

# eMails digital signieren und verschlüsseln mit Zertifikaten

Martin Heinold, Andreas Hirsch  
Werdenfels-Gymnasium, Garmisch-Partenkirchen

## **GAPONLINE**

Bürgernetzverein für den Landkreis Garmisch-Partenkirchen e.V.

2007-02-22

## Inhaltsverzeichnis

<b>1</b>	<b>Prinzip und Arbeitsweise</b>	<b>2</b>
1.1	Signieren . . . . .	2
1.2	Verschlüsseln . . . . .	2
<b>2</b>	<b>Passwörter</b>	<b>3</b>
2.1	Drei Bereiche, die durch Passwörter geschützt werden . . . . .	3
2.2	Passwort für das Kryptographie-Modul einrichten . . . . .	3
<b>3</b>	<b>Ablauf</b>	<b>5</b>
3.1	Import des CA-Root-Zertifikats und der Revokation-URL in ihren Browser und ihr eMail-Programm . . . . .	5
3.2	Erstellung des CAcert-Accounts . . . . .	8
3.3	Bestätigung ihrer Identität . . . . .	11
3.4	Erzeugung des Zertifikats . . . . .	11
3.5	Zertifikat in das eMail-Programm installieren . . . . .	13
3.6	Konfiguration ihres eMail-Programms für die Zertifizierung . . . . .	15

# 1 Prinzip und Arbeitsweise

Wie auch beim GPG-System besteht das Zertifikat aus einem privaten und einem öffentlichen Teil.

## 1.1 Signieren

Bei einer digital unterschriebenen Mail ...

- ... ist sichergestellt, dass derjenige, der die Mail abgeschickt hat, den privaten Teil des Zertifikats besitzt und das Passwort zu dessen Verwendung kennt – nach menschlichem Ermessen also die Person ist, die im Zertifikat ausgewiesen ist.
- ... die Mail während des Transports durch das Internet nicht verändert werden kann.

Die Empfänger benötigen den öffentlichen Teil des Zertifikats, um die Signatur zu verifizieren. Der Vorteil des Zertifikatsystems gegenüber GPG ist nun, dass ...

- ... dieser Teil grundsätzlich mit der Mail geliefert wird.
- ... die Authentizität dieses Zertifikats bestätigt ist.

Daher entfällt der bei GPG nicht unerhebliche Aufwand, sich selbst um die öffentlichen Schlüssel zu bemühen und deren Authentizität selbst zu prüfen bzw. der Prüfung durch eine andere Person zu vertrauen. Ebenso entfällt die Pflege dieses privat geführten Keyrings.

Um diese Anforderungen zu erfüllen, muss das Verfahren, welches ein Zertifikat für gültig erklärt, zweifelsfrei sicherstellen, dass die angegebene eMail-Adresse wirklich zu der betreffenden Person gehört. Daher ist ein wenig Aufwand nicht vermeidbar.

## 1.2 Verschlüsseln

Die Verschlüsselung einer Mail stellt sicher, dass dritte keinen Zugriff auf den Inhalt haben.

Um eine Mail verschlüsseln zu können, benötigt man von jedem Empfänger dessen öffentlichen Teil des Zertifikats. Die Empfänger benötigen ihren privaten Teil des Zertifikats und das zugehörige Passwort. Damit gilt für die Zuverlässigkeit, dass nur die berechtigten Empfänger den Inhalt der Mail zu Kenntnis nehmen können, das gleiche wie oben beim Abschicken einer signierten Mail.

## 2 Passwörter

### 2.1 Drei Bereiche, die durch Passwörter geschützt werden

Im Laufe der Einrichtung des Systems werden an mehreren Stellen Passwörter erfragt. Diese lassen sich jeweils eine der drei folgenden Rubriken zuordnen:

**Accountpasswort für CAcert** Damit schützen sie den Zugriff auf ihren CAcert-Account. Diesen benötigen sie beispielsweise zur Erzeugung ihres Zertifikats sowie für alle zukünftigen Änderungen ihrer Daten (z.B. zugeordnete eMail-Adresse).

**Krypto-Passwort für Firefox bzw. Thunderbird** Dieses – auch Masterpasswort – genannte Passwort schützt den Zugriff auf das eingebaute Kryptographie-Modul welches zum einen ihre gespeicherten Anmeldedaten für Websites und eMail-Konten schützen kann (und deshalb vielleicht schon in Verwendung ist), zum anderen autorisiert es den Zugriff auf ihr Zertifikat.

**Backup-Passwort des Zertifikats** Dieses Passwort wird benötigt, wenn sie ihr Zertifikat als Datei auf der Festplatte speichern oder von dort laden. Es verhindert, dass fremde, denen diese Datei in die Hände fällt, ihre Identität annehmen können.

Die beiden letztgenannten Passwörter werden beide von Firefox bzw. Thunderbird (siehe 3.5) erfragt.

### 2.2 Passwort für das Kryptographie-Modul einrichten

Falls sie dieses Passwort noch nicht gesetzt haben sollten – es schützt den Zugriff auf die Anmeldedaten von Webseiten und Mailservern – empfiehlt es sich, dies nun – vor der eigentlichen Zertifikatseinrichtung – zu erledigen.

Führen sie dazu im Firefox und im Thunderbird folgende Schritte (in Klammern Thunderbird, falls anders bezeichnet) durch:

- Extras
- Einstellungen
- Erweitert (Datenschutz)
- Verschlüsselung (Sicherheit)

Sie erreichen dadurch das zentrale Einstellungsmenu (Bild 1), welches wir im weiteren Verlauf immer wieder als Ausgangspunkt benötigen werden. Klicken sie nun auf **Kryptographie-Module** und anschließend im linken Bereich (Bild 2) auf **Software-Kryptographie-Modul**. Nach einem Klick auf **Passwort ändern** erhalten sie den in Bild 3 gezeigten Dialog. Im Falle der erstmaligen Vergabe des Master-Passwortes sind nur die

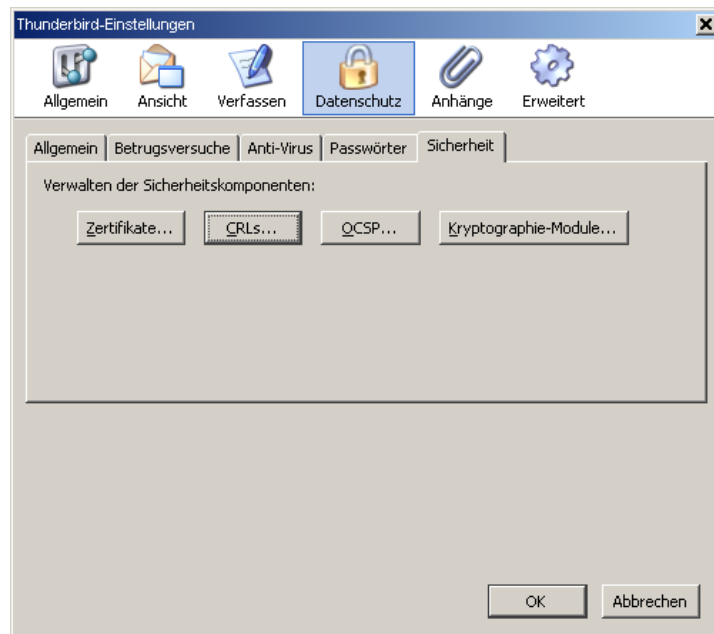


Abbildung 1: Der zentrale Ausgangspunkt: Die Registerkarte Sicherheit

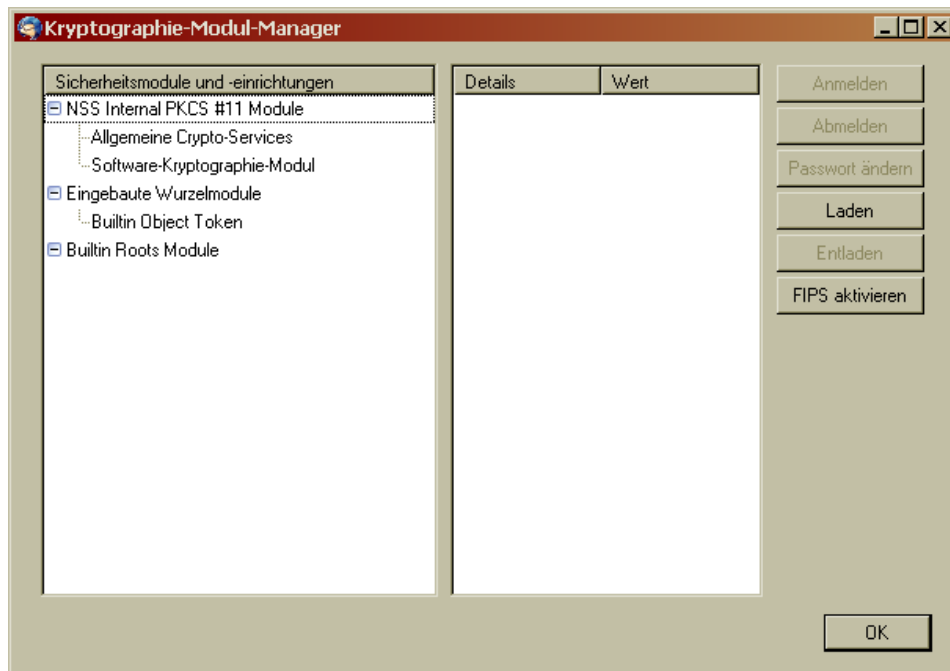


Abbildung 2: Kryptographie-Modul-Manager

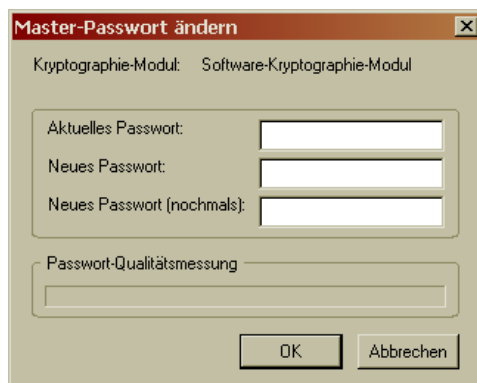


Abbildung 3: Dialogaufforderung zur Änderung des Master-Passwortes

beiden unteren Felder aktiv. Vergeben Sie ihr Passwort und beenden den Dialog mit **OK**, ebenso alle weiteren noch offenen Dialogfenster.

## 3 Ablauf

Je nach ihrer Arbeitsumgebung, Betriebssystem und den verwendeten Programmen sind nicht alle der nachfolgenden Schritte erforderlich. Unsere Beschreibung erklärt beispielhaft die Vorgehensweise bei Verwendung des Browsers Firefox und des eMail-Programms Thunderbird. Sie sollte es ihnen ermöglichen, diese Tätigkeiten auch in anderen Programmen zu finden.

### 3.1 Import des CA-Root-Zertifikats und der Revokation-URL in ihren Browser und ihr eMail-Programm

In den Programmen Firefox und Thunderbird ist die oberste Instanz des Zertifikatsystems CAcert leider noch nicht standardmäßig integriert<sup>1</sup>, daher ist es momentan noch erforderlich, diese sogenannten Root-Zertifikate in die beiden Programme zu importieren. Durch den Import dieser Root-Zertifikate vertrauen sie CAcert als oberste Instanz, dieses Vertrauen überträgt sich auf die untergeordneten (von CAcert bestätigten) Zertifikate.<sup>2</sup> Da dort die Gültigkeit der Zertifikate überwacht wird, gibt es regelmäßige Updates

<sup>1</sup>CAcert ist intensiv bemüht, die Mozilla-Organisation von der Integration zu überzeugen. In diesem Falle vereinfacht sich diese Anleitung deutlich.

<sup>2</sup>Nach dem gleichen Prinzip arbeiten auch viele Websites von Banken, welche beispielsweise ein Zertifikat von VeriSign vorweisen. Der Unterschied ist nur, dass ihr Browser der Firma VeriSign vertraut, ohne dass sie vorher gefragt wurden.

Class 1 PKI Schlüssel  
[Klicken Sie hier, wenn Sie das Root-Zertifikat in den Microsoft Internet Explorer importieren möchten.](#)  
[Root-Zertifikat \(PEM Format\)](#)  
[Root-Zertifikat \(DER Format\)](#)  
[CRL](#)

Class 3 PKI Schlüssel  
[Root-Zertifikat \(PEM Format\)](#)  
[Root-Zertifikat \(DER Format\)](#)

GPG/PGP Schlüssel  
[CAcerts GPG Key](#)

PKI Fingerprint mit dem CAcert GPG Key unterschrieben.

```
-----BEGIN PGP SIGNED MESSAGE-----  
Hash: SHA1  
  
For most software, the fingerprint is reported as:  
A6:1B:37:5E:39:0D:9C:36:54:EE:ED:20:31:46:1F:6B  
  
Under MSIE the thumbprint is reported as:  
135C EC36 F49C B8E9 3B1A B270 CD80 8846 76CE 8F23  
-----BEGIN PGP SIGNATURE-----
```

Abbildung 4: Download des CA-Root-Zertifikates und der Revocation-URL

über abgelaufene und zurückgezogene Zertifikate. Sie müssen ihrem Browser und ihrem eMail-Programm mitteilen, von wo es diese Updates erhält.

Besuchen Sie die Internetadresse <https://www.cacert.org/index.php?id=3> und speichern sie – jeweils durch Rechtsklick auf **Root Certificate (PEM Format)** – in den Abschnitten **Class 1 PKI Key** und **Class 3 PKI Key** (Bild 4) die Root-Zertifikate auf ihrer Festplatte. Wir werden diese (siehe unten) gleich in ihren Browser und in ihr eMail-Programm importieren, nutzen aber zuvor die gerade geladene Webseite für einen nächsten Schritt:

Kopieren sie mit einem Rechtsklick auf **CRL** die Revocation-URL in die Zwischenablage (Link-Adresse kopieren) und führen sie dann die aus 2.2 auf Seite 3 bereits bekannten Schritte bis zur Registerkarte Sicherheit (Bild 1) durch!

Anschließend gehen sie wie folgt weiter vor:

- Klicken sie dort auf Revocation-Listen bzw. CRL
- Importieren
- Kopieren sie dann den Inhalt der Zwischenablage hinein (STRG-V) oder Rechtsklick → Einfügen (Bild 5) und bestätigen sie mit OK
- Warten sie auf die Bestätigung (Bild 6) des erfolgreichen Imports und klicken sie in dieser auf JA
- Aktivieren sie das Auto-Update wie in Bild 7 gezeigt

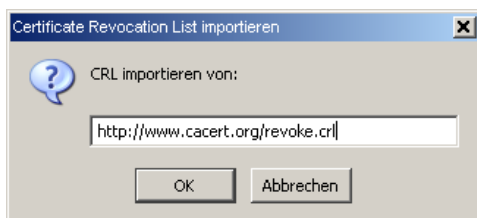


Abbildung 5: CRL-Adresse einfügen

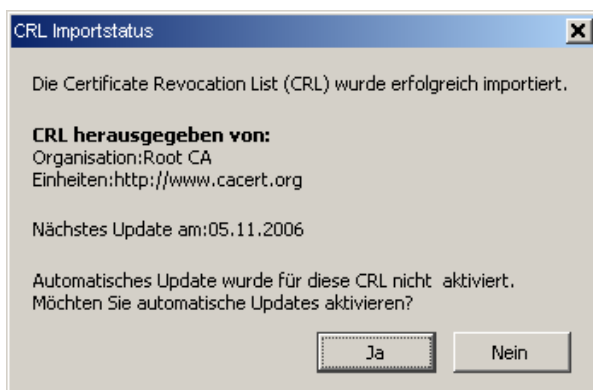


Abbildung 6: Bestätigung des erfolgreichen CRL-Imports

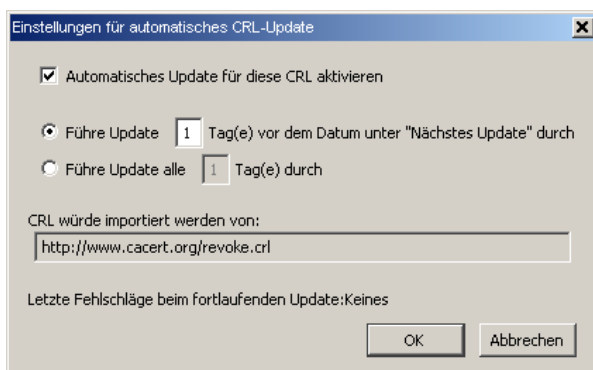


Abbildung 7: Updateeinstellungen für die Revocation-Liste

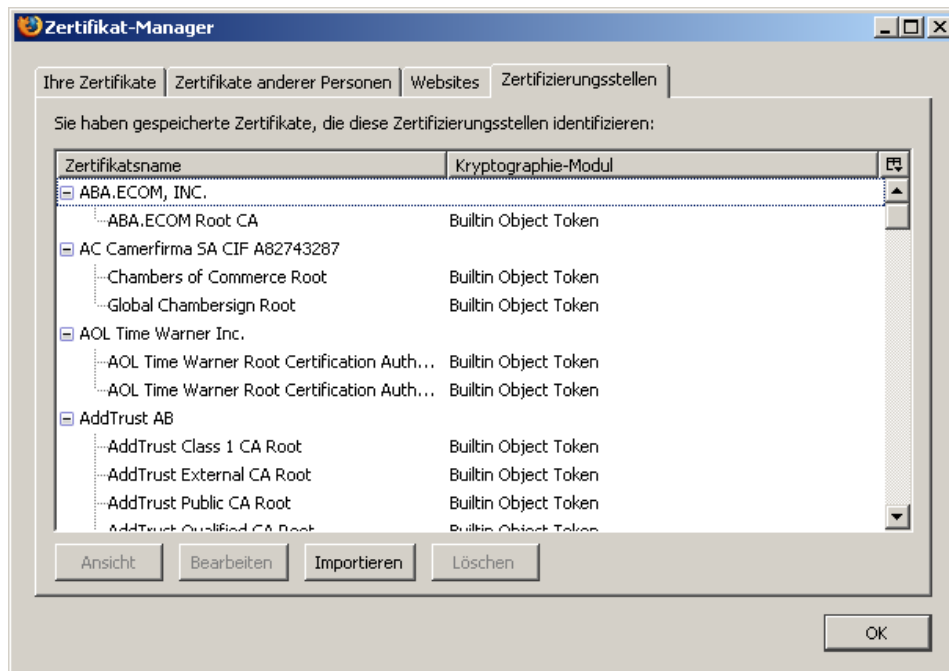


Abbildung 8: Zertifizierungsstellen verwalten

Nun müssen sie nur noch das Root-Zertifikat, das sie bereits auf ihrer Festplatte gespeichert haben, in ihren Browser und in ihr eMail-Programm importieren:

- Begeben sie sich dazu *in beiden Programmen* wieder zur Registerkarte Sicherheit (siehe 2.2 auf Seite 3)
- Klicken sie auf Zertifikate
- Wählen sie die Karteikarte Zertifizierungsstellen (Bild 8)
- Klicken sie auf importieren und wählen sie den Speicherort (Bild 9) der eben gespeicherten Root-Zertifikate
- Wählen sie für den ersten Import `root.crt`
- Bestätigen Sie die Verwendungsmöglichkeiten für dieses Zertifikat (Bild 10)

Wiederholen sie diese Schritte für das zweite Root-Zertifikat (`class3.crt`)

Führen sie nun die gleichen Schritte in ihrem eMail-Programm durch!

### 3.2 Erstellung des CAcert-Accounts

Besuchen Sie die Internetadresse <https://www.cacert.org/index.php?id=1> (Bild 11) und füllen Sie das Formular aus.

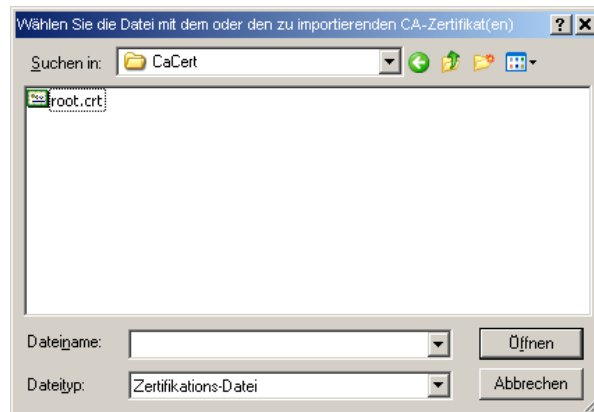


Abbildung 9: Zertifikat von der Festplatte laden

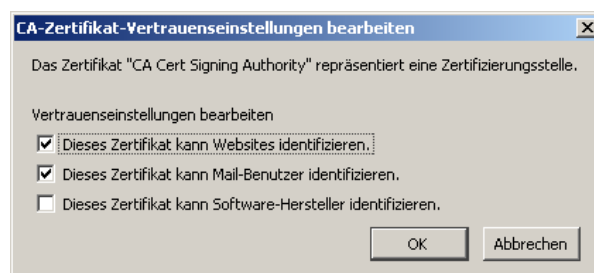


Abbildung 10: Verwendungsmöglichkeiten des Zertifikats festlegen

Meine Details	
Vorname:	<input type="text"/>
Mittlere Namen (optional)	<input type="text"/>
Familienname:	<input type="text"/>
Suffix (optional)	<input type="text"/>
Geburtsdatum (tt/mm/jjjj)	7 <input type="text"/> Januar (1) <input type="text"/>
E-Mail Adresse:	<input type="text"/>
Passwort*:	<input type="password"/>
Passwort bestätigen*:	<input type="password"/>
*Bitte beachten Sie, dass aus Sicherheitsgründen Ihr Passwort aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen bestehen muss.	
Ich-habe-mein-Passwort-vergessen-Fragen: Bitte geben Sie aus Sicherheitsgründen fünf Fragen und die dazupassenden Antworten ein, die sie in 5 Jahren möglichst identisch beantworten können sollten.	
1)	<input type="text"/>
2)	<input type="text"/>
3)	<input type="text"/>
4)	<input type="text"/>
5)	<input type="text"/>
Es ist möglich Benachrichtigungen über bevorstehende Veranstaltungen oder allgemeine Ankündigungen zu erhalten. Entfernen Sie den jeweiligen Haken wenn Sie darüber keine Benachrichtigung erhalten wollen. Damit lokale Benachrichtigungen funktionieren müssen Sie einmal Ihren Standort auswählen nachdem Ihr Konto überprüft wurde und Sie eingeloggt sind.	
Benachrichtige mich bei:	<input checked="" type="checkbox"/> Allgemeine Ankündigungen <input checked="" type="checkbox"/> Landesankündigungen <input checked="" type="checkbox"/> Regionale Ankündigungen <input checked="" type="checkbox"/> Ankündigungen innerhalb von 200 km
<input type="button" value="Weiter"/>	

Abbildung 11: Antrag auf Erstellung eines CAcert-Accounts

**Aktualisiert**

Ihr Konto und/oder Ihre E-mail-Adresse wurde verifiziert. Sie können nun Zertifikate für diese Adresse ausstellen.

Abbildung 12: CAcert-Account erfolgreich angelegt

Sie erhalten nach kurzer Zeit eine eMail um sicherzustellen, dass die angegebene eMail-Adresse gültig ist. Klicken sie auf den Link in dieser eMail. Daraufhin wird eine Website geladen, auf der sie die Verwendung dieser eMail-Adresse bestätigen müssen.

Damit ist ihr Account bei CAcert angelegt, das Angebot, ein Zertifikat anzulegen (Bild 12) nehmen wir jedoch jetzt noch *nicht* wahr. (Dieses vorläufige Zertifikat ist zwar voll funktional, allerdings nicht mit ihrer Person assoziiert. Wir werden daher erst die Assoziierung durchführen und müssen dadurch nur einmal ein Zertifikat erzeugen und importieren)

### 3.3 Bestätigung ihrer Identität

Damit ihr Account gültig wird (genau genommen: Dass ihr Account eindeutig ihrer Person zugeordnet ist), müssen sie sich persönlich mit Personen treffen, die schon einen höheren Status im System haben (sogenannte *Assurer*) und sich diesen gegenüber ausweisen. Der Assurer wird dann ihre Identität im System bestätigen und darüber eine Niederschrift anfertigen, die auch sie unterzeichnen müssen.

Um die Sicherheit zu erhöhen, kann ein einzelner Assurer in der Regel nur max. 35 Punkte vergeben, für die Gültigkeit ihres Zertifikats sind aber 50 Punkte erforderlich. Sie benötigen also mindestens zwei Assurer.

Sobald sie selbst 100 Punkte erreicht haben, können sie sich selbst als Assurer betätigen.

### 3.4 Erzeugung des Zertifikats

**Ihr Zertifikat wird nach der Erzeugung im Browser nur bei ihnen gespeichert! Sie sollten daher das exportierte Zertifikat unbedingt auf einem externen Datenträger speichern und sicher aufbewahren. CAcert kann dieses Zertifikat nicht erneut bereitstellen – ihre bis dahin verschlüsselten eMails bleiben für immer verschlüsselt!**

Nachdem sie von den Assurern mindestens 50 Punkte erhalten haben (sie erhalten jedesmal eine Bestätigungsmail) melden sie sich wieder auf der CAcert-Seite (<https://www.cacert.org/index.php?id=4>) mit ihren Accountdaten an (Bild 13).

Nach der erfolgreichen Anmeldung (Bild 14) wählen sie Client-Zertifikate und dann Neu.

Login	
Email Address:	<input type="text" value="sysadmin@werdenfels-g"/>
Pass Phrase:	<input type="password" value="*****"/>
<input type="button" value="Login"/>	

Abbildung 13: Auf CAcert anmelden

CAcert.org
<a href="#">Go Home</a>
<a href="#">Logout</a>
<b>+ My Details</b>
<b>+ Email Accounts</b>
<b>+ Client Certificates</b>
<b>+ Domains</b>
<b>+ Server Certificates</b>
<b>+ CAcert Web of Trust</b>
<b>+ CAP/TTP Forms</b>
<b>+ GPG/PGP Keys</b>
<b>+ Disputes/Abuses</b>

Abbildung 14: Auf CAcert erfolgreich angemeldet

Neues Client-Zertifikat	
Hinzufügen	Adresse
<input checked="" type="checkbox"/>	marcus@bitzl.com
<input type="radio"/> Signieren mit dem Klasse 1 Root Zertifikat <input checked="" type="radio"/> Signieren mit dem Klasse 3 Root Zertifikat Bitte beachten Sie: Das Klasse 3 Root Zertifikat und das Klasse 1 Zertifikat müssen beide in Ihr E-Mail-Programm installiert/importiert werden, damit das Programm den vollständigen Vertrauenspfad (Trust-Path) überprüfen kann. Bis in Zukunft das CAcert Zertifikat von den Browserherstellern vorinstalliert wird, dürfte das für die meisten Benutzer eine weniger wünschenswerte Option sein.	
<input type="radio"/> Kein Name <input checked="" type="radio"/> Einfügen 'Marcus Bitzl'	
Optional Client CSR, no information on the certificate will be used	
<div style="border: 1px solid black; height: 40px; width: 100%;"></div>	
<input type="button" value="Weiter"/>	

Abbildung 15: Zertifikat erstellen

**Installieren Ihres Zertifikats**

Sie sind dabei, ein Zertifikat zu installieren. Wenn Sie Mozilla/Netscape/Firefox basierte Browser verwenden, werden Sie nicht informiert, dass das Zertifikat erfolgreich installiert wurde. Sie können in die Einstellungen gehen, unter Security und Zertifikatsverwaltung können Sie sehen, ob das Zertifikat korrekt installiert wurde.

[Klicken Sie hier](#) um Ihr Zertifikat zu installieren.

Abbildung 16: Zertifikat erfolgreich erstellt – Import starten

Ergänzen Sie das Formular wie in Bild 15 gezeigt und schicken sie die Seite mit Weiter ab.

Bestätigen Sie die vorgeschlagene Schlüsselqualität.

Nach der erfolgreichen Zertifikatserstellung (Bild 16) werden sie aufgefordert, das Zertifikat in ihren Browser zu installieren. Beachten sie, dass der Firefox bis Version 1.5 den erfolgreichen Abschluss dieser Aktion leider *nicht* bestätigt. Im nächsten Schritt wird sich jedoch gleich zeigen, ob es erfolgreich importiert wurde.

### 3.5 Zertifikat in das eMail-Programm installieren

Das eben in den Browser importierte Zertifikat wird nun aus diesem ex- und in das eMail-Programm importiert. Führen sie dazu wieder folgende Schritte durch:

- Extras → Einstellungen
- Rubrik Erweitert
- Registerkarte Sicherheit (siehe Bild 1)

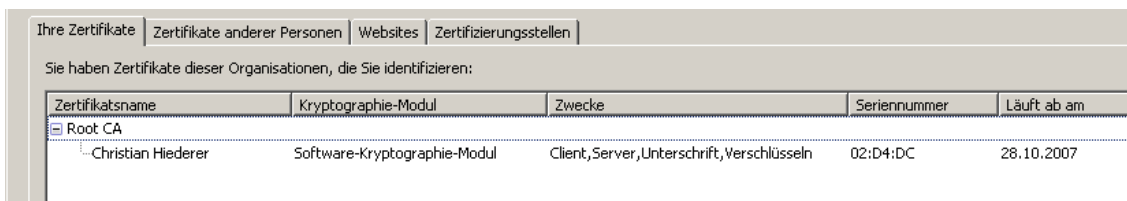


Abbildung 17: Zertifikatsverwaltung im Browser

- Klicken sie dort auf Zertifikate (siehe Bild 1)
- Wählen sie die Karteikarte Ihre Zertifikate (siehe Bild 17)
- Markieren sie ihr Zertifikat
- Backup
- Speicherort des Zertifikats wählen

Im Verlauf des Exports müssen sie zwei Passwörter wählen. Beachten sie hierzu die Erläuterungen in 2! Wir empfehlen (sofern noch kein Masterpasswort vergeben wurde), für beide Zwecke das gleiche Passwort zu verwenden. (siehe Bild 18) Dieses sollte jedoch

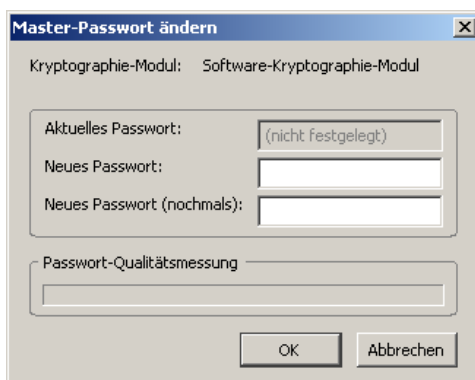


Abbildung 18: Erstellung der Masterpassworts

nicht das Passwort für ihren CAcert-Account sein, da dieses ja auf fremden Rechnern liegt und somit nicht zusätzlich für private Zwecke eingesetzt werden sollte.

Nach dem erfolgreichen Export des Zertifikats kann es nun in das eMail-Programm importiert werden. Dazu müssen sie nur in diesem an die gleiche Stelle gehen wie eben im Browser:

- Extras → Einstellungen
- Rubrik Datenschutz
- Registerkarte Sicherheit (siehe Bild 1)

- Klicken sie dort auf Zertifikate (siehe Bild 1)
- Wählen sie die Karteikarte Ihre Zertifikate (siehe Bild 17)
- Importieren
- Sie werden nun nach ihrem Krypto-Passwort (siehe 2) gefragt (bzw. zur erstmaligen Neuanlage dieses Passwortes aufgefordert)
- Speicherort wählen
- Geben sie nun das Backup-Passwort ein, welches sie eben (beim Abspeichern des Zertifikats auf Festplatte) vergeben haben
- OK

### 3.6 Konfiguration ihres eMail-Programms für die Zertifizierung

Zum Schluss richten wir nun ihr eMail-Programm so ein, dass es das Zertifikat verwendet. Führen sie dazu folgende Schritte durch:

- Extras → Konten
- S/MIME-Sicherheit (Bild 19)
- Klicken sie auf Auswählen
- Bestätigen sie den Vorschlag (Bild 20)
- Vorschlag für Verschlüsselungszertifikat annehmen (Bild 21)
- Haken bei Nachrichten digital unterschreiben setzen

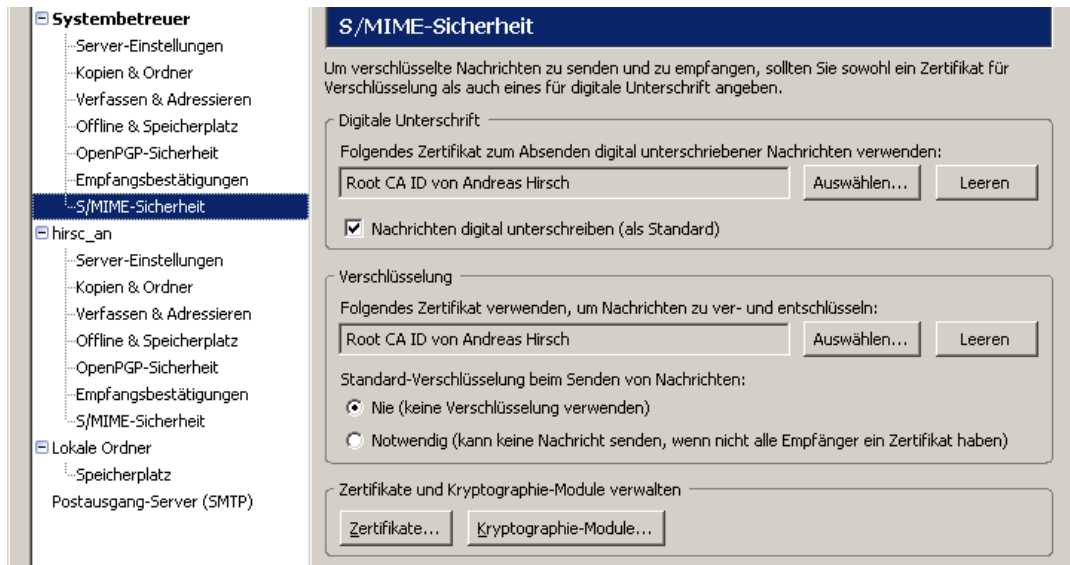


Abbildung 19: Zertifikatsverwaltung im eMail-Programm

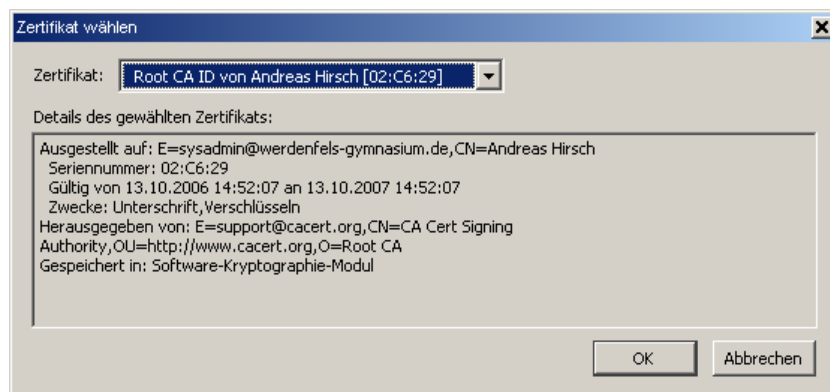


Abbildung 20: Zertifikat auswählen

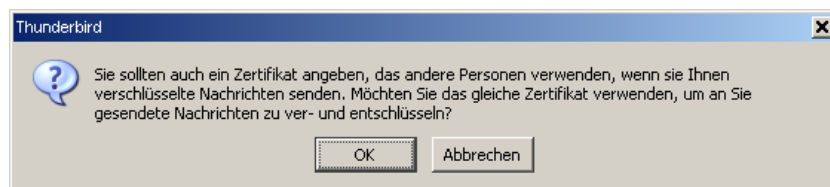


Abbildung 21: Zertifikat für die Verschlüsselung bestätigen