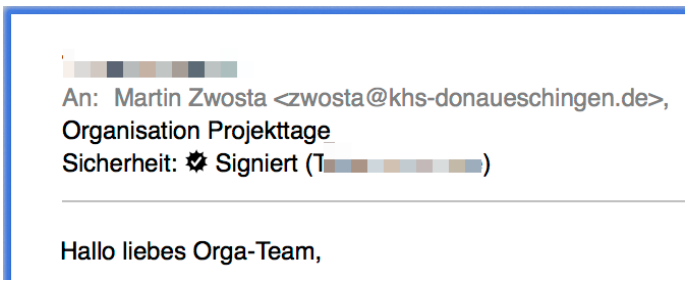
Jetzt sind alle Vorbereitungen getroffen und Sie können nun bequem verschlüsseln und signieren!

Praktische S/MIME-Anwendung

Versenden einer digital unterschriebenen Mail: Klicken Sie auf S/MIME und wählen Sie die Option „*Nachricht unterschreiben*“ aus – mehr ist dafür nicht zu machen. Sie verfassen einfach Ihren Mailtext, fügen evtl. noch Anhänge hinzu, und senden die Mail dann einfach ab.

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 wird[5].

Der Empfänger sieht die gültige Signatur (natürlich je nach email – Programm, hier: mac – Mail) am „Stern mit integriertem Haken“ - ein Mausklick darauf zeigt nähere Informationen an. Wurden von irgendjemanden Änderungen am Mailinhalt vorgenommen, ist die Unterschrift ungültig und es wird ein anderes Icon zur Warnung angezeigt.



Wie im obigen Beispiel-Mailtext beschrieben, ist als Nebeneffekt das Zertifikat des Absenders **automatisch** im Zertifikatsspeicher des Empfängers gespeichert. Eine Nachfrage dazu erfolgt nicht.

Sie müssen jedem Kommunikations-Partner, der auch in der Lage sein soll Ihnen verschlüsselte Informationen zu mailen, einmal eine unterschriebene Mail senden. Damit hat das Gegenüber, wie gerade beschrieben, Ihr öffentliches Zertifikat. Genau dieses Zertifikat von Ihnen wird für verschlüsselte Mails benötigt.

So gesehen ist es grundsätzlich eine gute Idee, emails ab jetzt grundsätzlich zu signieren. Empfänger, die nur einen Webmailer verwenden, sind allerdings dann oft etwas verwirrt, da bei ihnen die digitale Signatur als Mailanhang in einer P7-Datei erscheint.

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

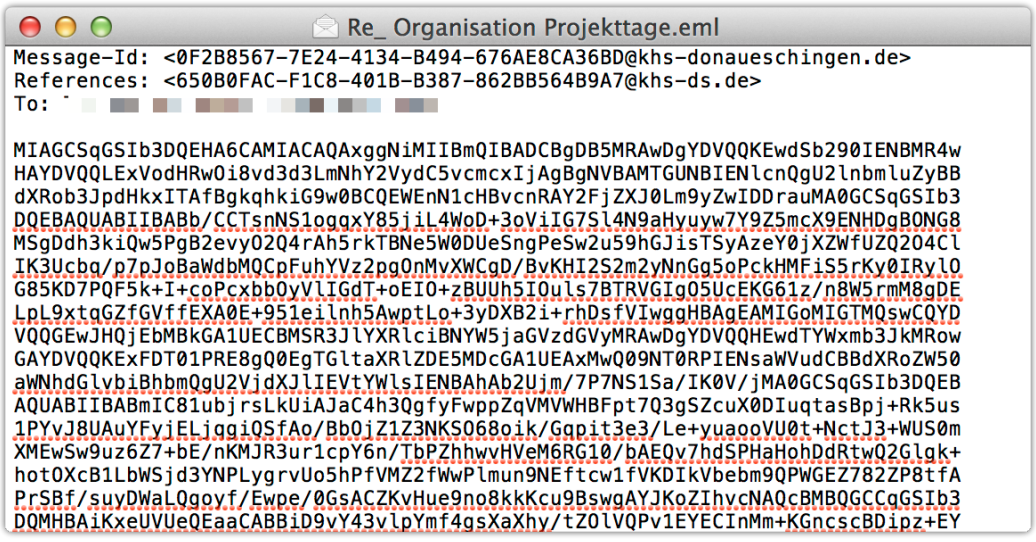
Verschlüsselte Mails

Grundvoraussetzung für verschlüsselte Mails: Der Empfänger muss Ihnen 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 das Symbol für Verschlüsseln (das Schloss) anklicken . Beachten Sie auch den Mailtext.

Das kann nicht so einfach sein …

Oh doch …, wenn Sie bis hierher gekommen sind, dann ist das nachfolgend sooooo 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. Ziehen Sie die mail auf den Desktop und öffnen Sie dann die mail mit dem Text - Editor („TextEdit“) Ihres Rechners. Sie sehen dann den Quellcode der Mail:



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