S/MIME Zertifikat beantragen und benutzen

(Stand: 05. 01. 2016)

1. Einführung
2. *Master*-Passwort für *Firefox* setzen (bei Mozilla-Produkten **notwendig**)
3. S/MIME Zertifikat in *Browser Mozilla Firefox* beantragen
4. Zertifikat in *Browser Mozilla Firefox* importieren
5. *Backup* eines Zertifikats in *Browser Mozilla Firefox* erstellen
6. Zertifikate in *E-Mail-Client* importieren und benutzen
   - 6.1. Mozilla Thunderbird
     - 6.1.1. *Master*-Passwort setzen
     - 6.1.2. Eigenes Zertifikat importieren
     - 6.1.3. Fremdes Zertifikat manuell importieren
     - 6.1.4. LDAP-Verzeichnis-*Server* einrichten
     - 6.1.5. Zertifikate anzeigen
     - 6.1.6. E-Mail signieren/verschlüsseln
   - 6.2. Novell GroupWise-Windows Client
     - 6.2.1. Eigenes Zertifikat importieren
     - 6.2.2. Fremdes Zertifikat manuell importieren
     - 6.2.3. LDAP-Verzeichnis-*Server* einrichten
     - 6.2.4. Zertifikate anzeigen
     - 6.2.5. E-Mail signieren/verschlüsseln
   - 6.3. Novell GroupWise WebAccess Client

1. Einführung

S/MIME (Secure / Multipurpose Internet Mail Extensions) ist ein Standard, den heutige *E-Mail-Clients* unterstützen und mit dem eine *E-Mail* einfach verschlüsselt und/oder signiert werden kann. Neben einem privaten Schlüssel wird ein öffentlicher Schlüssel benötigt, der von einer vertrauenswürdigen Instanz mit einem Zertifikat beglaubigt wird. Es gibt verschiedene Klassen von Zertifikaten, die sich in der Überprüfung des Antragstellers unterscheiden. In der niedrigsten Klasse 1 wird nur überprüft, ob die *E-Mail*-Adresse existiert, die in das Zertifikat übernommen wird, während sich der Antragsteller in der Klasse 3 persönlich ausweisen muss. Im Zertifikat stehen dann unter anderem der Name des Besitzers, die *E-Mail*-Adresse und der von der Zertifizierungsstelle digital signierte öffentliche Schlüssel.

Mit dem öffentlichen Schlüssel des Empfängers der *E-Mail* wird eine Nachricht verschlüsselt, sodass der Empfänger sie mit seinem privaten Schlüssel entschlüsseln und dann lesen kann. Der öffentliche Schlüssel darf also frei verteilt werden, während der private Schlüssel sehr gut geschützt werden muss. Öffentliche Schlüssel können zum Beispiel einer signierten *E-Mail* entnommen oder eventuell auch in der Datenbank einer Zertifizierungsstelle gesucht werden. Falls Sie den öffentlichen Schlüssel des Empfängers nicht kennen, müssen Sie den Empfänger zuerst bitten, Ihnen eine signierte *E-Mail* zu schicken, bevor Sie Ihre Nachricht an den Empfänger verschlüsseln können.

Das Schlüsselpaar (privater und öffentlicher Schlüssel) sollte lokal erzeugt werden (z. B. mithilfe des *Browsers Firefox*), damit der private Schlüssel wirklich nur dem Antragsteller bekannt ist. Der öffentliche Schlüssel wird dann zur Zertifizierungsstelle hochgeladen, die ihn mit einem Zertifikat versieht. Danach wird der zertifizierte öffentliche Schlüssel wieder in den *Browser* importiert und dort zusammen mit dem privaten Schlüssel im Zertifikatsspeicher gespeichert. Anschließend sollten

beide Schlüssel exportiert und zum Beispiel in einem verschlüsselten Dateisystem eines *Memory-Sticks* gespeichert werden. Auf diese Weise können beide Schlüssel auch auf andere Rechner übertragen werden. Eine verschlüsselte *E-Mail* kann nur mit einem *E-Mail-Client* gelesen werden, der den privaten Schlüssel kennt. Der private Schlüssel kann nicht neu erzeugt und auch nicht von irgendwo heruntergeladen werden. Die beiden Schlüssel sollten daher unbedingt exportiert und geschützt verwahrt werden. Weitere Informationen finden Sie in der Wikipedia Enzyklopädie: https://de.wikipedia.org/wiki/S/MIME.

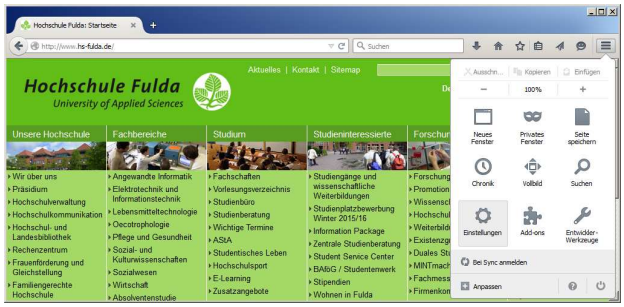
Sie sollten jede *E-Mail* mit Ihrer S/MIME-Signatur versehen, um Ihren zertifizierten öffentlichen Schlüssel zu verbreiten. Die meisten *E-Mail-Clients* sammeln alle öffentlichen Schlüssel Ihrer *Mail*-Partner automatisch ein, sodass Ihnen dann verschlüsselte Nachrichten geschickt werden können.

Aus historischen Gründen gibt es an der Hochschule Fulda eine externe und eine interne *E-Mail*-Adresse, die sich voneinander unterscheiden. Wenn die externe *E-Mail*-Adresse (Vorname.Nachname@...hs-fulda.de) für das Zertifikat benutzt wird, können signierte und/oder verschlüsselte Nachrichten an der Hochschule Fulda deshalb zurzeit nur mit dem *E-Mail-Client Mozilla Thunderbird* bearbeitet werden, der immer die externe *E-Mail*-Adresse verwendet. Der *E-Mail-Client Novell GroupWise-Windows* benutzt dagegen die interne *E-Mail*-Adresse (fd-Nummer@fhfd...), die natürlich nicht mit der *E-Mail*-Adresse des Zertifikats übereinstimmt, sodass Nachrichten mit diesem *Client* weder signiert noch verschlüsselt werden können. Mit dem *Novell GroupWise WebAccess Client* können aus Sicherheitsgründen nur „normale“ Nachrichten gesendet und gelesen werden.

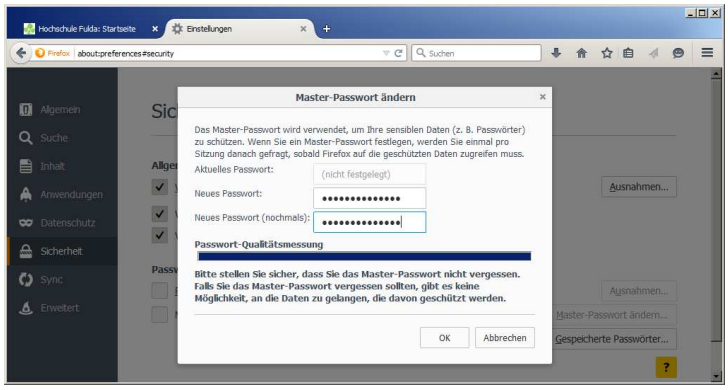
Zurzeit können signierte und/oder verschlüsselte Nachrichten nur mit *Mozilla Thunderbird* bearbeitet werden, da Zertifikate nur mit der externen *E-Mail*-Adresse „Vorname.Nachname@...hs-fulda.de“ erstellt werden sollen.

2. Master-Passwort für *Firefox* setzen (bei Mozilla-Produkten **notwendig**)

Firefox und *Thunderbird* schützen sensible Daten nur dann richtig, wenn Sie ein *Master*-Passwort benutzen. Sie sollten daher bei Mozilla-Produkten (*Firefox* und/oder *Thunderbird*) zuerst ein *Master*-Passwort setzen, bevor Sie einen privaten Schlüssel erzeugen oder importieren. Klicken Sie in der rechten oberen Ecke von *Firefox* auf das *Icon* mit den drei waagerechten Linien und dann auf „Einstellungen“. Die folgenden Abbildungen wurden mit *Firefox 38.0.5* erstellt, der eine zu *Firefox 37.x* veränderte Oberfläche aufweist („Einstellungen“ werden nicht mehr als neues Fenster sondern als neuer „Tab“ dargestellt).



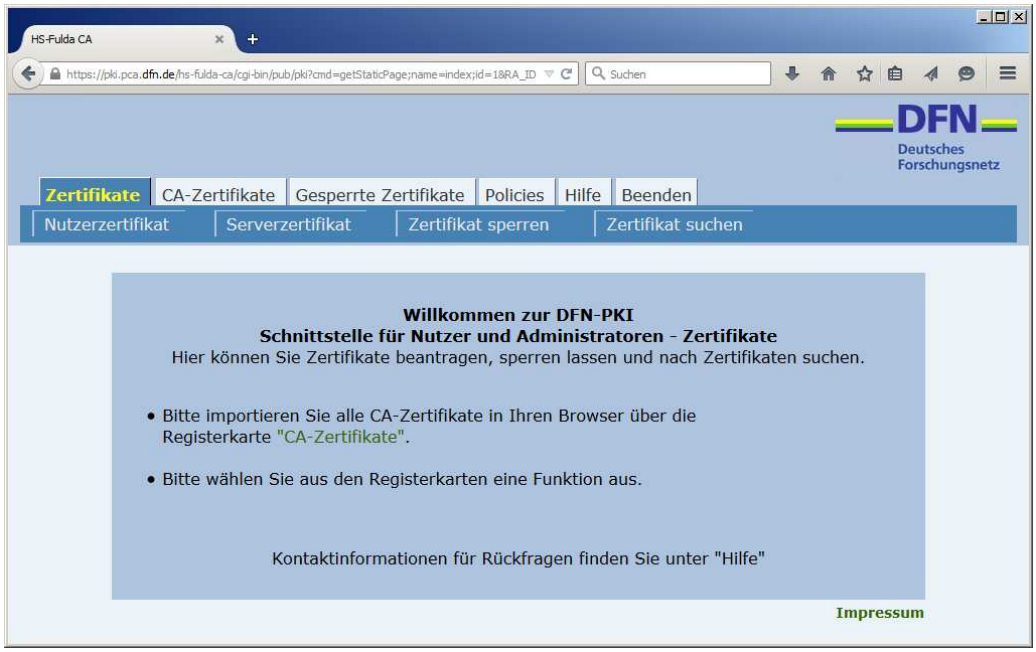
Wählen Sie den Bereich „Sicherheit“ aus und setzen Sie dann einen Haken vor „Master-Passwort verwenden“. Danach öffnet sich ein Fenster, in dem Sie das *Master*-Passwort setzen können. Wählen Sie ein gutes Passwort, das den Richtlinien der Hochschule Fulda entspricht, die Sie auf der Web-Seite https://www.hs-fulda.de/it-sicherheit finden (dort „Passwörter“ auswählen und Abschnitt 2 lesen).



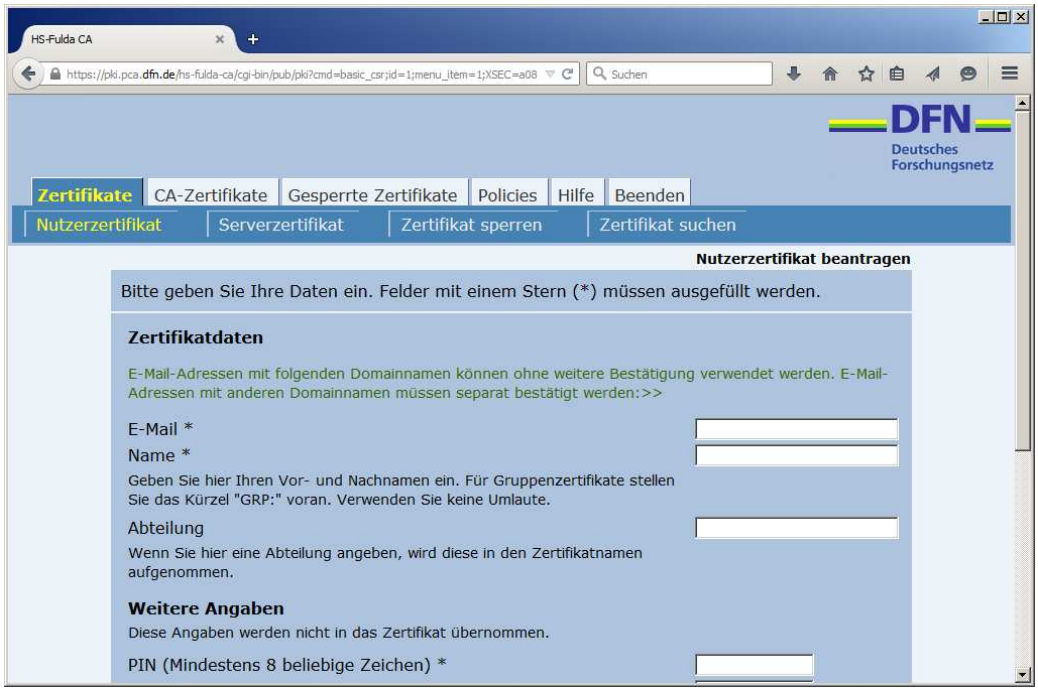
3. S/MIME Zertifikat in *Browser Mozilla Firefox* beantragen

Ein CA-Zertifikat kann über die CA-Web-Seite der Hochschule Fulda beantragt werden, indem zum Beispiel im *Browser Firefox* die folgende Adresse aufgerufen wird.

http://www.hs-fulda.de/hs-fulda-ca

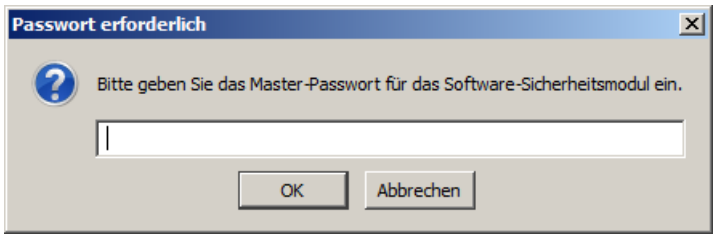


Dort wird der Abschnitt *Nutzerzertifikat* ausgewählt.



Wählen Sie eine gute PIN, die den Richtlinien für Passwörter der Hochschule Fulda entspricht, die Sie auf der Web-Seite https://www.hs-fulda.de/it-sicherheit finden (dort „Passwörter“ auswählen und Abschnitt 2 lesen). Sie sollten außerdem hinter „Ich stimme der *Veröffentlichung des Zertifikats* mit meinem darin enthaltenen Namen und der *E-Mail*-Adresse zu.“ einen Haken setzen, damit Ihr Zertifikat über den *Public-Key-Server* des DFN-Vereins gefunden wird. Nachdem Sie alle Angaben

eingetragen und bestätigt haben, werden Sie nach Ihrem *Master*-Passwort gefragt, bevor das Schlüsselpaar erzeugt wird.



Danach wird eine PDF-Datei mit dem Antrag erzeugt, die Sie ausdrucken. Unterschreiben Sie den Antrag und geben Sie ihn anschließend im Rechenzentrum ab, das ihn weiter bearbeitet. Denken Sie daran, Ihren **Personalausweis** mitzunehmen, da Sie sich identifizieren müssen. Der private Schlüssel für das Zertifikat wurde im *Browser* erzeugt und gespeichert, **sodass der zertifizierte öffentliche Schlüssel später nur in dem *Browser* importiert werden kann, von dem das Zertifikat beantragt worden ist.** Jetzt müssen Sie auf die *E-Mail* mit der Bestätigung zum Zertifikat warten, die u. a. folgende Informationen enthält.

...

Sehr geehrte Nutzerin, sehr geehrter Nutzer,

die Bearbeitung Ihres Zertifizierungsantrags ist nun abgeschlossen.

Ihr Zertifikat mit der Seriennummer xxxxxxxx ist auf den Namen
...

2. Ihr eigenes Zertifikat erhalten Sie direkt über folgenden Link:

https://pki.pca.dfn.de:443/hs-fulda-ca/...

Befolgen Sie bitte die in dem Dokument „Informationen für Zertifikatinhaber“ aufgeführten Regelungen: https://info.pca.dfn.de/doc/Info_Zertifikatinhaber.pdf
...

In der oben genannten PDF-Datei stehen unter Punkt 5 die folgenden Anweisungen:
...

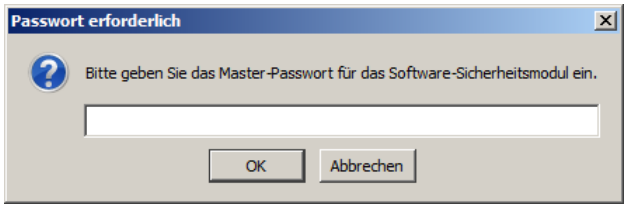
Insbesondere **muss bei Einsatz von Mozilla-Produkten ein „Master-Passwort“ gesetzt werden**.
...

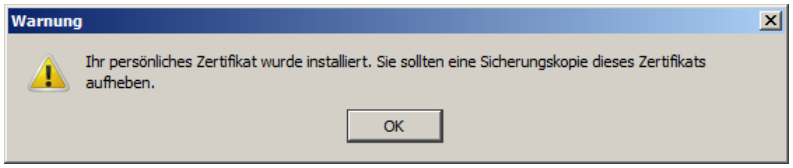
Die **Passphrase/PIN** darf nur Ihnen bekannt sein und muss **mindestens 8 Zeichen** lang sein.
...

4. Zertifikat in *Browser Mozilla Firefox* importieren

Klicken Sie auf die Web-Adresse für Ihr Zertifikat, die Ihnen mit der Bestätigungs-*Mail* zugeschickt worden ist und dann auf „Zertifikat importieren“.

Sie werden jetzt aufgefordert, Ihr *Master*-Passwort einzugeben. Danach wird das Zertifikat installiert.

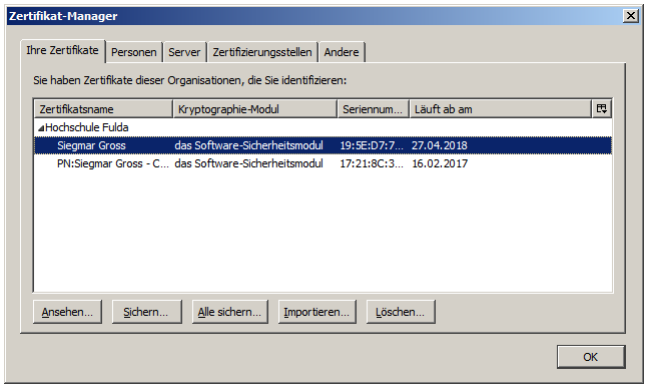




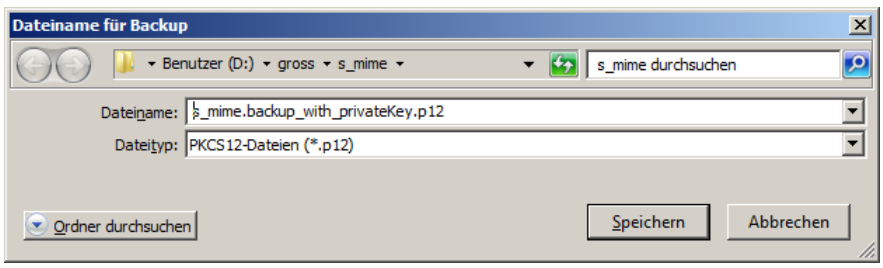
Falls Sie versuchen, das Zertifikat in einem *Browser* zu importieren, von dem Sie das Zertifikat nicht beantragt haben, erhalten Sie folgende Fehlermeldung.

5. *Backup* eines Zertifikats in *Browser Mozilla Firefox* erstellen

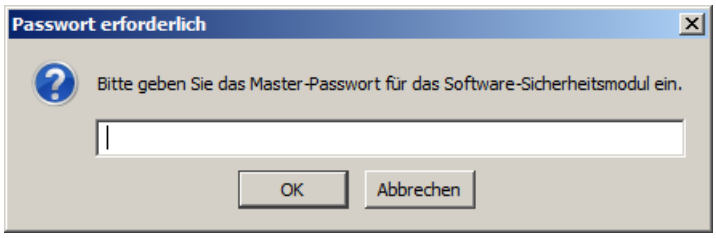
Klicken Sie wieder in der rechten oberen Ecke von *Firefox* auf das *Icon* mit den drei waagerechten Linien und dann auf „Einstellungen“. Wählen Sie den Bereich „Erweitert“ und dann den Reiter „Zertifikate“ aus. Klicken Sie anschließend auf „Zertifikate anzeigen“. Danach wird Ihnen das Fenster des Zertifikat-Managers angezeigt.

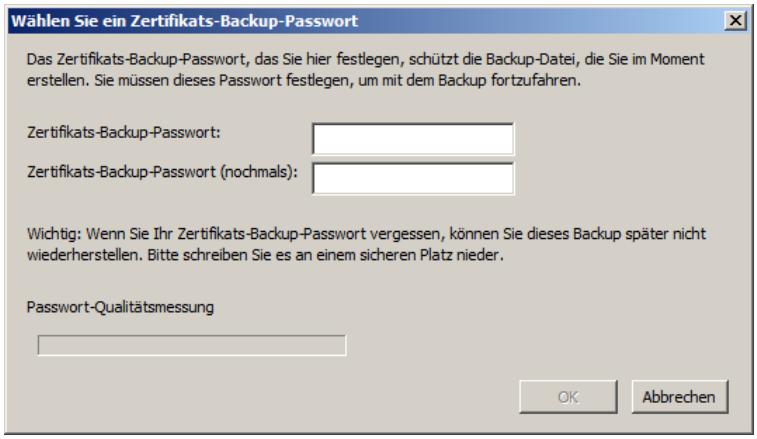


Wählen Sie das Zertifikat aus und klicken Sie dann auf „Sichern…“ oder auf „Alle sichern…“, wenn Sie alle Zertifikate sichern wollen. Wählen Sie ein Verzeichnis und einen Namen für die Datei und klicken Sie dann auf „Speichern“.



Sie werden zuerst nach dem *Master*-Passwort und dann nach einem Passwort für die *Backup*-Datei gefragt, bevor das Zertifikat gespeichert wird. Denken Sie daran, dass Sie ein gutes Passwort wählen, das den Richtlinien der Hochschule Fulda entspricht, die Sie auf der Web-Seite https://www.hs-fulda.de/it-sicherheit finden (dort „Passwörter“ auswählen und Abschnitt 2 lesen).


Passwort erforderlich
Bitte geben Sie das Master-Passwort für das Software-Sicherheitsmodul ein.
OK
Abbrechen


Wählen Sie ein Zertifikats-Backup-Passwort
Das Zertifikats-Backup-Passwort, das Sie hier festlegen, schützt die Backup-Datei, die Sie im Moment erstellen. Sie müssen dieses Passwort festlegen, um mit dem Backup fortzufahren.
Zertifikats-Backup-Passwort:
Zertifikats-Backup-Passwort (nochmals):
Wichtig: Wenn Sie Ihr Zertifikats-Backup-Passwort vergessen, können Sie dieses Backup später nicht wiederherstellen. Bitte schreiben Sie es an einem sicheren Platz nieder.
Passwort-Qualitätsmessung
OK
Abbrechen

Warnung
Ihre Sicherheits-Zertifikate und privaten Schlüssel wurden erfolgreich gesichert.
OK

6. Zertifikate in *E-Mail-Client* importieren und benutzen

In Kapitel 1 wurde bereits erwähnt, dass die meisten *E-Mail-Clients* öffentliche Schlüssel Ihrer *Mail*-Partner automatisch sammeln, sodass Sie ihnen verschlüsselte Nachrichten senden können. Wenn Ihr *E-Mail-Client* den öffentlichen Schlüssel Ihres *Mail*-Partners nicht kennt, haben Sie die folgenden Möglichkeiten den Schlüssel zu erhalten, um Ihrem *Mail*-Partner eine verschlüsselte Nachricht zu schicken.

1) Sie bitten ihren *Mail*-Partner, Ihnen eine signierte *E-Mail* zu schicken, sodass Ihr *E-Mail-Client* den öffentlichen Schlüssel automatisch importieren kann.

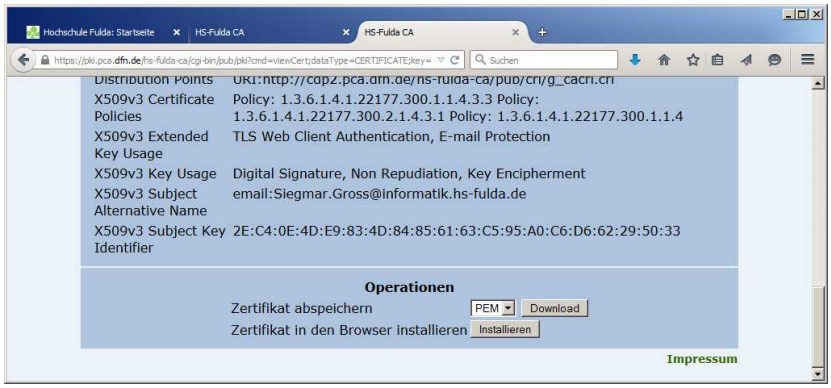
2) Sie suchen das Zertifikat Ihres *Mail*-Partners auf einem *Public-Key-Server*, um es danach manuell in Ihren *E-Mail-Client* zu importieren. Benutzen dafür Sie z. B. die folgende Adresse.

   http://www.hs-fulda.de/hs-fulda-ca

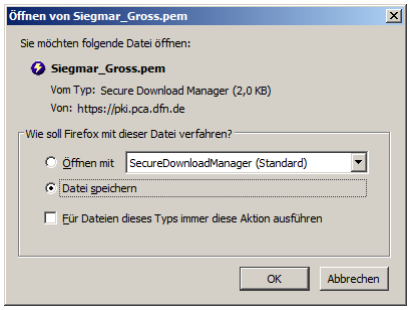
Dort wählen Sie „Zertifikat suchen“ aus und geben dann den Namen der Person oder die *E-Mail*-Adresse ein.

Klicken Sie auf das „i“ links neben der Seriennummer und gehen Sie dann an das Ende der

neuen Anzeige.



Klicken Sie auf „Download“ und speichern Sie das Zertifikat. **Achtung:** Wenn Sie das Zertifikat in den *GroupWise-Windows Client* importieren wollen, müssen Sie zuerst den Dateityp von „PEM“ auf „DER“ ändern, da *GroupWise* nur „CER“- und „DER“-Dateien importieren kann.



Sie können das Zertifikat anschließend manuell in den *E-Mail-Client* importieren. Dieser Vorgang wird in einem Unterkapitel der beiden folgenden Kapitel zu *Mozilla Thunderbird* und *Novell GroupeWise-Windows Client* beschrieben.

3) Sie richten in Ihrem *E-Mail-Client* einen LDAP-Verzeichnis-*Server* ein. Dieser Vorgang wird ebenfalls in einem Unterkapitel der beiden folgenden Kapitel zu *Mozilla Thunderbird* und *Novell GroupeWise-Windows Client* beschrieben.

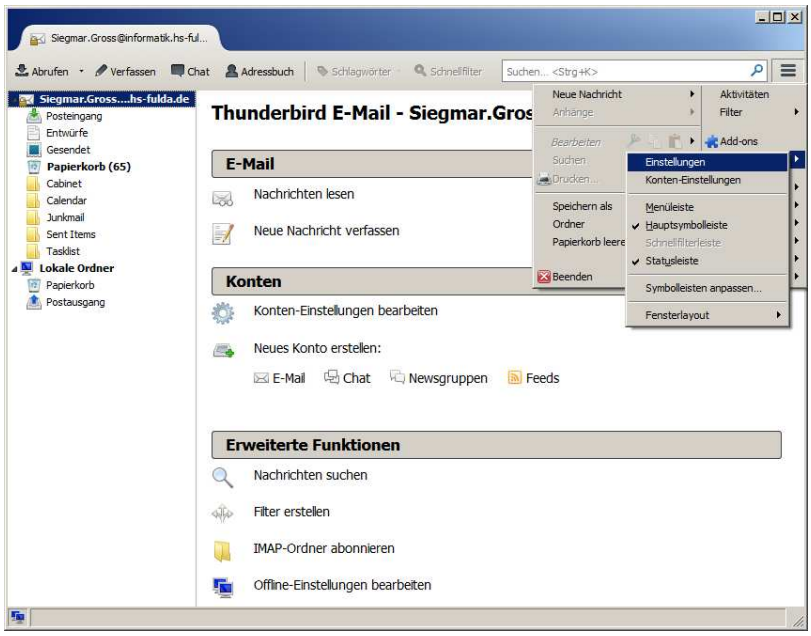
6.1. Mozilla Thunderbird

Auf den folgenden Web-Seiten finden Sie Informationen zu „Mozilla Thunderbird“.

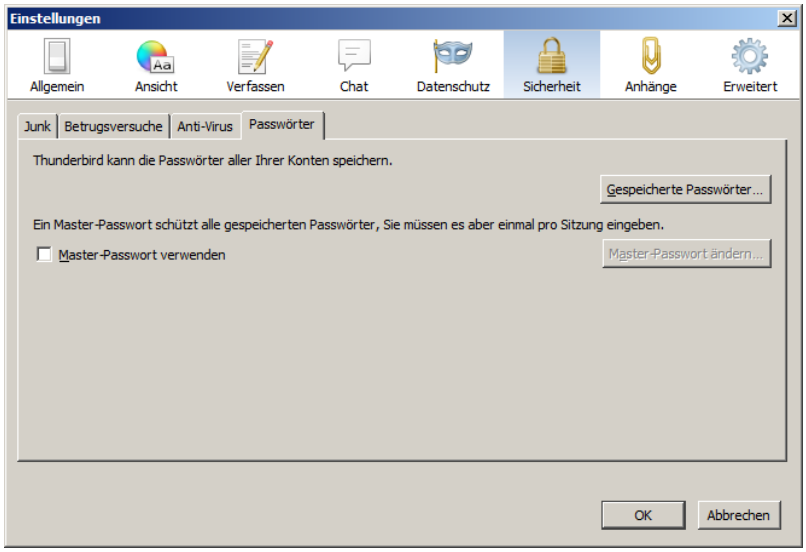
https://support.mozilla.org/en-US/products/thunderbird
http://en.flossmanuals.net/_booki/thunderbird/thunderbird.pdf
http://kb.mozillazine.org/Message_security

6.1.1. *Master*-Passwort setzen

Starten Sie *Thunderbird* und klicken Sie in der rechten oberen Ecke von *Thunderbird* auf das *Icon* mit den drei waagerechten Linien, dann auf „Einstellungen“ und anschließend wieder auf „Einstellungen“. Die folgenden Abbildungen wurden mit *Thunderbird 38.0.1* erstellt.



Wählen Sie dann den Abschnitt „Sicherheit“ und dort den Reiter „Passwörter“ aus

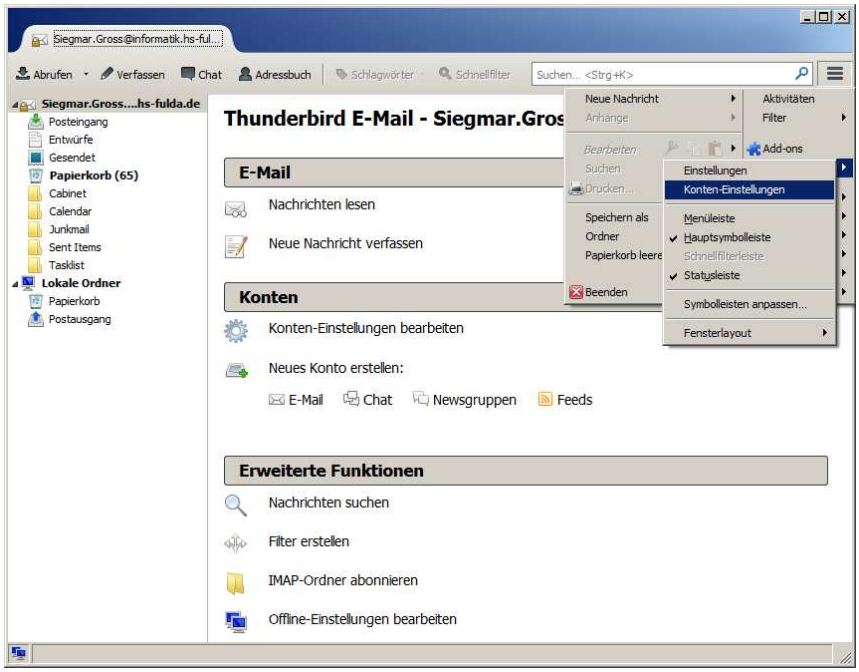


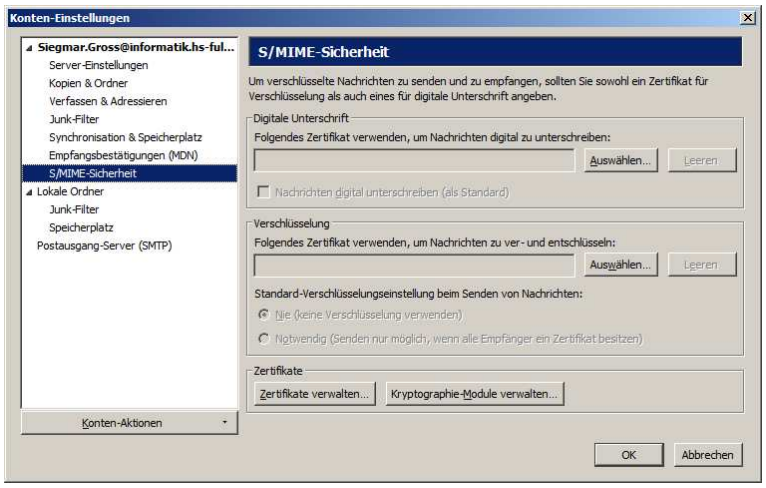
Setzen Sie einen Haken vor „Master-Passwort verwenden“. Danach öffnet sich ein Fenster, in dem

Sie das *Master*-Passwort setzen können. Wählen Sie ein gutes Passwort, das den Richtlinien der Hochschule Fulda entspricht, die Sie auf der Web-Seite https://www.hs-fulda.de/it-sicherheit finden (dort „Passwörter“ auswählen und Abschnitt 2 lesen).

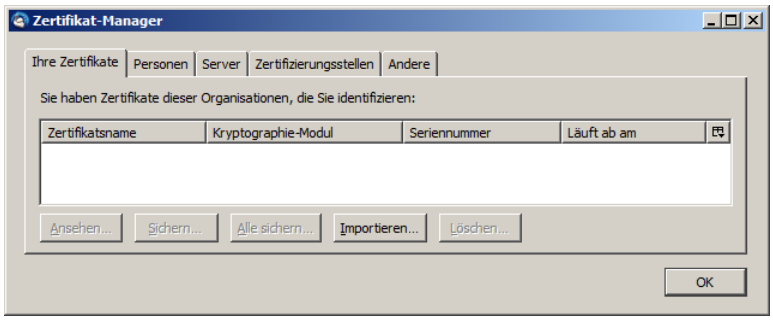
6.1.2. Eigenes Zertifikat importieren

Klicken Sie wieder in der rechten oberen Ecke von *Thunderbird* auf das *Icon* mit den drei waagerechten Linien, dann auf „Einstellungen“ und anschließend auf „Konten-Einstellungen“ oder direkt auf „Konto-Einstellungen bearbeiten“ im Abschnitt „Konten“ des Hauptfensters. Wählen Sie im neuen Fenster „S/MIME-Sicherheit“ aus.

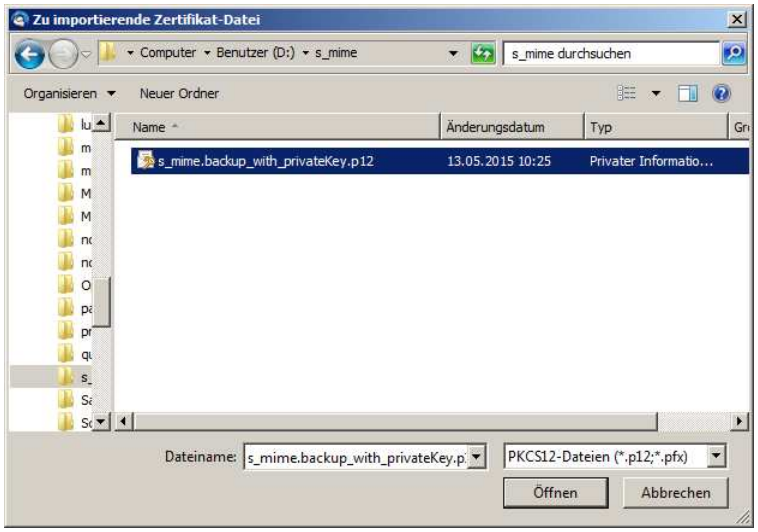




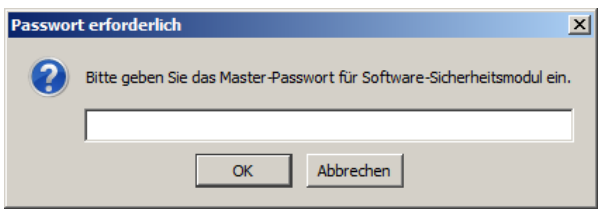
Klicken Sie auf „Zertifikate verwalten…“, um den Zertifikat-Manager zu öffnen.



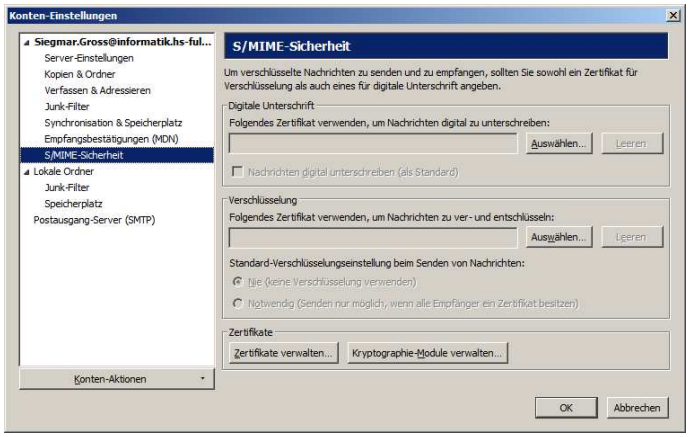
Wählen Sie den Reiter „Ihre Zertifikate“ aus und klicken Sie dann auf „Importieren…“.



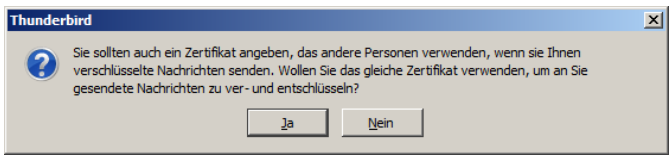
Wählen Sie Ihre Zertifikatsdatei aus. Sie müssen jetzt das „Master-Passwort“ und das Passwort Ihrer Zertifikatsdatei eingeben.



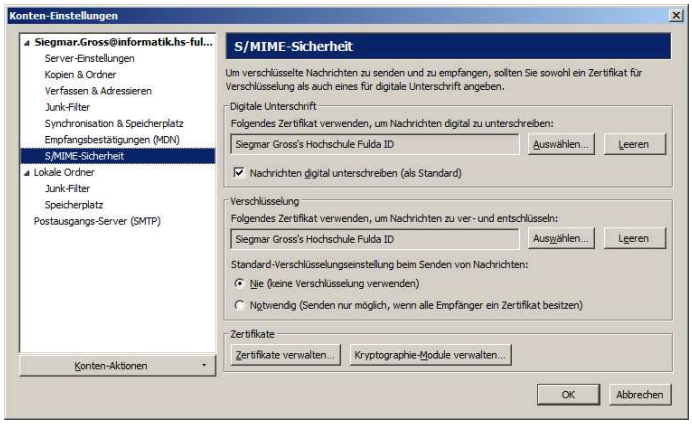
Benutzen Sie noch einmal das folgende Fenster und wählen Sie ein Zertifikat für Ihre digitale Unterschrift aus. Falls Sie nur ein Zertifikat besitzen, wird das gerade importierte Zertifikat angezeigt, wenn Sie auf „Auswählen…“ klicken.



Sie werden danach sofort gefragt, ob Sie dasselbe Zertifikat auch zur Verschlüsselung von Nachrichten benutzen wollen.



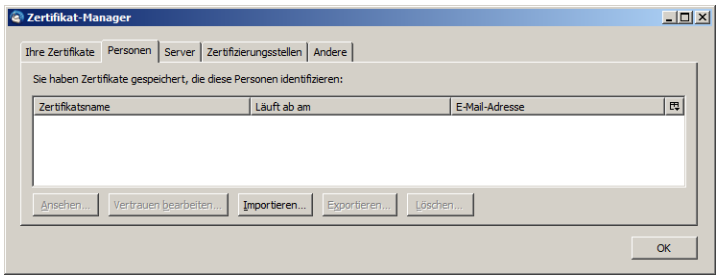
Anschließend sollte das Fenster Einträge für Ihre Zertifikate anzeigen.



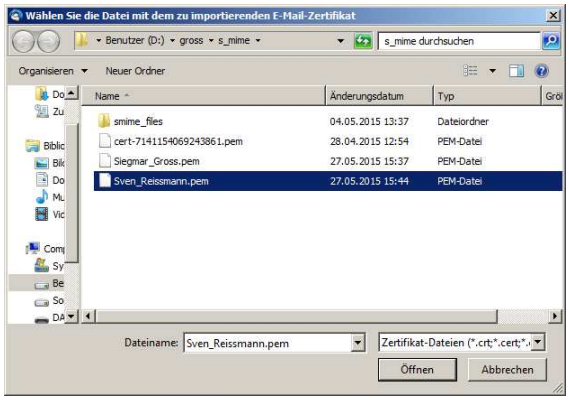
Sie können alle Nachrichten automatisch signieren und ggf. auch verschlüsseln, wenn Sie die entsprechenden Haken setzen. Anderenfalls müssen Sie diese Entscheidung für jede *E-Mail* individuell treffen.

6.1.3. Fremdes Zertifikat manuell importieren

Klicken Sie wie im Kapitel 6.1.2. in der rechten oberen Ecke von *Thunderbird* auf das *Icon* mit den drei waagerechten Linien, dann auf „Einstellungen“ und anschließend auf „Konten-Einstellungen“ oder wieder direkt auf „Konto-Einstellungen bearbeiten“ im Abschnitt „Konten“ des Hauptfensters. Wählen Sie im neuen Fenster „S/MIME-Sicherheit“ und dann wieder „Zertifikate verwalten…“ aus, um den Zertifikat-Manager zu öffnen.



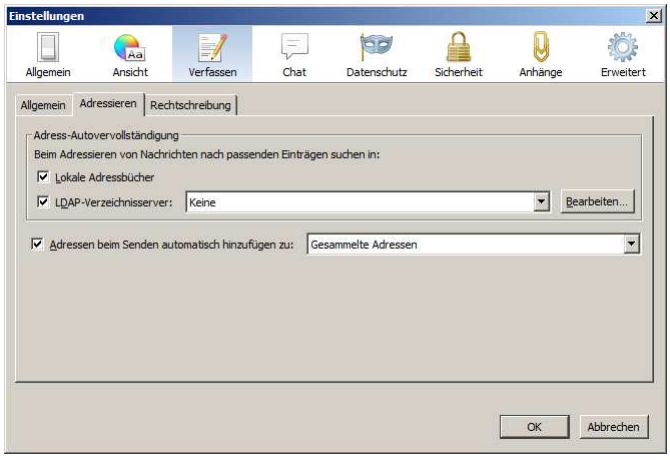
Wählen Sie den Reiter „Personen“ aus und klicken Sie dann auf „Importieren…“.



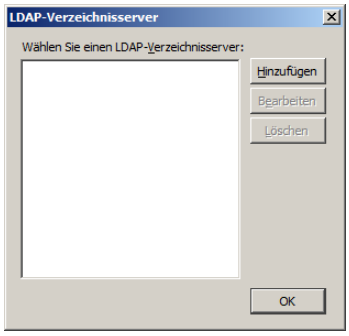
Wählen Sie die Zertifikatsdatei aus, die Sie manuell importieren wollen.

6.1.4. LDAP-Verzeichnis-*Server* einrichten

Klicken Sie wie im Kapitel 6.1.1. in der rechten oberen Ecke von *Thunderbird* auf das *Icon* mit den drei waagerechten Linien, dann auf „Einstellungen“ und anschließend noch einmal auf „Einstellungen“. Wählen Sie dort den Abschnitt „Verfassen“ und dann den Reiter „Adressieren“ aus.

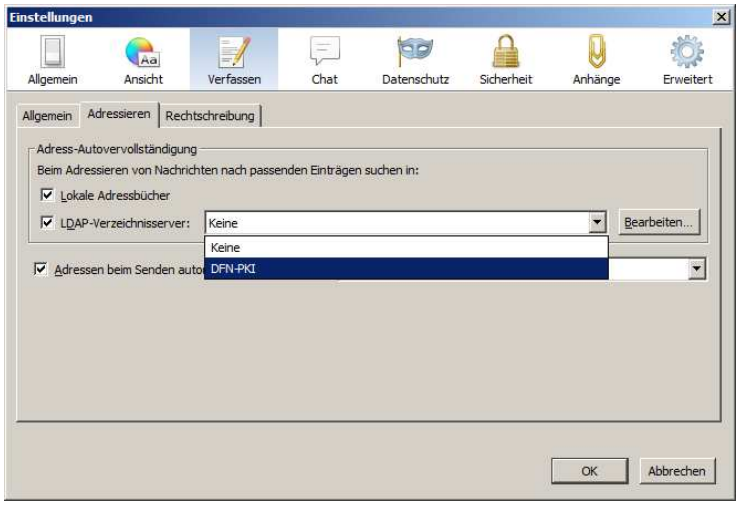


Setzen Sie einen Haken vor „LDAP-Verzeichnisserver:“ und klicken Sie dann auf „Bearbeiten…“.



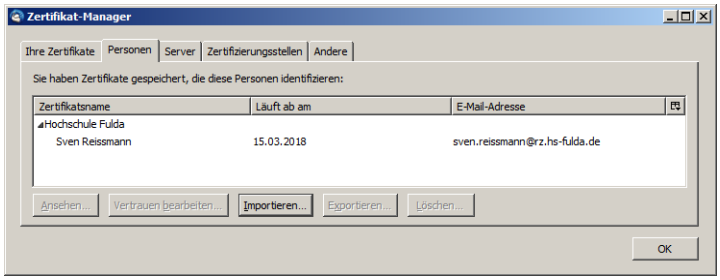
Klicken Sie auf „Hinzufügen“, tragen Sie im neuen Fenster die angegeben Werte ein und bestätigen Sie dann mit „OK“ und noch einmal mit „OK“.

Wählen Sie jetzt aus der Auswahlliste für „LDAP-Verzeichnisserver“ den Eintrag „DFN-PKI“ aus und bestätigen Sie mit „OK“.



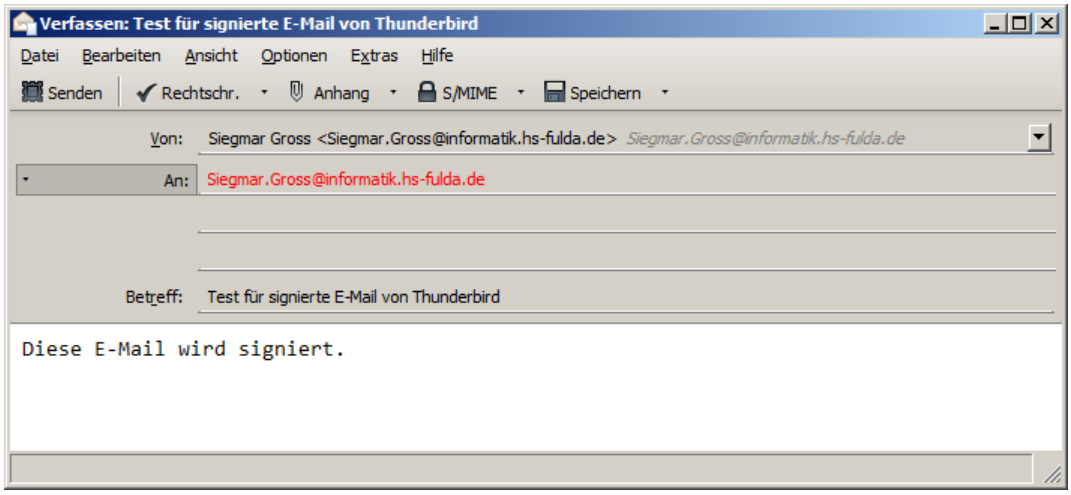
6.1.5. Zertifikate anzeigen

Klicken Sie wie im Kapitel 6.1.2. in der rechten oberen Ecke von *Thunderbird* auf das *Icon* mit den drei waagerechten Linien, dann auf „Einstellungen“ und anschließend auf „Konten-Einstellungen“ oder wieder direkt auf „Konto-Einstellungen bearbeiten“ im Abschnitt „Konten“ des Hauptfensters. Wählen Sie im neuen Fenster „S/MIME-Sicherheit“ und dann wieder „Zertifikate verwalten…“ aus, um den Zertifikat-Manager zu öffnen. Über den Reiter „Personen“ können Sie später sehen, welche öffentlichen Zertifikate *Thunderbird* von Ihren *E-Mail*-Partnern eingesammelt hat bzw. welche Zertifikate Sie selbst manuell hinzugefügt haben.

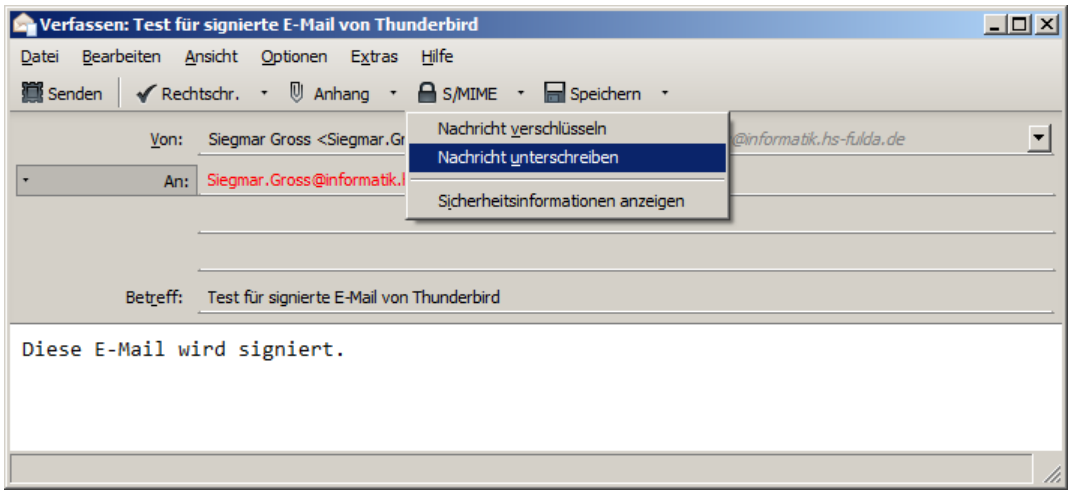


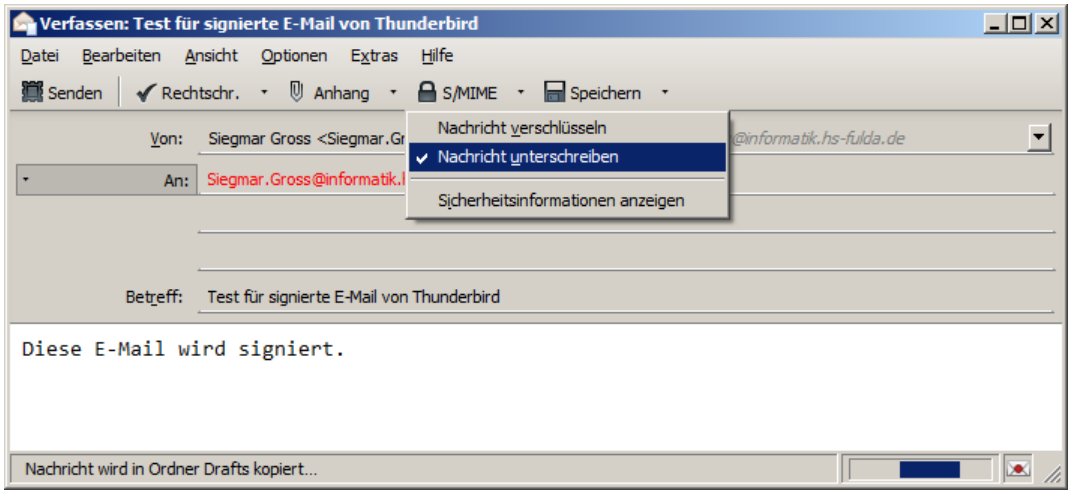
6.1.6. E-Mail signieren/verschlüsseln

Jetzt können Sie eine signierte und/oder verschlüsselte *E-Mail* verschicken.



Klicken Sie auf den Pfeil rechts neben S/MIME und wählen Sie „Nachricht unterschreiben“ aus, bevor Sie die Nachricht abschicken, falls Ihre Nachrichten nicht automatisch digital unterschrieben werden. Wenn Sie außerdem „Nachricht verschlüsseln“ auswählen, wird die Nachricht auch noch verschlüsselt.





Wenn Sie auf „Senden“ klicken, müssen Sie ggf. Ihr *Master*-Passwort eingeben, das den Zugriff auf Ihr Zertifikat schützt, bevor die Nachricht abgeschickt wird. Die Eingabe des *Master*-Passworts ist einmal pro Sitzung erforderlich.

Signierte und/oder verschlüsselte Nachrichten werden durch Symbole im Nachrichtenkopf gekennzeichnet. Klicken Sie auf die Symbole, wenn Sie ausführlichere Informationen haben wollen. Falls *Thunderbird* eine verschlüsselte Nachricht nicht entschlüsseln kann, wird anstelle der Nachricht eine entsprechende Meldung angezeigt.

Es werden die folgenden Symbole verwendet.

PC	Mac	Bedeutung
		Signierte Nachricht (der rote Punkt symbolisiert Siegellack)
		Signierte Nachricht mit unsicherer Signatur, z. B. wenn die *E-Mail*-Adresse des Senders nicht der *E-Mail*-Adresse des Zertifikats entspricht
		Signierte Nachricht mit ungültiger Signatur, da die Nachricht z. B. modifiziert wurde oder das Zertifikat von einer nicht-vertrauenswürdigen Zertifizierungsstelle (z. B. eigenes Zertifikat) herausgegeben wurde
		Verschlüsselte Nachricht
		Verschlüsselte Nachricht mit ungültiger Verschlüsselung

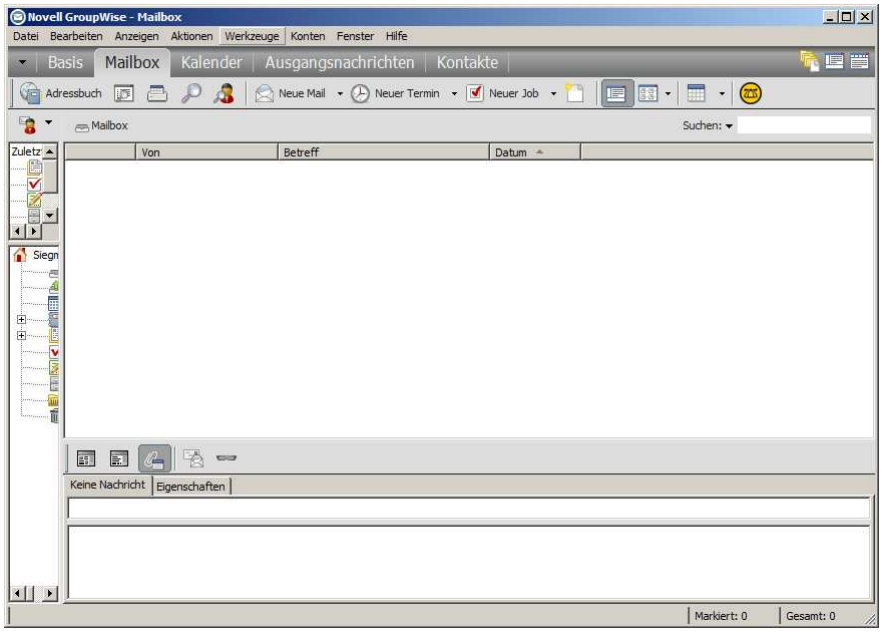
6.2. Novell GroupWise-Windows Client

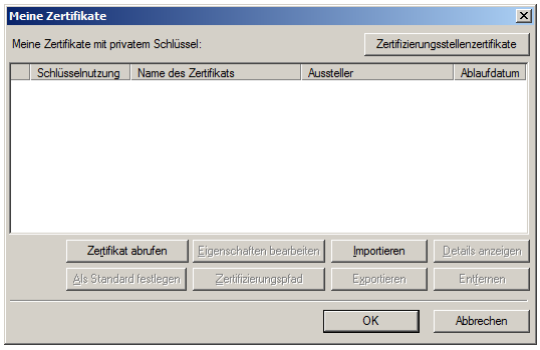
Auf den folgenden Web-Seiten finden Sie Informationen zu „Novell GroupWise“.

https://www.novell.com/documentation/groupwise2014/
https://www.novell.com/documentation/groupwise2014/pdfdoc/gw2014_guide_userwin/gw2014_guide_userwin.pdf

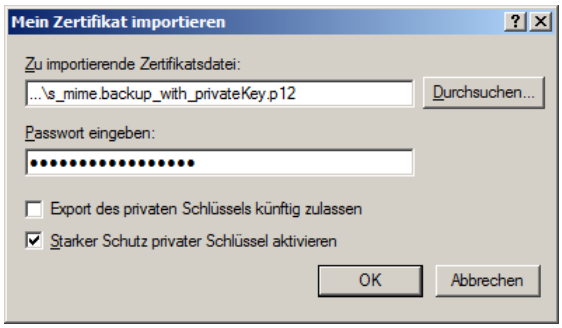
6.2.1. Eigenes Zertifikat importieren

Starten Sie den *Novell GroupWise-Windows Client* und wählen Sie unter „Werkzeuge“ den Eintrag „Optionen…“ aus. Danach müssen Sie einen Doppelklick auf „Zertifikate“ ausführen. Die folgenden Abbildungen wurden mit *GroupWise Client 12.0.3* erstellt.





Klicken Sie auf „Importieren“, wählen Sie Ihre Zertifikatsdatei aus, geben Sie das Passwort für die Zertifikatsdatei ein, entfernen Sie den Haken vor „Export des privaten Schlüssels künftig zulassen“ und setzen Sie einen Haken vor „Starker Schutz privater Schlüssel aktivieren“.



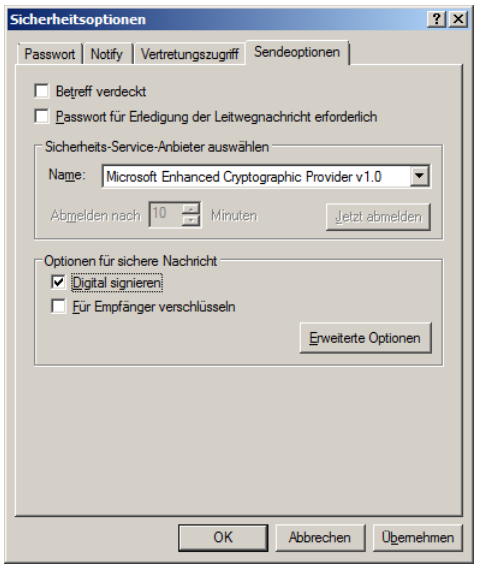
Klicken Sie auf „Sicherheitsstufe…“ und wählen Sie die hohe Sicherheitsstufe.

Jetzt müssen Sie ein Passwort zum Schutz des privaten Schlüssels eingeben. Wählen Sie ein gutes Passwort, das den Richtlinien der Hochschule Fulda entspricht, die Sie auf der Web-Seite https://www.hs-fulda.de/it-sicherheit finden (dort „Passwörter“ auswählen und Abschnitt 2 lesen).

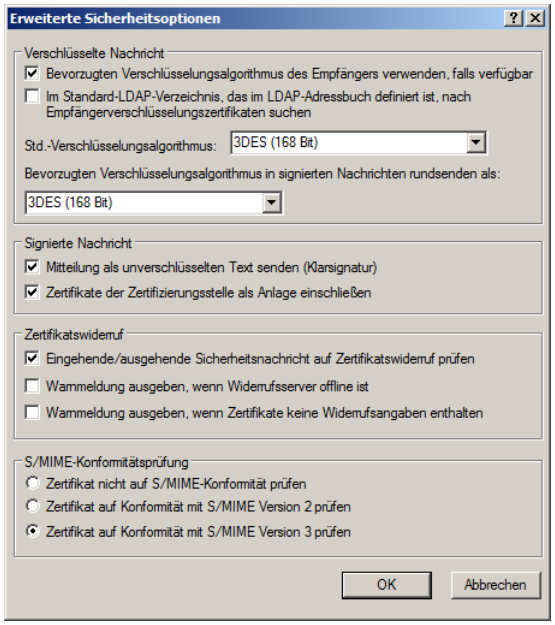
Im Kapitel 1 wurde bereits erwähnt, dass GroupWise zurzeit ein Problem mit der offiziellen und der internen *E-Mail*-Adresse hat, das spätestens mit der Übernahme aller *E-Mail*-Dienste von der Universität Gießen nach Fulda gelöst sein sollte. Wenn das **Zertifikat mit der offiziellen *E-Mail*-Adresse „Vorname.Nachname@...hs-fulda.de“** erstellt worden ist, erscheint das folgende Fenster **ohne Warnung oder Fehlermeldung und die Sicherheitsstufe wird automatisch wieder auf „mittlere Sicherheitsstufe“ zurückgesetzt**. Das Zertifikat wird mit der hohen Sicherheitsstufe importiert, wenn es mit der internen *E-Mail*-Adresse „fd-Nummer@fhfddvz1...“ erstellt worden ist.

Wenn die hohe Sicherheitsstufe akzeptiert worden ist, erscheint sofort das folgende Fenster.

Wenn die hohe Sicherheitsstufe akzeptiert worden ist, können Nachrichten automatisch signiert werden. Außerdem sollten Sie dann einen besseren Verschlüsselungsalgorithmus einstellen, da der Standardschlüssel mit 40 Bit sehr unsicher ist. Wählen Sie unter „Werkzeuge“ den Eintrag „Optionen…“ aus. Danach müssen Sie einen Doppelklick auf „Sicherheit“ ausführen, den Reiter „Sendeoptionen“ wählen und dort einen Haken vor „Digital signieren“ setzen.



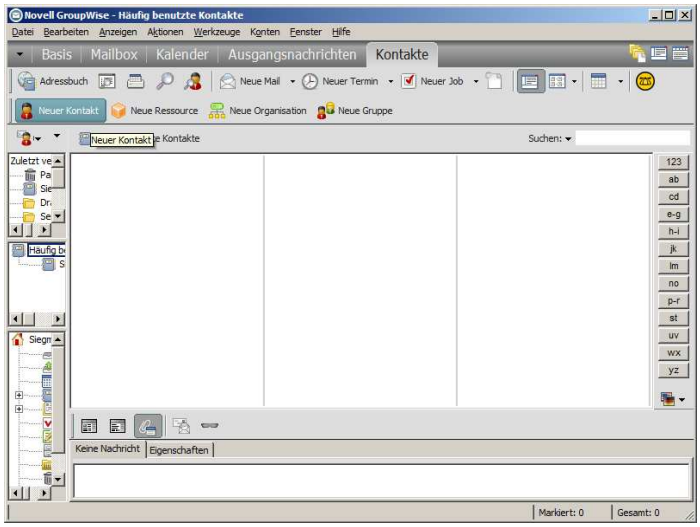
Klicken Sie dann auf „Erweiterte Optionen“ und ändern Sie die beiden Einträge für die Verschlüsselungsalgorithmen von „RC2 (40 Bit) auf „3DES (168 Bit)“, um eine sicherere Verschlüsselung zu erhalten.

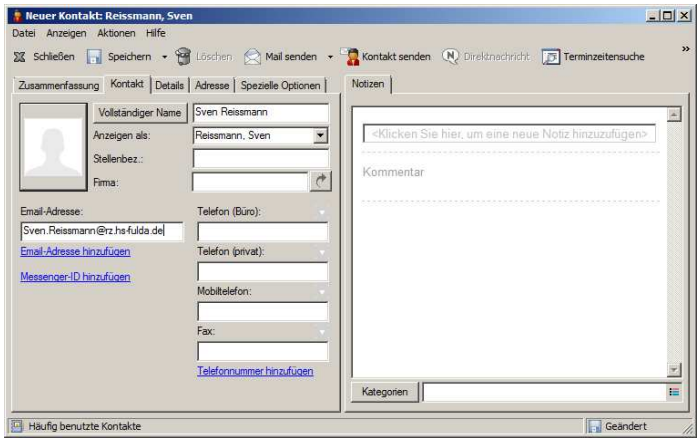


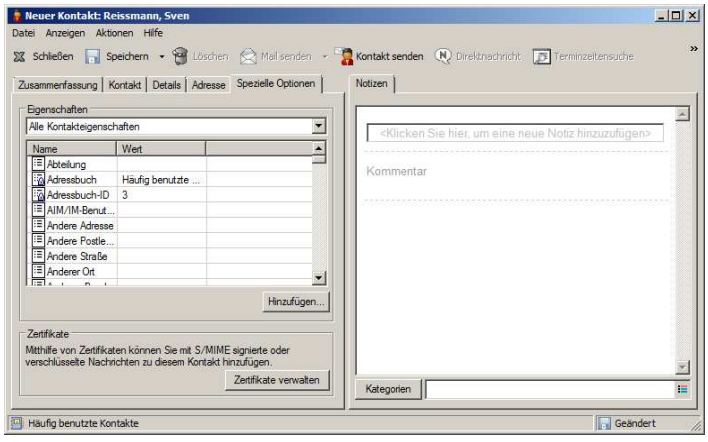
6.2.2. Fremdes Zertifikat manuell importieren

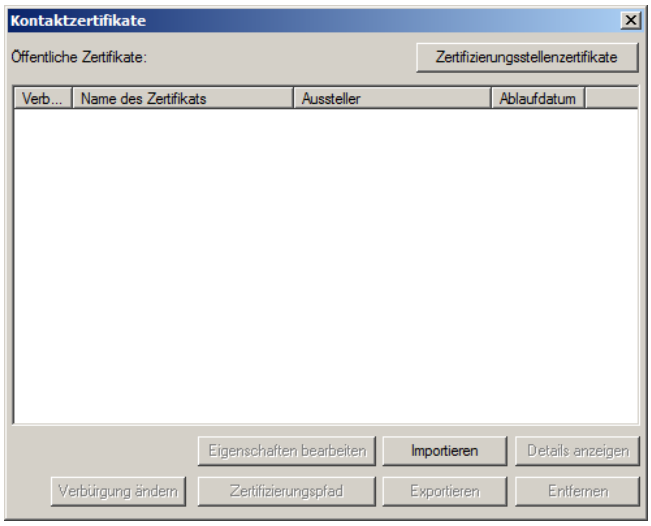
Wenn man ein Zertifikat manuell importiert, scheint es automatisch ein unsicheres Zertifikat zu werden, da man bestätigen soll, dass man für die Sicherheit des Zertifikats bürgt und als Ansprechpartner dient, obwohl es sich um ein offizielles Zertifikat einer Zertifizierungsstelle handelt, d. h., dass man in *GroupWise* keine offiziellen Zertifikate manuell importieren kann.

Man kann zum Beispiel das Zertifikat von Herrn Reißmann von der Zertifizierungsstelle herunterladen und als neuen Kontakt hinzufügen. In *GroupWise* auf den Reiter „Kontakte“ und dann auf „Neuer Kontakt“ klicken. Es wird ein Fenster geöffnet, in dem der Name des Eigentümers des Zertifikats eingetragen wird. Anschließend auf „Spezielle Optionen“ und danach auf „Zertifikate verwalten“ klicken.

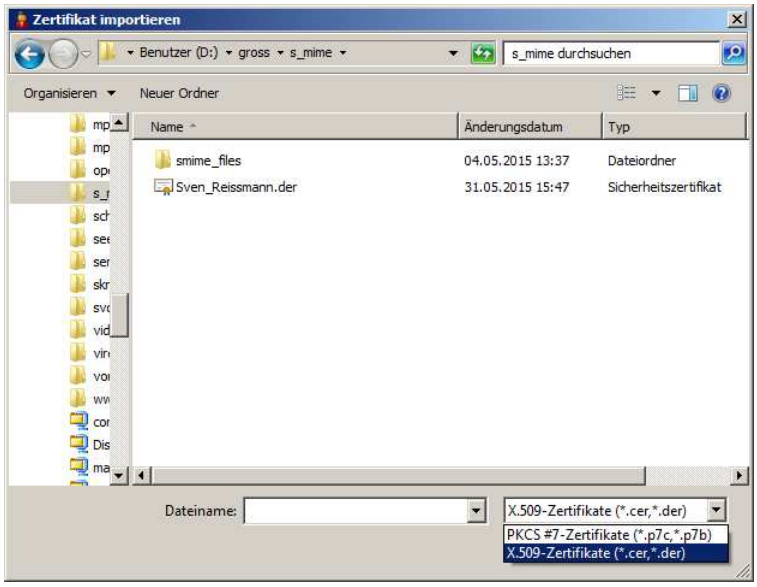


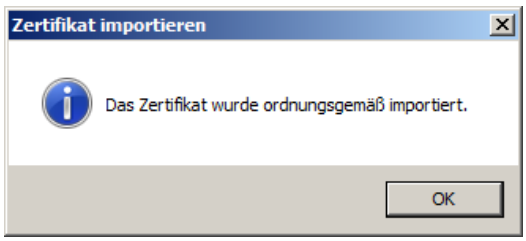


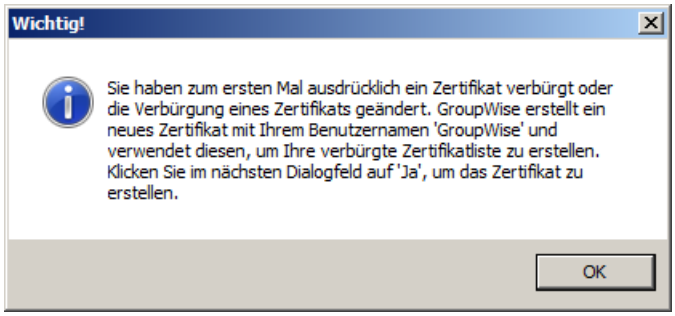


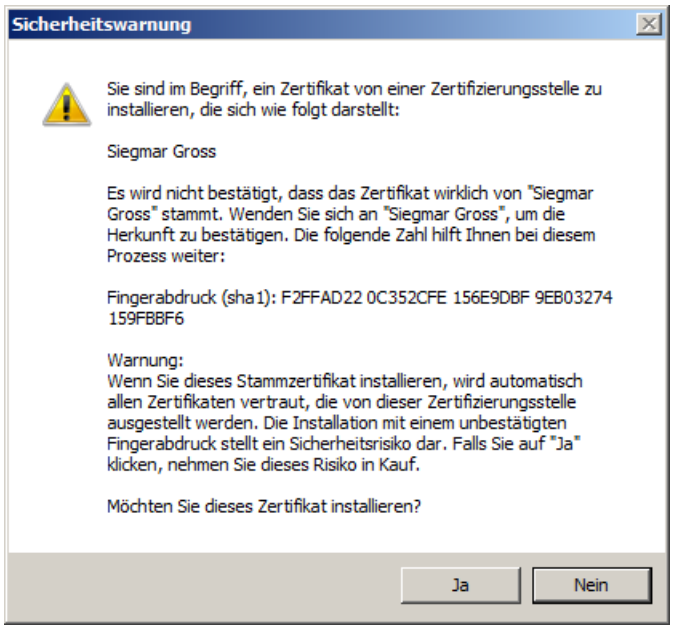


Auf „Importieren“ klicken, den Dateityp „X.509-Zertifikate (*.cer,*der)“ auswählen und die Zertifikatsdatei mit einem Doppelklick importieren.

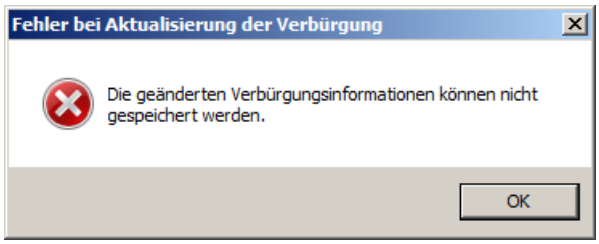






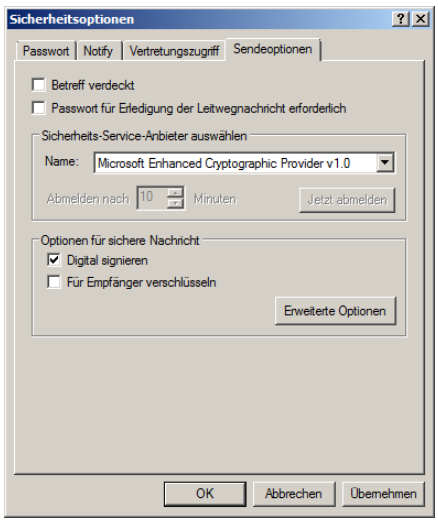


Der Vorgang wurde mit „Nein“ beendet.

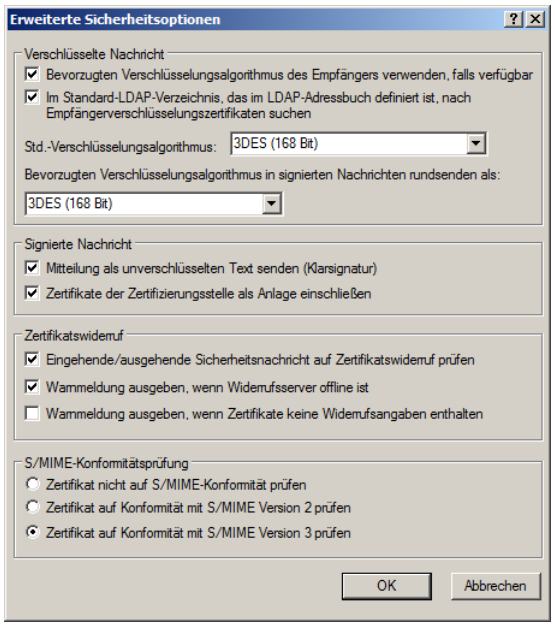


6.2.3. LDAP-Verzeichnis-*Server* einrichten

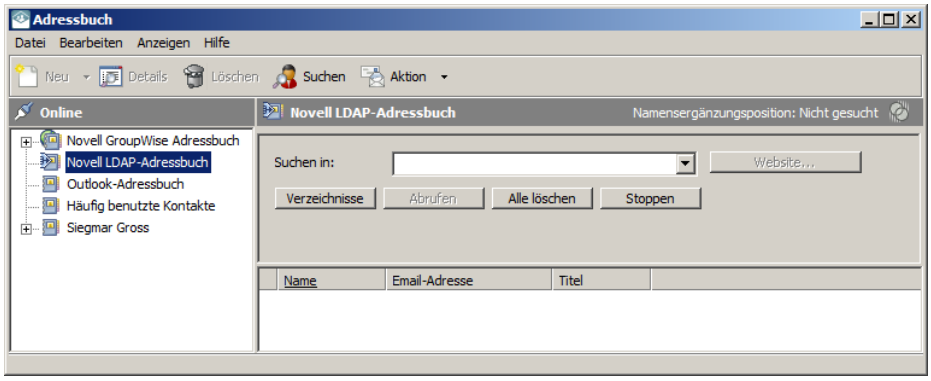
Wählen Sie unter „Werkzeuge“ den Eintrag „Optionen…“ aus. Danach müssen Sie einen Doppelklick auf „Sicherheit“ ausführen und im neuen Fenster den Reiter „Sendeoptionen“ wählen.



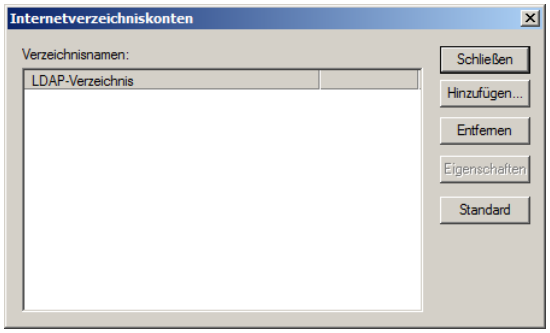
Klicken Sie auf „Erweiterte Optionen“ und setzen Sie im neuen Fenster einen Haken vor „Im Standard-LDAP-Verzeichnis, das im LDAP-Adressbuch definiert ist, nach Empfängerzertifikaten suchen“.

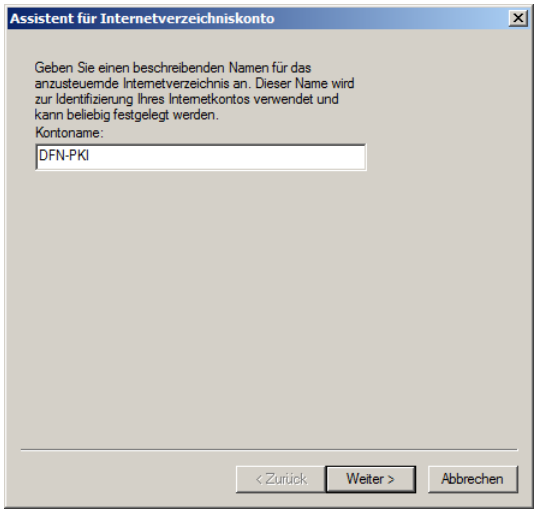


Wählen Sie unter „Werkzeuge“ den Eintrag „Adressbuch“ und im neuen Fenster auf der linken Seite den Eintrag „Novell LDAP-Adressbuch“ aus.

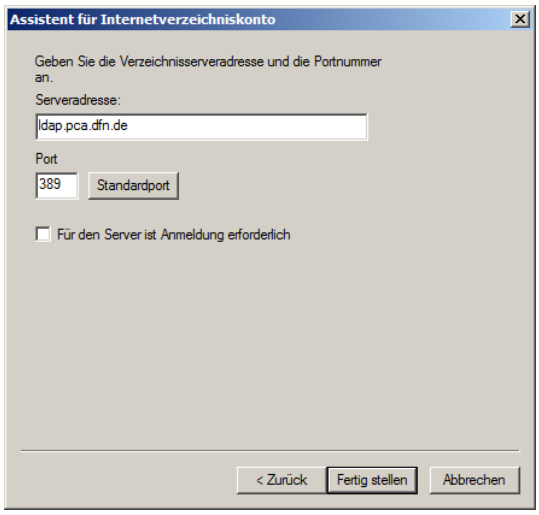


Klicken Sie auf „Verzeichnisse“ und dann auf „Hinzufügen…“.

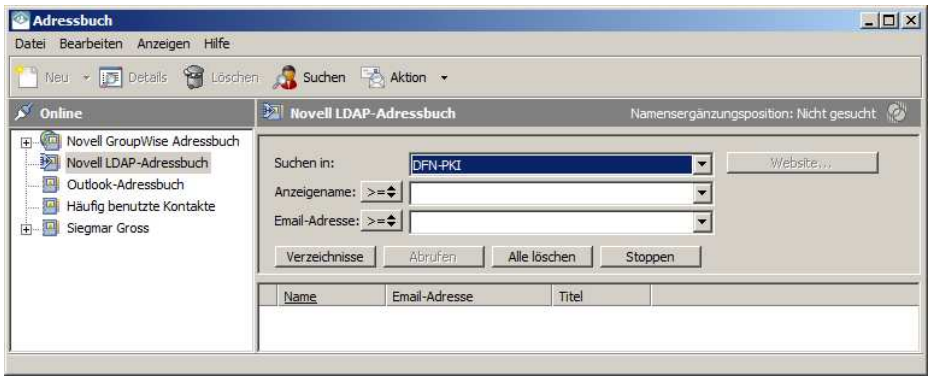




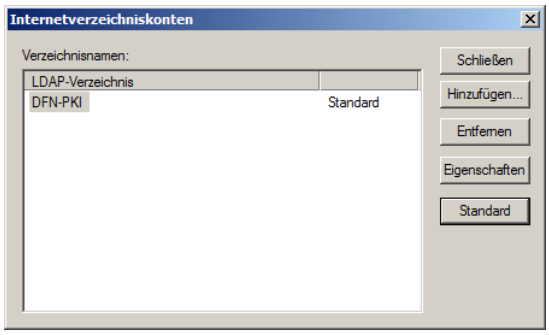
Tragen Sie den Namen „DFN-PKI“ ein und klicken Sie auf weiter. Geben Sie die Adresse „ldap.pca.dfn.de“ des *Servers* ein, klicken Sie auf „Fertig stellen“ und schließen Sie das nachfolgende Fenster.



Markieren Sie den neuen Verzeichnisdienst und klicken Sie dann erneut auf „Verzeichnisse“.

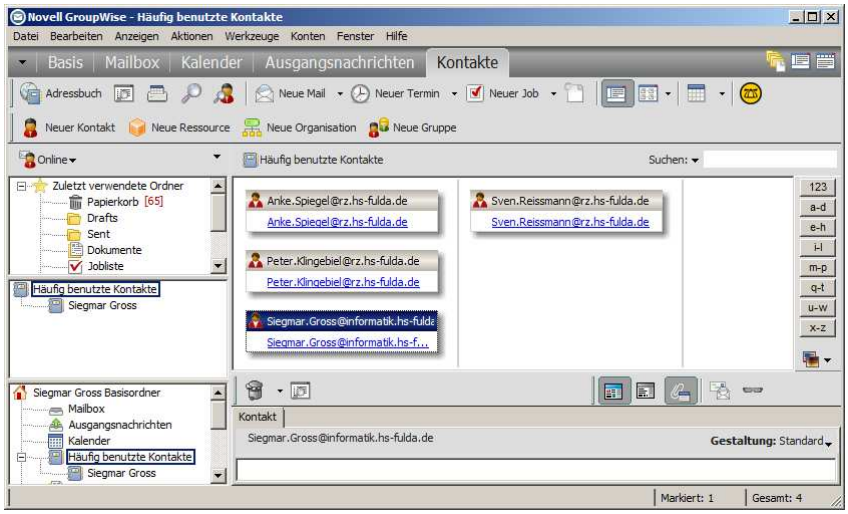


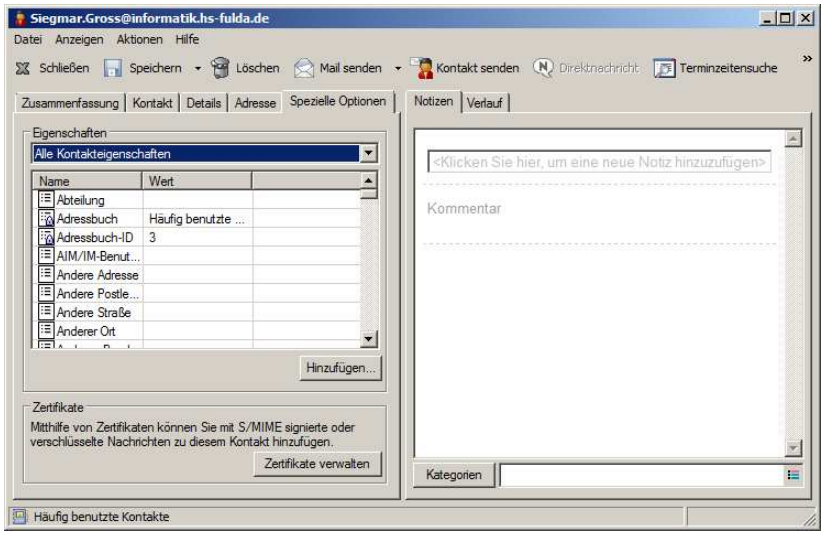
Klicken Sie auf „Standard“, damit der neue Verzeichnisdienst zur Suche nach Sicherheitszertifikaten benutzt wird und schließen Sie danach das Fenster und das Adressbuchfenster.



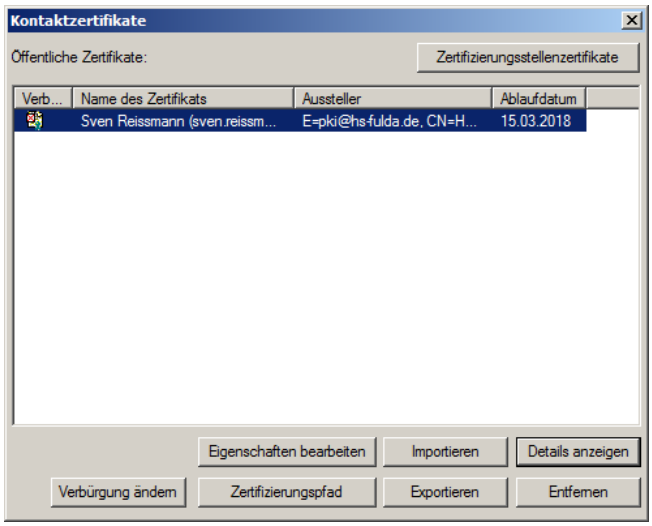
6.2.4. Zertifikate anzeigen

Wählen Sie den Reiter „Kontakte“ aus, klicken Sie doppelt auf einen Kontakteintrag und wählen Sie im neuen Fenster den Reiter „Spezielle Optionen“ aus.

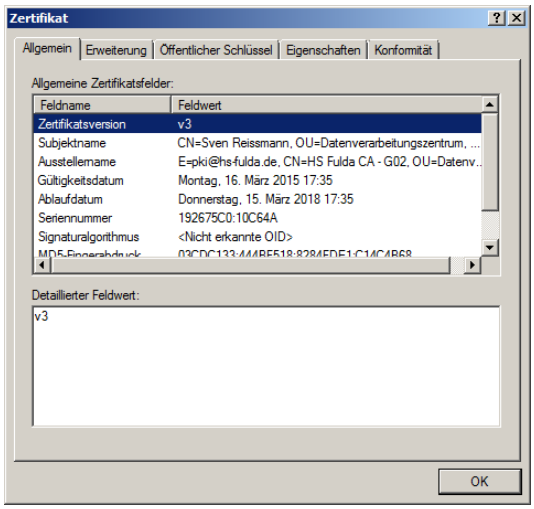




Klicken Sie jetzt auf „Zertifikate verwalten“. Sie erhalten dann zum Beispiel das folgende Fenster.

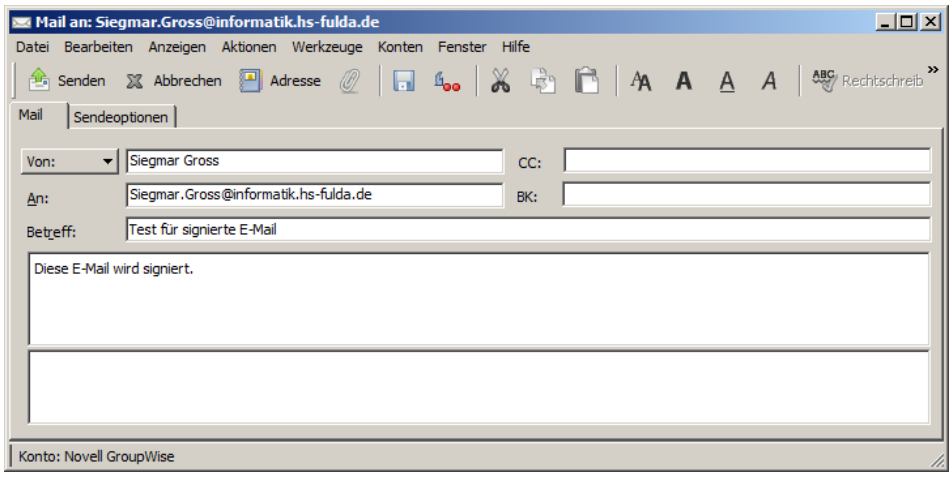


Klicken Sie auf „Details anzeigen“. Sie können sich verschiedene Informationen zum Zertifikat ansehen.

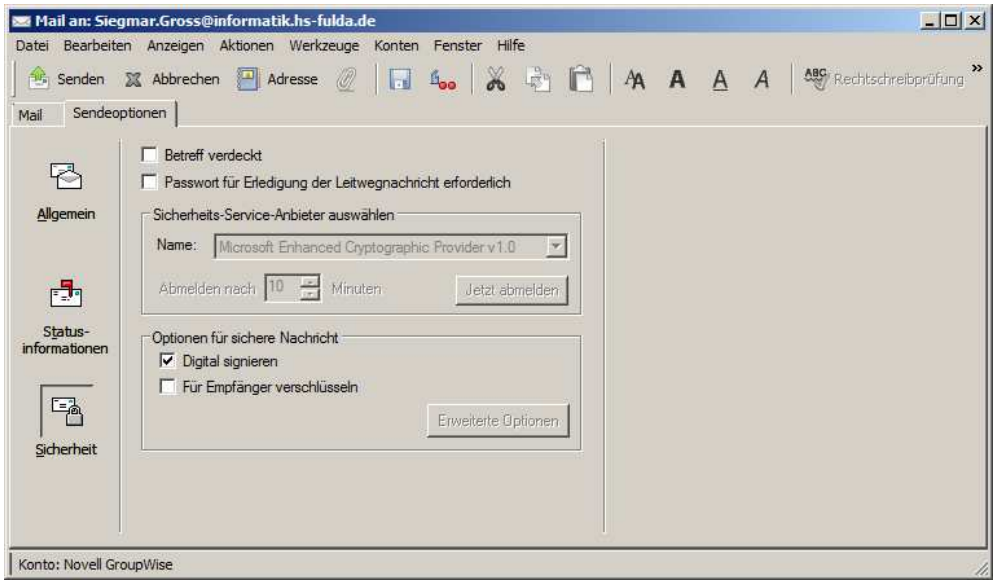


6.2.5. E-Mail signieren/verschlüsseln

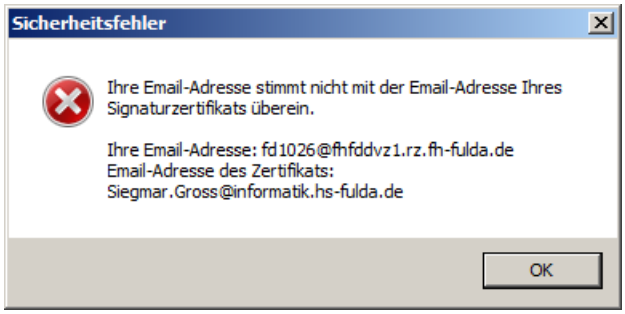
Jetzt können Sie eine signierte und/oder verschlüsselte *E-Mail* verschicken.



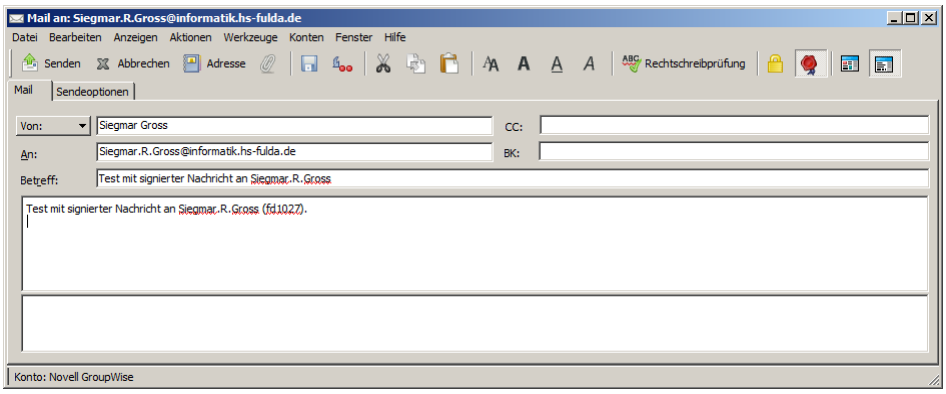
Wählen Sie jetzt „Sendeoptionen“ und dann „Sicherheit“ aus und setzen Sie einen Haken vor „Digital signieren“, bevor Sie die Nachricht abschicken. Wenn Sie einen Haken vor „Für Empfänger verschlüsseln“ setzen, wird die Nachricht verschlüsselt.

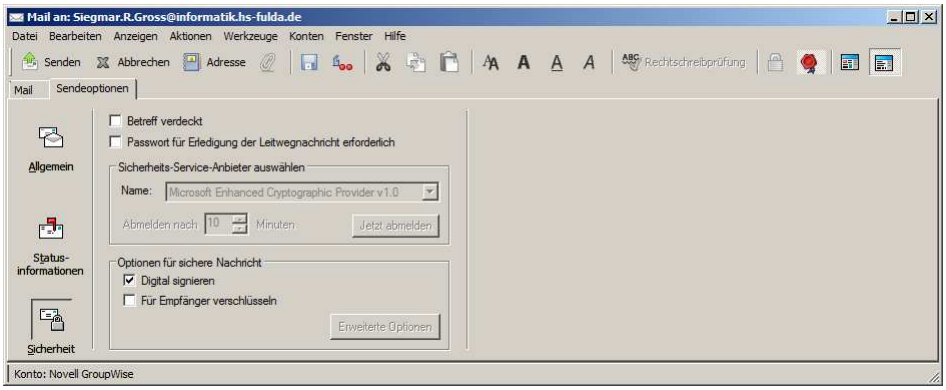


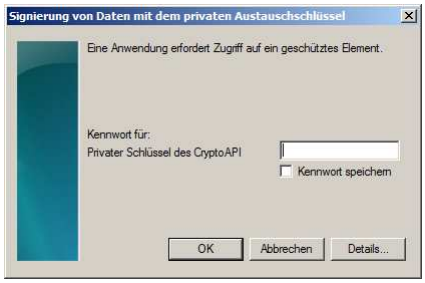
Leider funktioniert es nicht mit einem Zertifikat mit der offiziellen *E-Mail*-Adresse, da *GroupWise* die interne *E-Mail*-Adresse zur Weiterleitung der Nachricht an den X.500-Dienst der Universität Gießen benutzt, sodass die beiden Adressen nicht übereinstimmen.

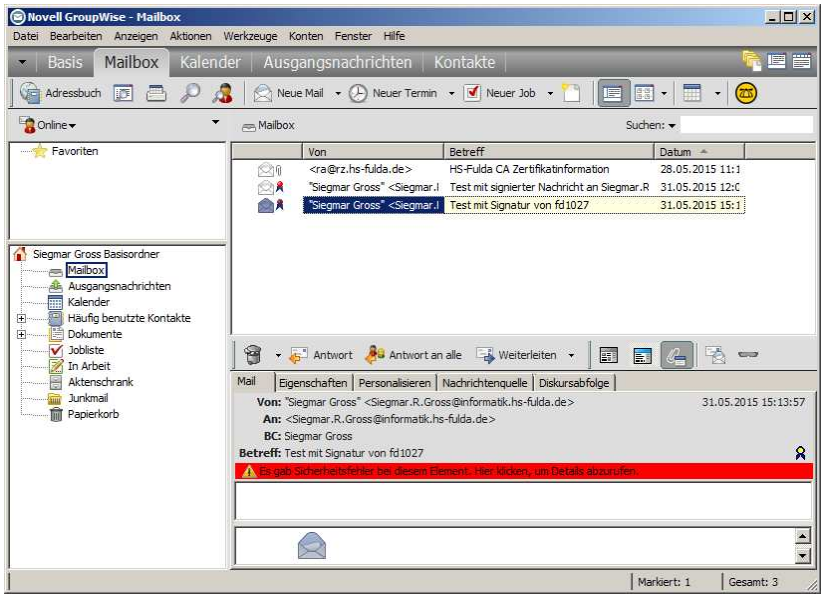


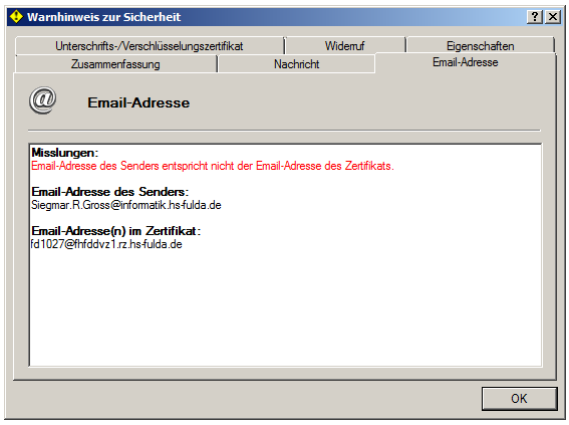
Neuer Versuch mit einem Zertifikat mit einer internen *E-Mail*-Adresse. Jetzt kann die Nachricht signiert und verschlüsselt aber anschließend nicht gelesen werden, da die empfangene Nachricht die offizielle *E-Mail*-Adresse und das Zertifikat die interne Adresse benutzt.











***GroupWise* kann zurzeit für signierte/verschlüsselte Nachrichten auf keinen Fall benutzt werden!**

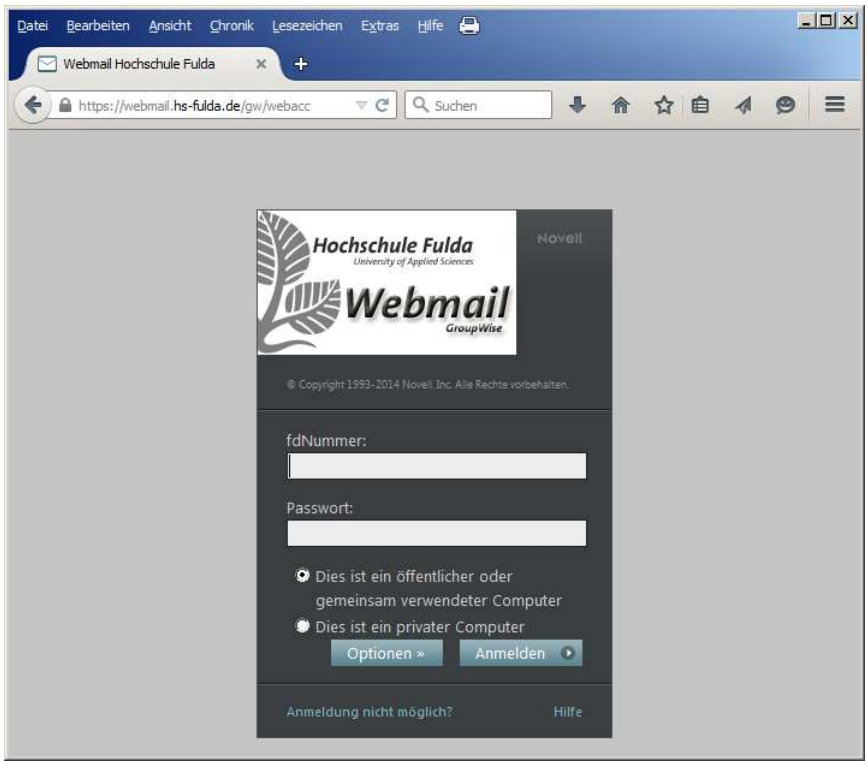
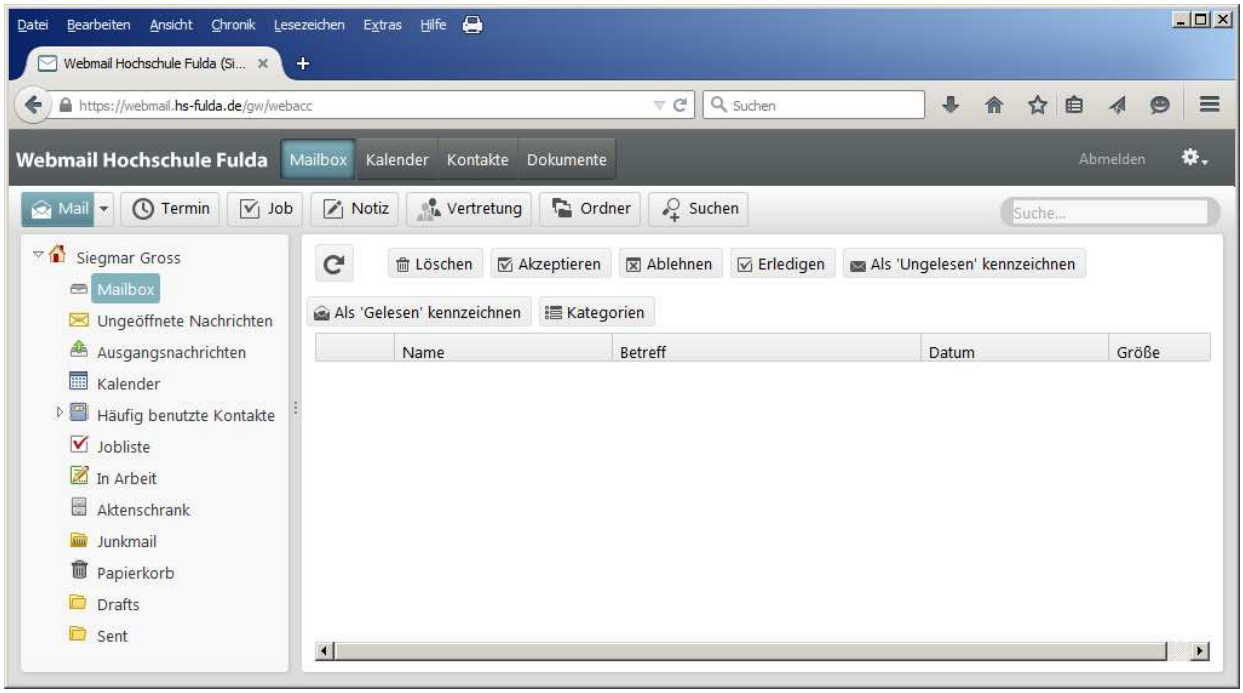
Signierte und/oder verschlüsselte Nachrichten werden durch Symbole im Nachrichtenkopf gekennzeichnet. Klicken Sie auf die Symbole, wenn Sie ausführlichere Informationen haben wollen.

Es werden die folgenden Symbole verwendet.

PC	Bedeutung
	Signierte Nachricht
	Verschlüsselte Nachricht
	Signierte und verschlüsselte Nachricht
	Nachrichten mit unsicherer oder ungültiger Signatur enthalten eine Warnung im Nachrichtenkopf, z. B.

6.3. Novell GroupWise WebAccess Client

Auf den folgenden Web-Seiten finden Sie Informationen zu „Novell GroupWise WebAccess“.

https://www.novell.com/documentation/groupwise2014/
https://www.novell.com/documentation/groupwise2014/pdfdoc/gw2014_guide_userweb/gw2014_guide_userweb.pdf

Sie können nur „normale“ Nachrichten senden und lesen. Signieren und/oder verschlüsseln von Nachrichten bzw. lesen von verschlüsselten Nachrichten ist nicht möglich. Melden Sie sich bei *GroupWise* über Ihren *Browser* mit der Adresse https://webmail.hs-fulda.de an.