Free Email Certificate

Um E-Mails zu verschlüsseln zu können, benötigen Sie ein S/MIME-Zertifikat. Anbei vier Anbieter, die auch kostenfreie Zertifikate zur Verfügung stellen.

Diese Zertifikate haben in der Regel eine Gültigkeitsdauer von einem Jahr und ermöglichen das verschlüsseln von Emails an Empfänger, die ebenfalls ein S-Mime-Zertifikat benutzen. Es spielt dabei keine Rolle, von wem das Zertifikat des Kommunikationspartners ausgestellt wurde, es müssen lediglich beide gültig sein.

Für beruflichen Einsatz, oder wenn man bereits sicher ist, dass man künftig grundsätzlich verschlüsseln möchte, sollte man sich überlegen, ob ein kostenpflichtiges Zertifikat, dass 3 Jahre Gültigkeit hat, nicht besser geeignet ist, da bei jedem Zertifikatwechsel, die Kommunikationspartner den öffentlichen Teil des Schlüssels ersetzen müssen – klingt schlimmer als es ist, nervt aber.

Beispiel: Über 12 Jahre hinweg bedeutet dies, dass man entweder 12 mal ein 1-Jahres-Zertifikat ausstellen und verteilen muss, gegenüber 4 mal, bei 3-jährigen aber kostenpflichtigen Zertifikaten. Diese kosten dann etwa 30-60 Euro, je nach Herausgeber und Art des Zertifikates.

Inhalt:

Funktionsweise S-Mime (Kurzbeschreibung)

Jeder Kommunikationspartner hat einen privaten und einen öffentlichen Schlüssel.

Der private Schlüssel existiert nach der Erstellung zunächst nur auf dem Rechner des Eigentümers und sollte auf ein weiteres Medium (z.B. USB-Stick) gespeichert werden, da auch der Aussteller maximal den öffentlichen Schlüssel in seinem Verzeichnis hält.

Der private Schlüssel enthält auch den öffentlichen Schlüssel und ist mit einem Passwort gesichert, das nicht zurückgesetzt werden kann, wenn es verloren geht.

Der öffentliche Schlüssel wird ab sofort an alle Personen bei dem Mailversand mitgeschickt, mit denen man künftig verschlüsselt kommunizieren möchte.
Man kann den öffentlichen Schlüssel auch auf der Internetseite zum herunterladen anbieten.

Selbst fügt man, je nach System, manuell oder automatisch, die empfangenen öffentlichen Schlüssel der Kommunikationspartner in das eigene System (PC, Mac, iPhone oder anderes Gerät) ein.

Bei der verschlüsselten Kommunikation wird nun mit dem eigenen privaten Schlüssel (der auch den eigenen öffentlichen Schlüssel enthät) und den öffentlichen Schlüsseln für den Empfänger ein „Paket“ erstellt, dass von jedem, der den passenden privaten Schlüssel, der zu einem der enthaltenen öffentlichen Schlüssel gehört, geöffnet werden kann.
Je nach System nach zusätzliche Eingabe des Kennwortes oder automatisch.

Systemanforderung

Es sind keine Installationen auf Serverseite notwendig.
Auf den Clients können, ohne administrative Rechte zu benötigen, derzeit folgende Mailprogramme ohne Zusatz Software die Mailverschlüsselung nutzen:

- Outlook
- Thunderbird
- Lotus Notes
- Mac Mail
- iOS-Mail
- Android

Für die Erstellung der Zertifikate sind in der Regel folgende Browser kompatibel

- Internet Explorer
- Firefox
- Safari
- ...

Folgende Browser funktionieren nicht:

- EDGE
- ...

Anbieter von kostenfreien Zertifikaten

Hier eine Liste ohne Anspruch auf Vollständigkeit und Aktuallität:

Secerio

https://www.secorio.com/de/

Wisekey

https://www.wisekey.com/wiseid/

comodo

https://www.comodo.com/

Fraunhofer SIT

https://volksverschluesselung.de/

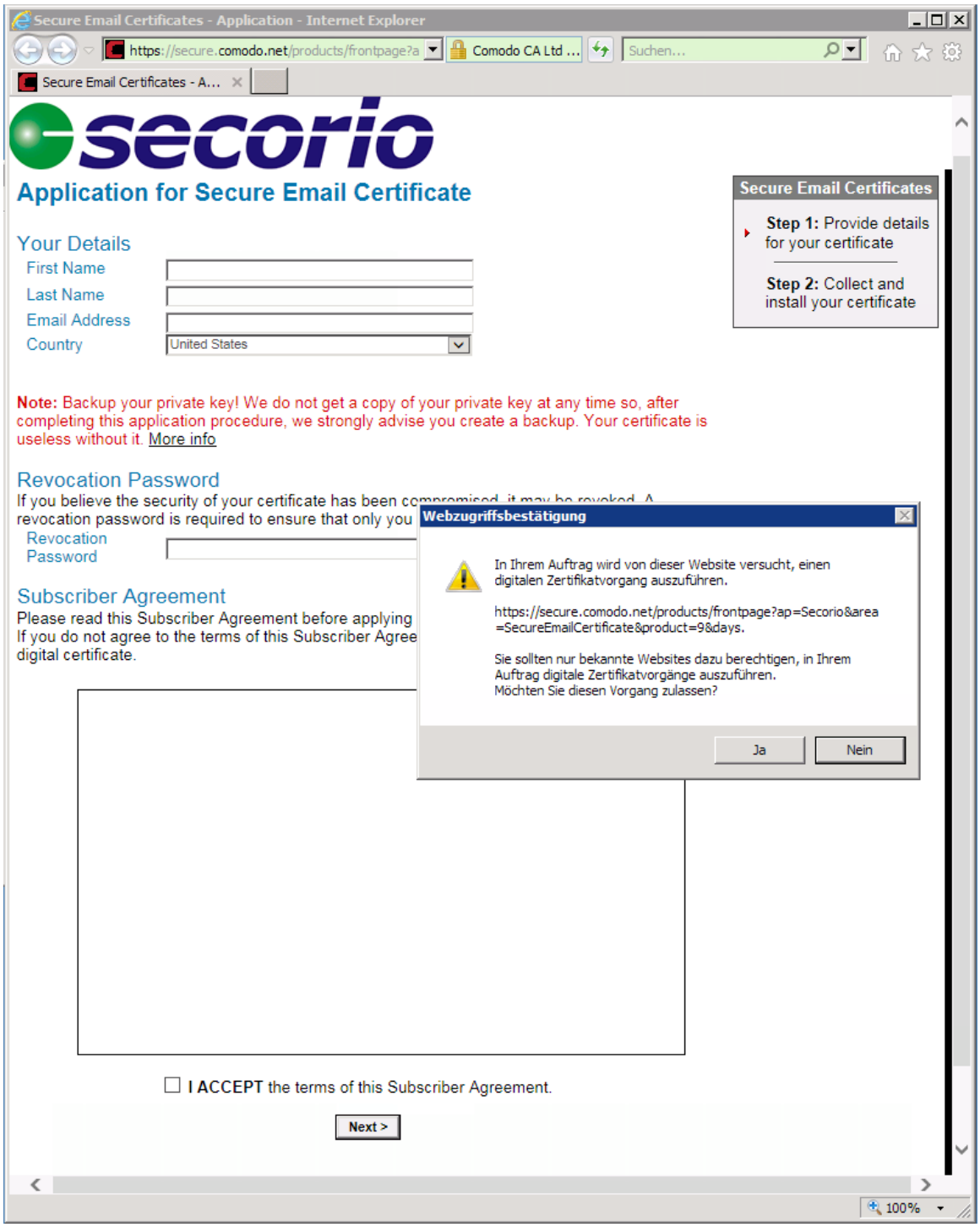
Erstellung eines Email Zertifikates unter Windows / Internet Explorer

Als Beispiel auf der Seite von Comodo:

Aufruf der Seite

Starten Sie in einem Browser (nicht EDGE) folgenden Link und tragen Sie Ihren Namen und Ihre Mailadresse ein:

https://secure.comodo.com/products/frontpage?area=SecureEmailCertificate&currency=EUR&region=Europe&country=DE&entryURL=https%3A//www.comodo.com/home/email-security/free-email-certificate.php



Bestätigen Sie die Meldung immer mit JA, damit auf Ihrem Rechner, unter Ihrem Browser ein Programm ausgeführt werden kann, dass Ihren Schlüssel berechnet.
Dieses Popup erscheint wiederholt und Sie müssen es jedes mal mit JA bestätigen.

Wenn Sie nicht zustimmen, kann kein Zertifikat berechnet werden.

Bei anderen Browsern kann es sein, dass dieses Popup nicht erscheint, dann sehen Sie folgende Meldung:

Und Sie müssen oben links in der URL-Zeile auf das Schloss klicken und in dem Popup-Menue daß ausführen der Anwendung zur Schlüsselerzeugung gestatten.

Eingabe Ihrer Daten

Geben Sie Ihren Vor- und Nachnamen sowie die zu verwendende E-Mail-Adresse ein, für die das Zertifikat erstellt werden soll.

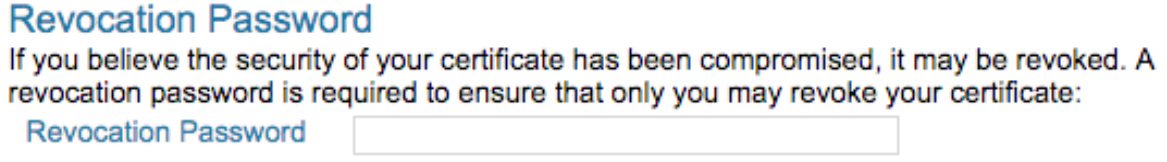
Hinweis: Es kann nur eine E-Mail-Adresse pro Zertifikat vergeben werden.

Revocation Password

Für den Fall, dass Sie zu einem späteren Zeitpunkt das Zertifikat für ungültig erklären möchten / müssen, vergeben Sie bitte hier ein Kennwort.

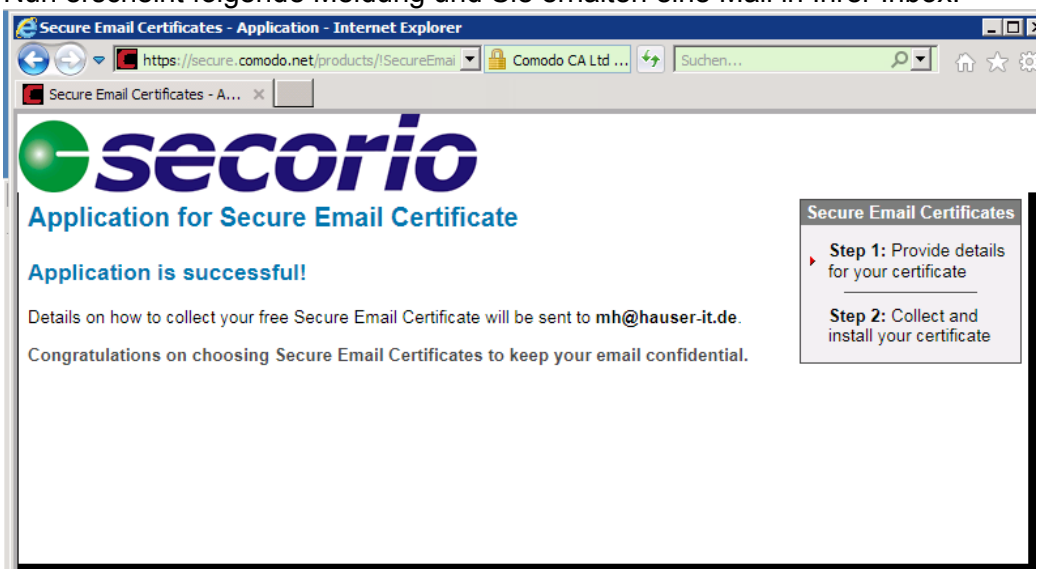
Dies kann z.B. der Fall sein, wenn Sie feststellen, dass Ihr Rechner gehackt wurde, oder eine Kopie des Zertifikates verlorengegangen ist.

Tipp: Schreiben Sie das Kennwort erst auf einen Zettel und schreiben es dann von dort ab!



Bestätigen

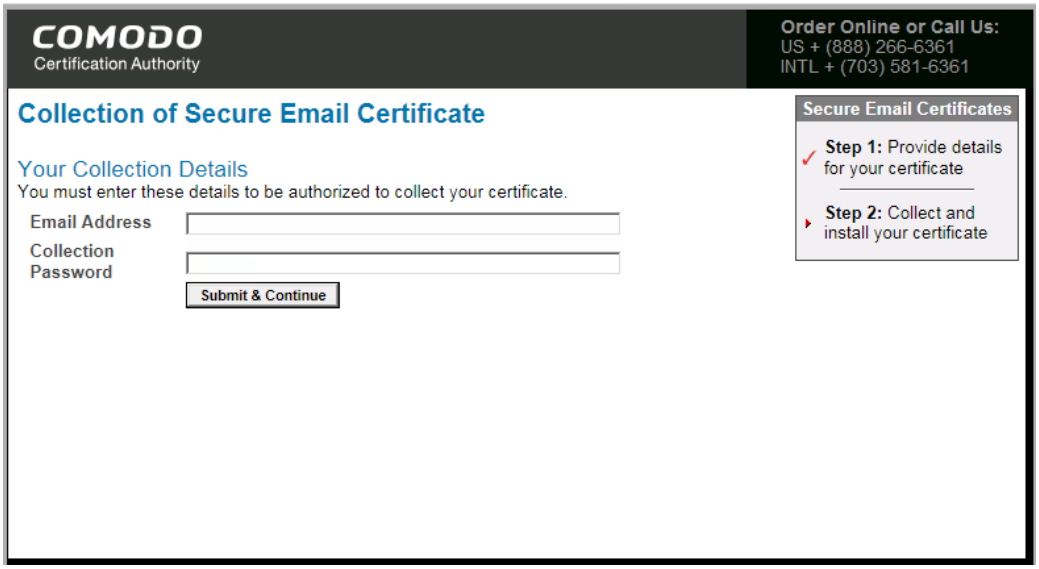
Bestätigen Sie die AGB und klicken auf „weiter“.
Nun erscheint folgende Meldung und Sie erhalten eine Mail in Ihrer Inbox.



In der Mail finden Sie folgenden Textabschnitt in ähnlicher Form:

„Note:- If the above button does not work, please navigate to
https://secure.comodo.net/products/!SecureEmailCertificate_Collec2
Enter your email address and the Collection Password which is: oLSQe23Utdz-0ZUX“

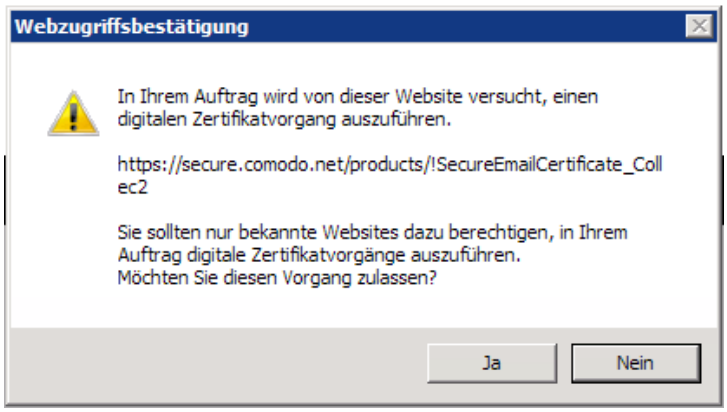
Folgen Sie der Anweisung, kopieren den Link in ein neues Browserfenster / Tab Ihres Internet Explorers und Sie bekommen folgende Anzeige:



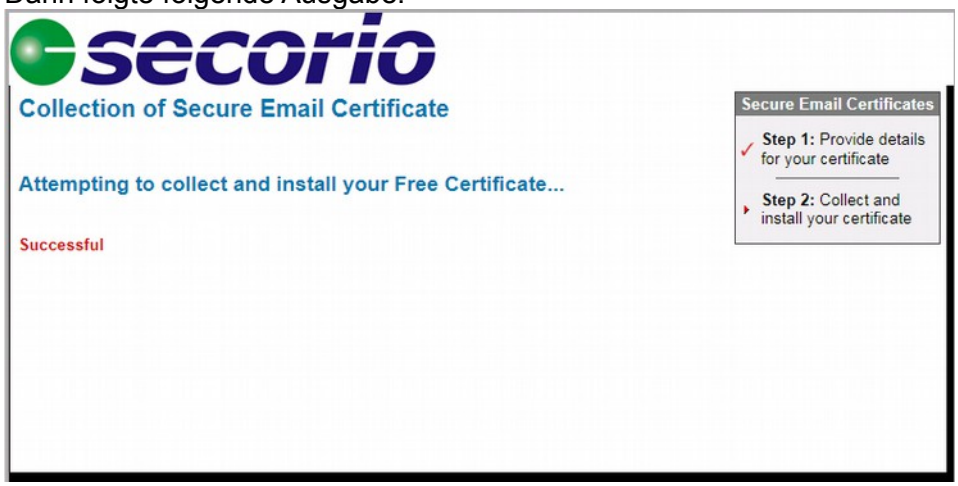
Tragen Sie die vergebene E-Mail-Adresse ein und geben Sie bei „Collection Password“ die Zeichenkombination nach „Password which is:“ ein.

Tipp: markieren Sie die Zeichenfolge und kopieren diese – Achten Sie auf vor- bzw. nachstehende Leerzeichen (die gehören nicht dazu!)

Wählen Sie nun „Submit & Continue“ und Sie bekommen evtl. wieder folgendes Fenster, dass Sie mit JA bestätigen:



Dann folgte folgende Ausgabe:



Sie haben erfolgreich ein Zertifikat erstellt nud auf Ihrem Rechner gespeichert!

Sichern des Zertifikates und Erstellen des public Keys

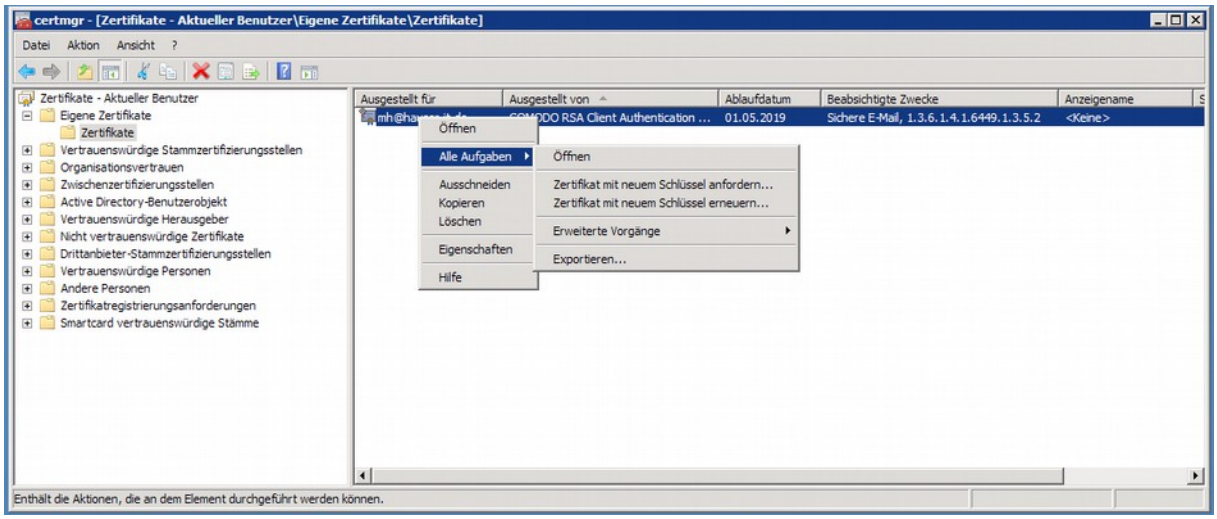
Starten des Verwaltungsprogramms - certmgr.msc

Geben Sie unter Windows „Ausführen“ den Programmnamen „certmgr.msc“ ein und bestätigen Sie dies mit Return.

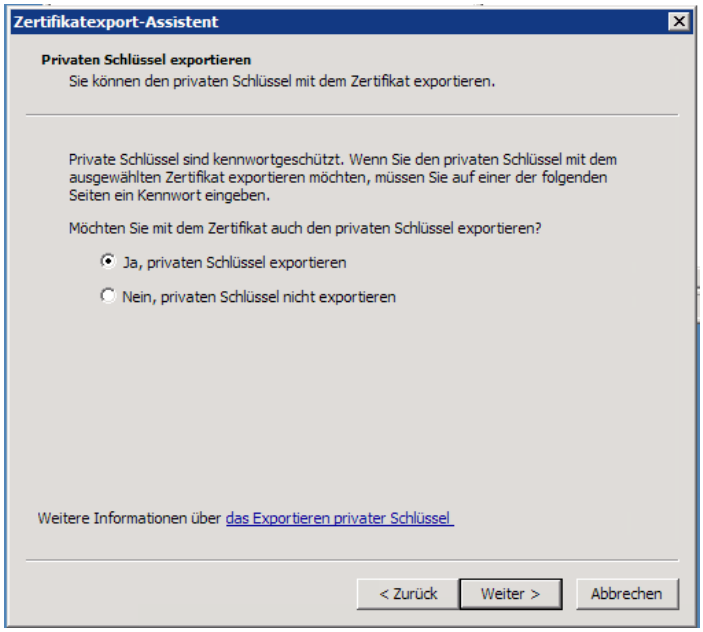
Exportieren des Zertifikates

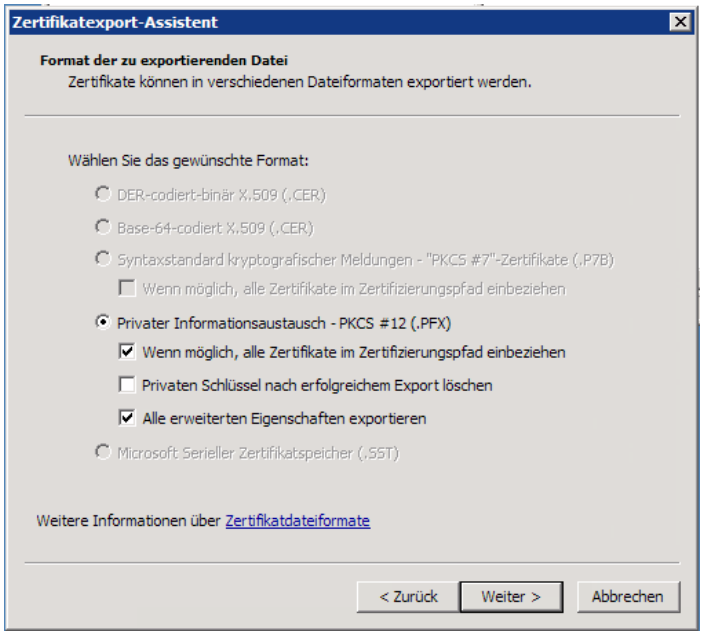
Wenn Sie nun unter „Eigene Zertifikate“ auf „Zertifikate“ klicken, finden Sie nun das, von Ihnen erstellte, Zertifikate auf dem rechten Fenster angezeigt.

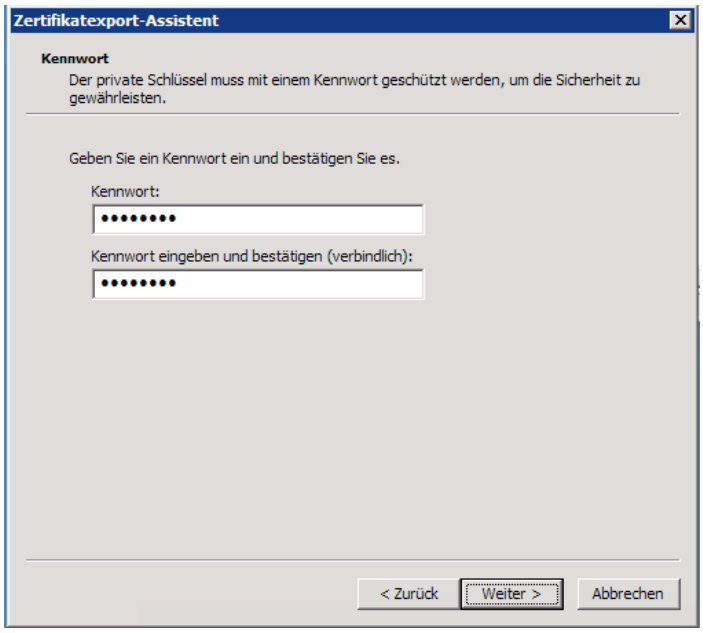
Klicken Sie mit der rechten Maustaste auf den Eintrag des Zertifikates und wählen aus „Alle Aufgaben“ den Unterpunkt „Exportieren...“

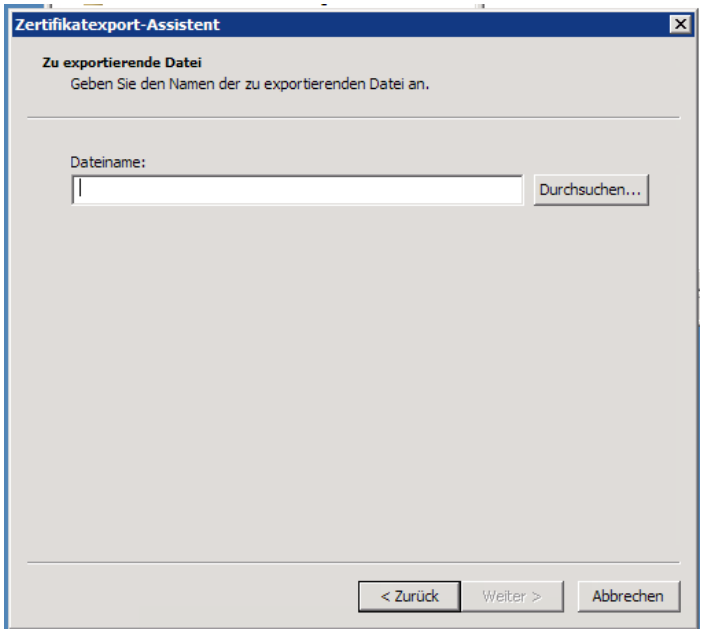


Exportieren des secret keys – Privater Schlüssel





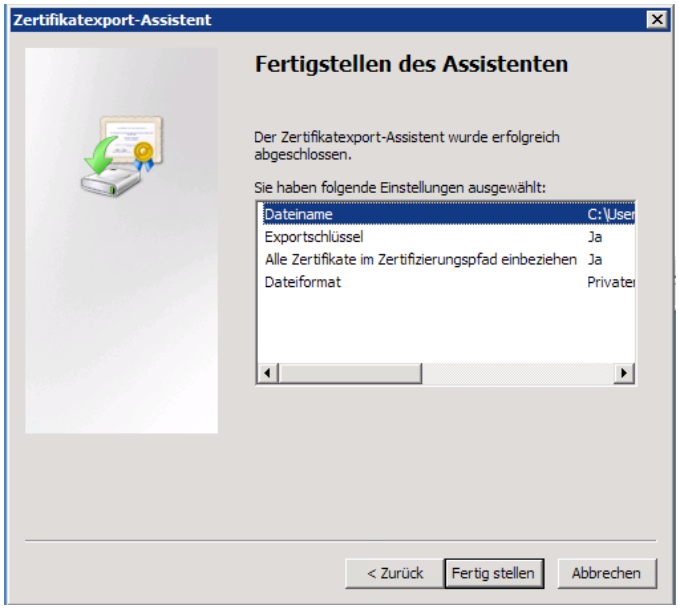


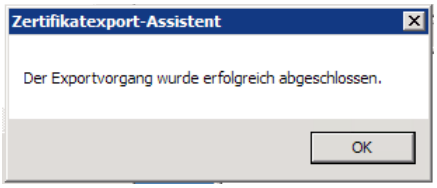


Tipp:
Vergeben Sie einen aussagekräftigen Namen für Ihr privates Zertifikat, damit Sie immer die Gewissheit haben, dass Sie beim Verwalten der Dateien das richtige Zertifikat verwenden, ohne es vorher öffnen zu müssen.

z.B.: C:\Users\User\Desktop\Vorname_Nachname_Comodo-Cert_-20190501.pfx

Sie können die Datei auch direkt auf einem USB-Stick erzeugen.

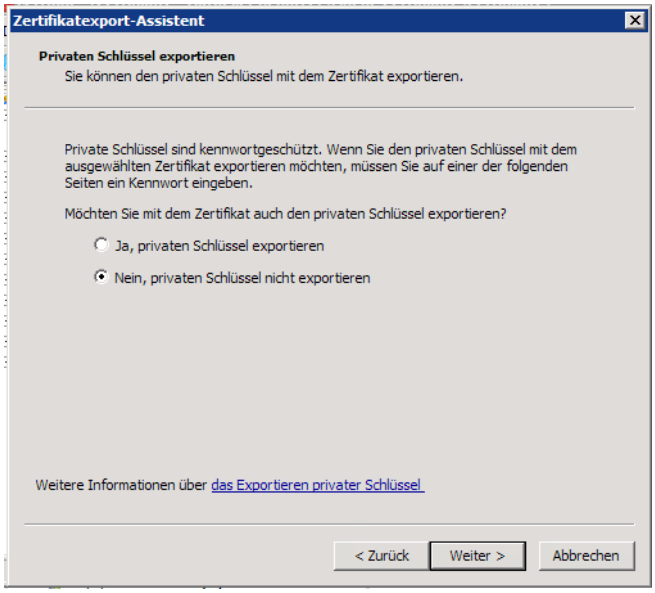


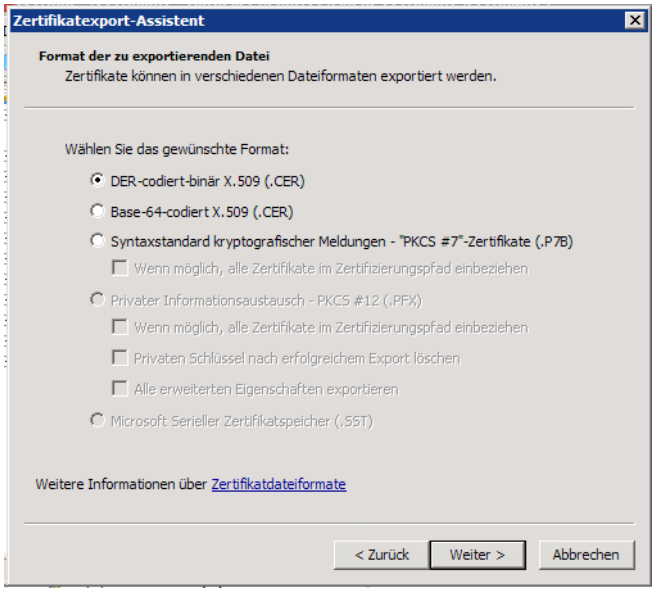


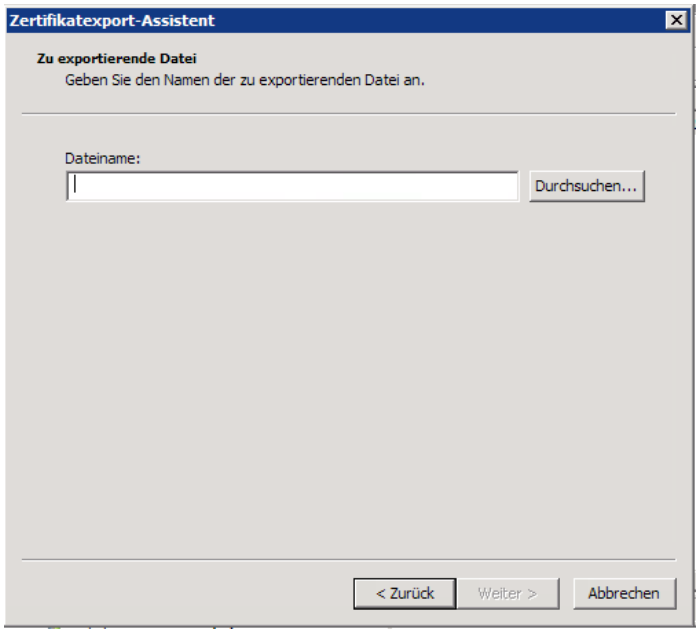
Achtung:
Die Datei und das bei Export verwendete Kennwort sollte nicht auf dem Rechner verbleiben, sondern idealer Weise auf einem externen Datenträger kopiert werden, der ausschließlich für Ihre Zertifikate verwendet wird. Legen Sie diesen mit einem verschlossenen Kuvert, in dem die Kennwörter genannt werden, in einen Tresor.

Exportieren public key – öffentlichen Schlüssel

Verfahren Sie anfangs wie bei dem Secret key und wählen dann aber wie folgt:

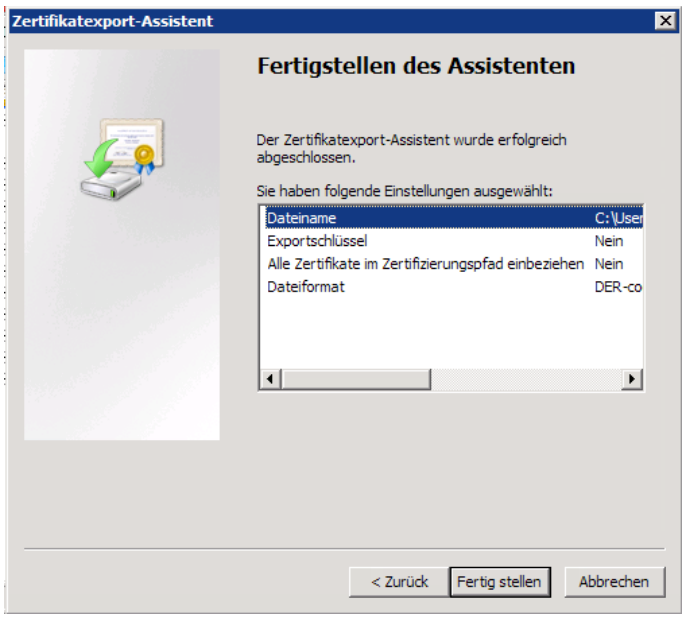


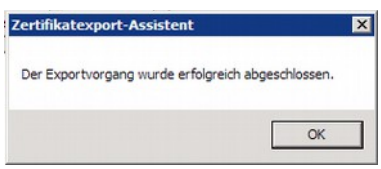




Tipp:
Vergeben Sie einen aussagekräftigen Namen für Ihr öffentliches Zertifikat, damit Sie und Ihr Kommunikationspartner immer die Gewissheit haben, dass Sie das richtige und gültige Zertifikat verwenden, ohne es vorher öffnen zu müssen.

z.B.: C:\Users\User\Desktop\Vorname_Nachname_Firmenname_-20190501.cer

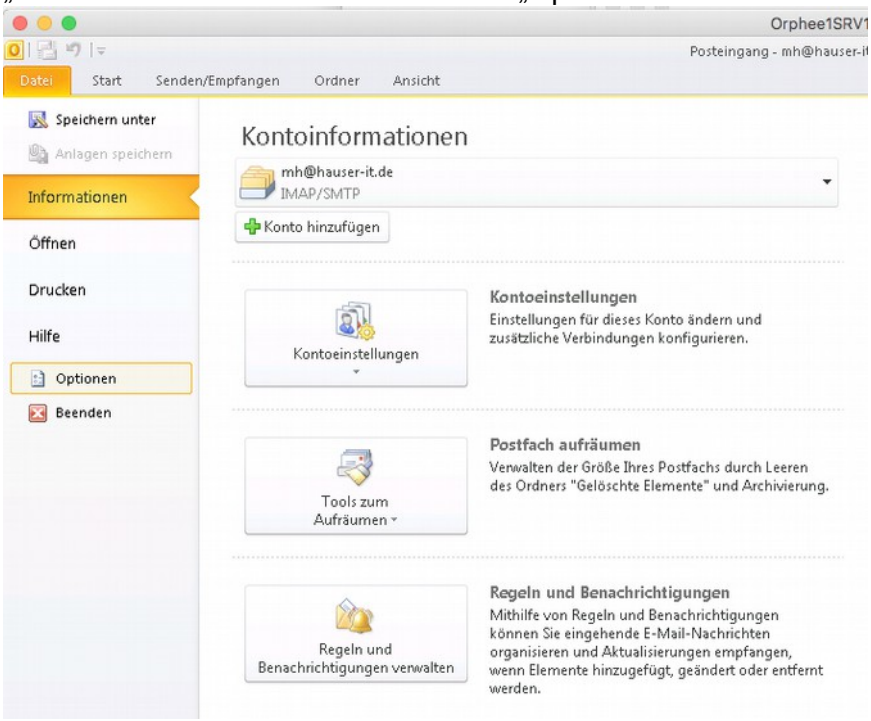




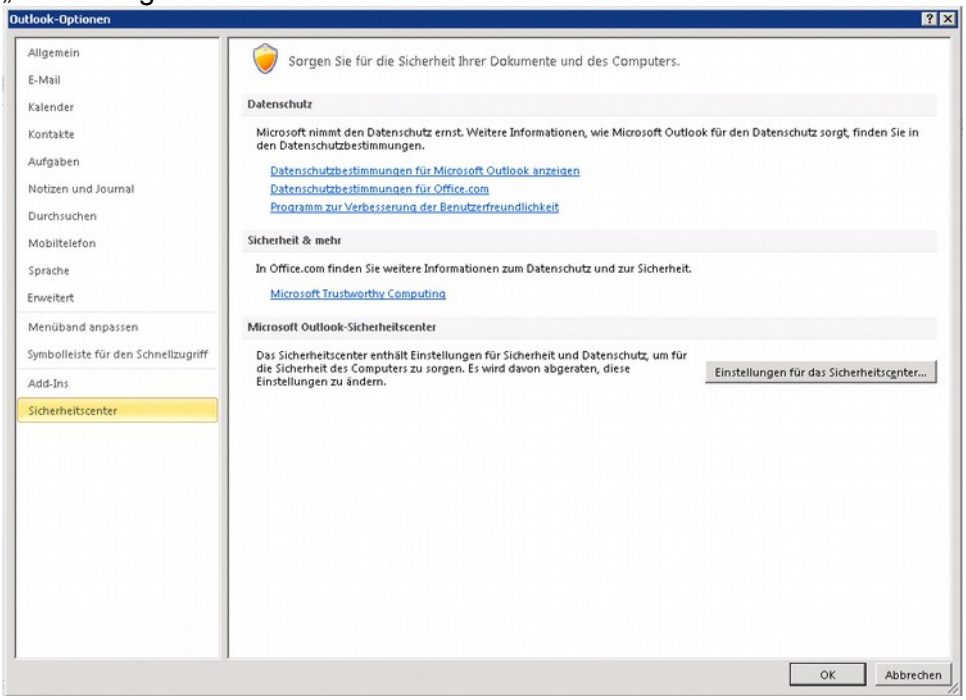
Zertifikate in Outlook

Eigenes Zertifikat in Outlook aktivieren

Zum aktivieren Ihres Zertifikates, dass bereits in der lokalen Zertifikatsverwaltung des Windows Betriebssystemes eingebunden ist, müssen Sie Outlook starten, und den Reiter „Datei“ auswählen und dann den Punkt „Optionen“



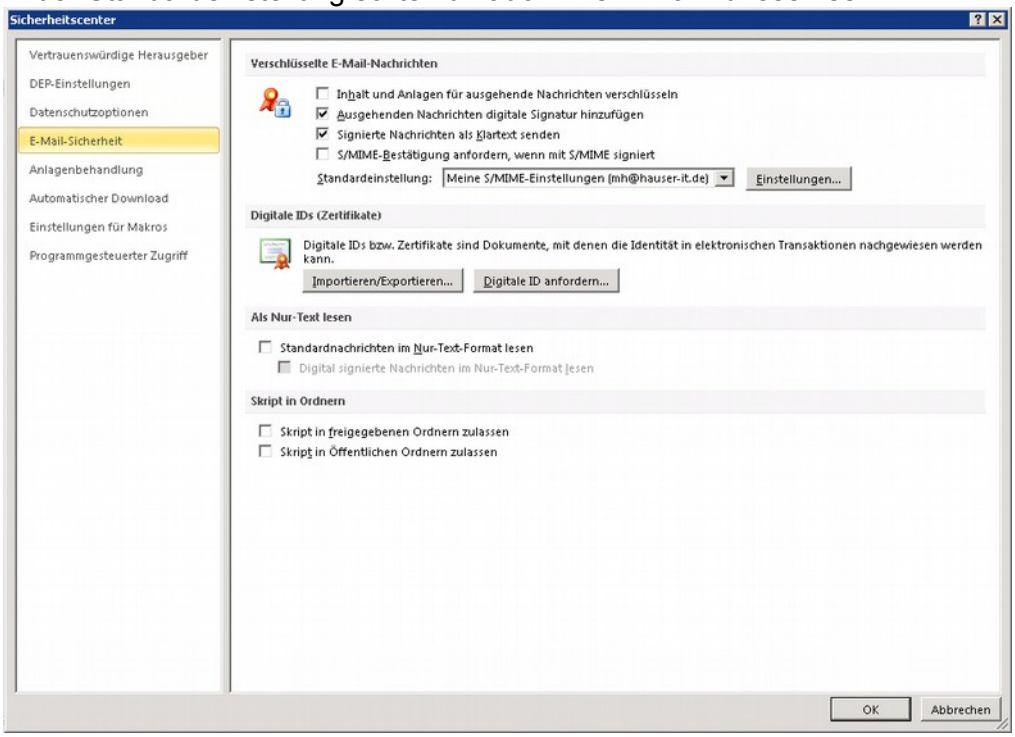
Im Fenster „Outlook-Optionen“ wählen Sie „Sicherheitscenter“ und in Folge den Punkt „Einstellungen für Sicherheitscenter“ in der rechten Fensterhälfte.



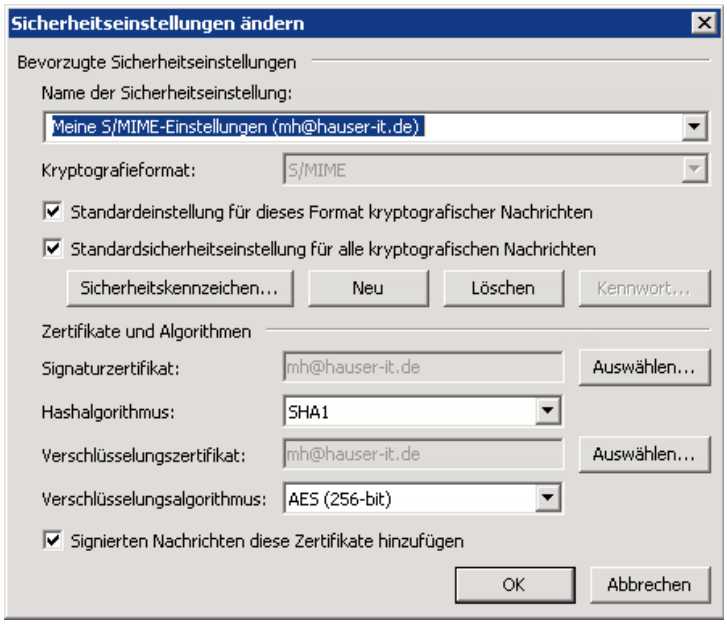
Im Fenster „Sicherheitscenter nun den Punkt „E-Mail-Sicherheit“ auswählen und die Haken entsprechend dem folgenden Abbild setzen.
Aktiv (mit Haken) sind:

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

In der Standardeinstellung sollte nun auch Ihre E-Mail zu lesen sein.



ggf. noch über den Punkt „Einstellungen“ prüfen, ob das Zertifikat angezeigt wird.

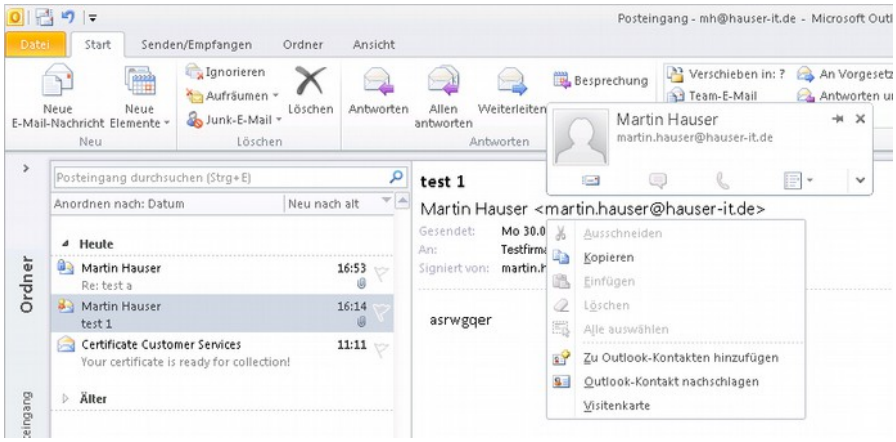


Alle Fenster mit OK schließen und damit die Änderungen speichern.

Neuen Kommunikationspartner zur verschlüsselten Kommunikation vorbereiten

Bekommen Sie eine Mail von einem Kommunikationspartner, die ebenfalls mit einem Zertifikat signiert ist, erkennen Sie dies an dem Symbol rechts (Siegel)

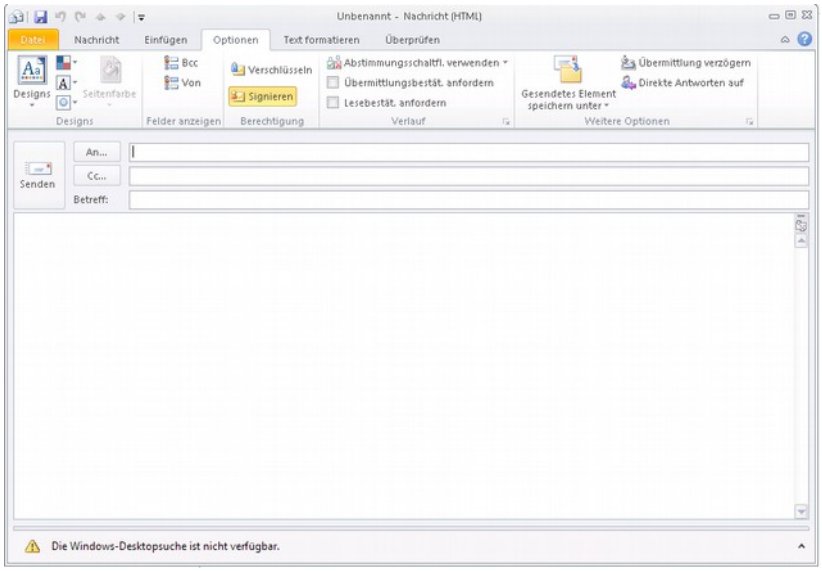
Nun müssen Sie lediglich in der empfangenen Mail mit der rechten Maustaste auf die Absendermailadresse klicken und im Menue den Punkt „Zu Outlook-Kontakten hinzufügen“ auswählen



Mailversand

signierte Mail an Empfänger

Öffnen Sie in Outlook eine neue Mail und wählen unter dem Reiter „Optionen“ den Punkt/Bereich „Signieren“ im Menueband aus. (dies sollte gemäß der vorherigen Einstellung aber bereits aktiviert sein)



verschlüsselte Mail an Empfänger

Öffnen Sie in Outlook eine neue Mail und wählen unter dem Reiter „Optionen“ den Punkt/Bereich „Verschlüsseln“ im Menueband aus.

Verschlüsselte Mails erkennen Sie an dem Symbol (blaues Schloß)