Signieren mit dem Thunderbird

Ihr E-Mailclient muss mit der gleichen Absenderadresse eingerichtet sein, wie sie im Zertifikat enthalten ist.

Für die Installation der Wurzel- und CA-Zertifikate gehen Sie wie folgt vor:

1. Alle Wurzel und CA-Zertifikate finden Sie hier:
2. Klicken Sie mit der rechten Maustaste auf die Links zu den Zertifikaten und wählen "Ziel speichern unter ...". Wählen Sie den Speicherort und vergeben Sie einen Namen.
3. Navigieren Sie danach in Thunderbird über:
   Extras - Konten - S/MIME-Sicherheit - Zertifikate - Zertifizierungsstellen - Importieren
   Wählen Sie die Datei mit dem zu importierenden Zertifikat aus und klicken Sie auf Öffnen.

Beim Importieren der Zertifikate, müssen Sie bei der folgenden Abfrage, der Zertifizierungsstelle (CA) mindestens in den Optionen Webseiten und E-Mail zu identifizieren, vertrauen. Setzen Sie die entsprechenden Hacken.

Abbildung: Abfrage CA Vertrauen

Verfahren Sie so mit allen Wurzel- und CA-Zertifikaten.

Installieren kryptographische Komponente PKCS#11 (cvP11.dll)

Eine Installationsanleitung für den Cryptovision CSP finden Sie hier:

Standardmäßig befindet sich diese DLL danach im Verzeichnis system32 in Ihrer Microsoft Windows-Installation (üblicherweise C:\WINNT\system32 auf Windows NT- und Windows 2000-Plattformen; C:\WINDOWS\system32 auf Windows XP- und Windows 2003-Plattformen).

Navigieren Sie im Browser und Mailclient über:
Extras - Einstellungen - Datenschutz - Sicherheit - Kryptographie-Module - laden.
Vergeben Sie einen Modulnamen (z.B. FHCard) und wählen mit Durchsuchen unter:
C:\WINDOWS\system32\cvP11.dll

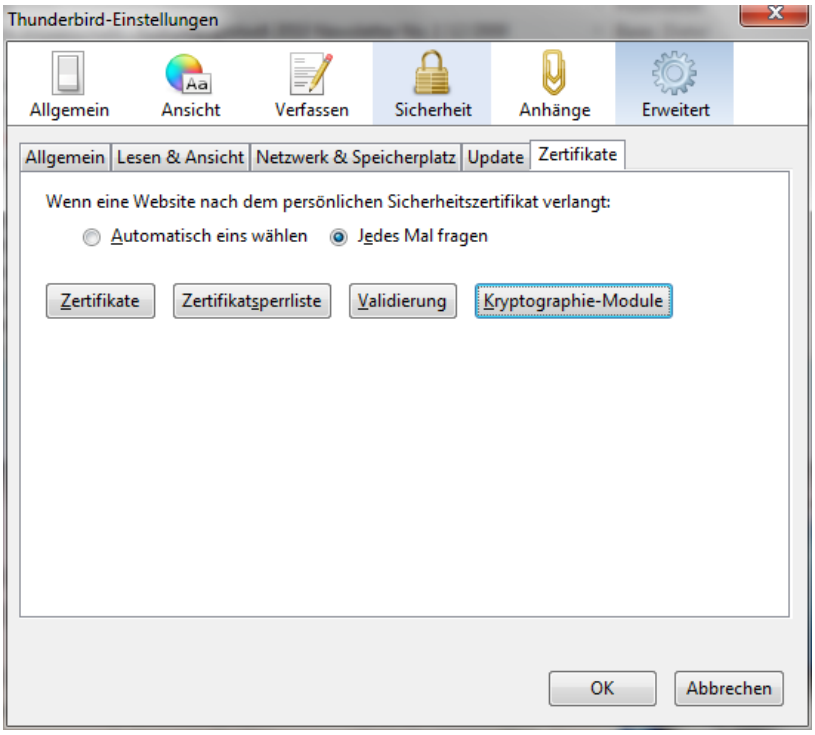

Abbildung: Installation Sicherheitsmodul 1

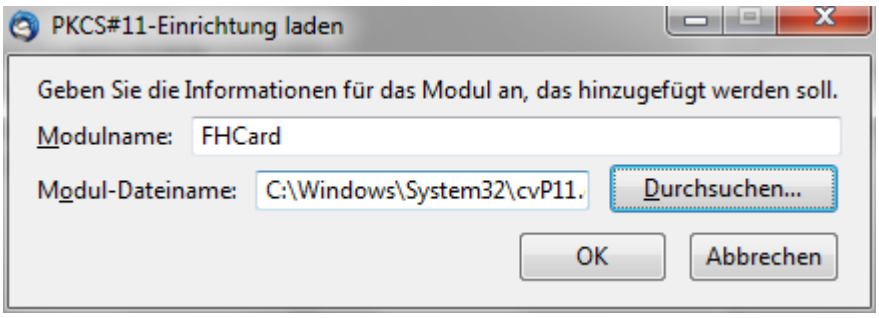

Abbildung: Installation Sicherheitsmodul 2

Dies fügt das entsprechende Sicherheitsmodul nach Ihrer Bestätigung Ihrem Browser/Mailclient automatisch hinzu.

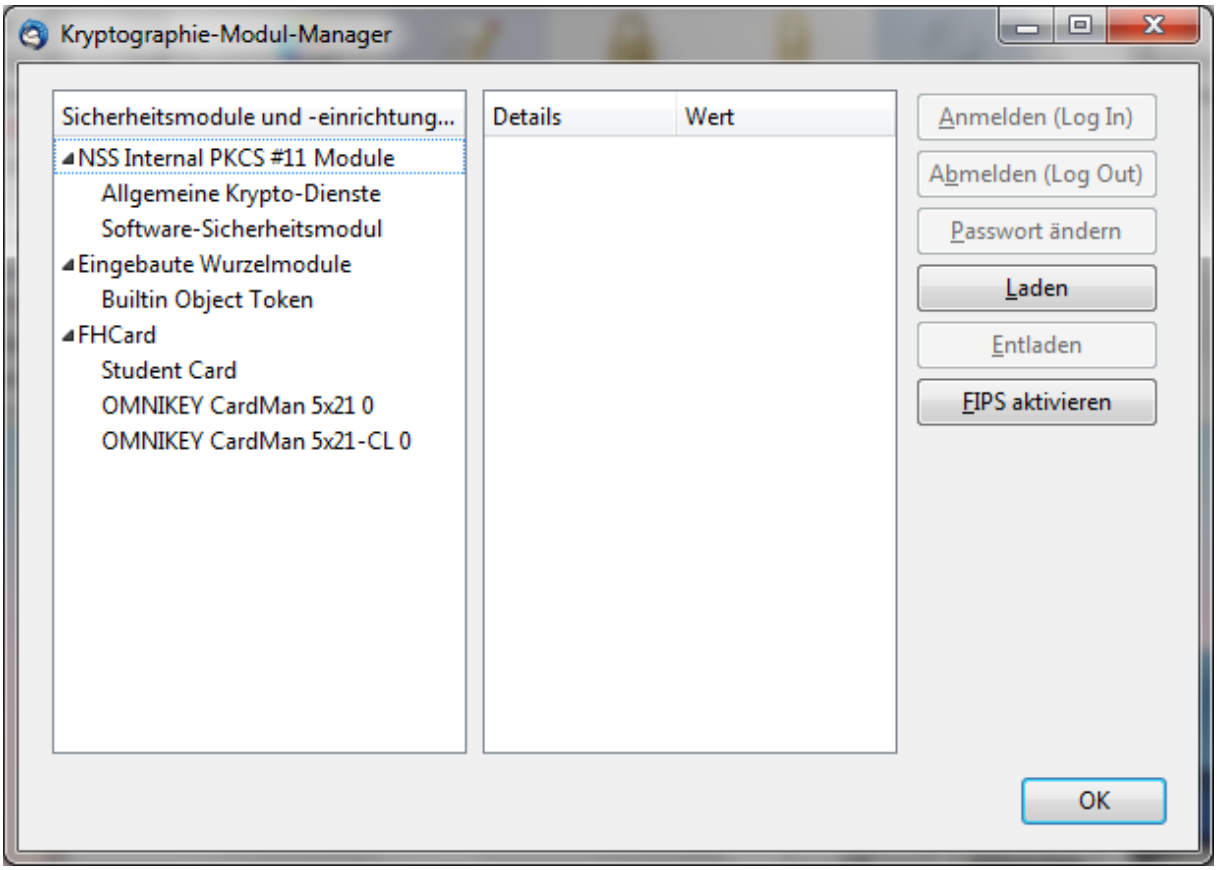

Abbildung: Neues Sicherheitsmodul

Integration des Zertifikat in den Thunderbid Mailclient

Für die Nutzung von Signatur- und Verschlüsselungsfunktionen müssen Sie einige wenige Konfigurationen an Ihren lokalen Konteneinstellungen vornehmen, u.a. muss wie oben beschrieben das kryptographische Modul geladen sein.

Klicken Sie auf **Extras - Konten - S/MIME-Sicherheit**

Auf der rechten Auswahlseite können Sie jetzt Ihr Zertifikat wählen. Bei Zertifikaten auf Smartcard muss sich die Karte im Reader befinden. Eventuell werden Sie zur Eingabe Ihrer PIN aufgefordert.

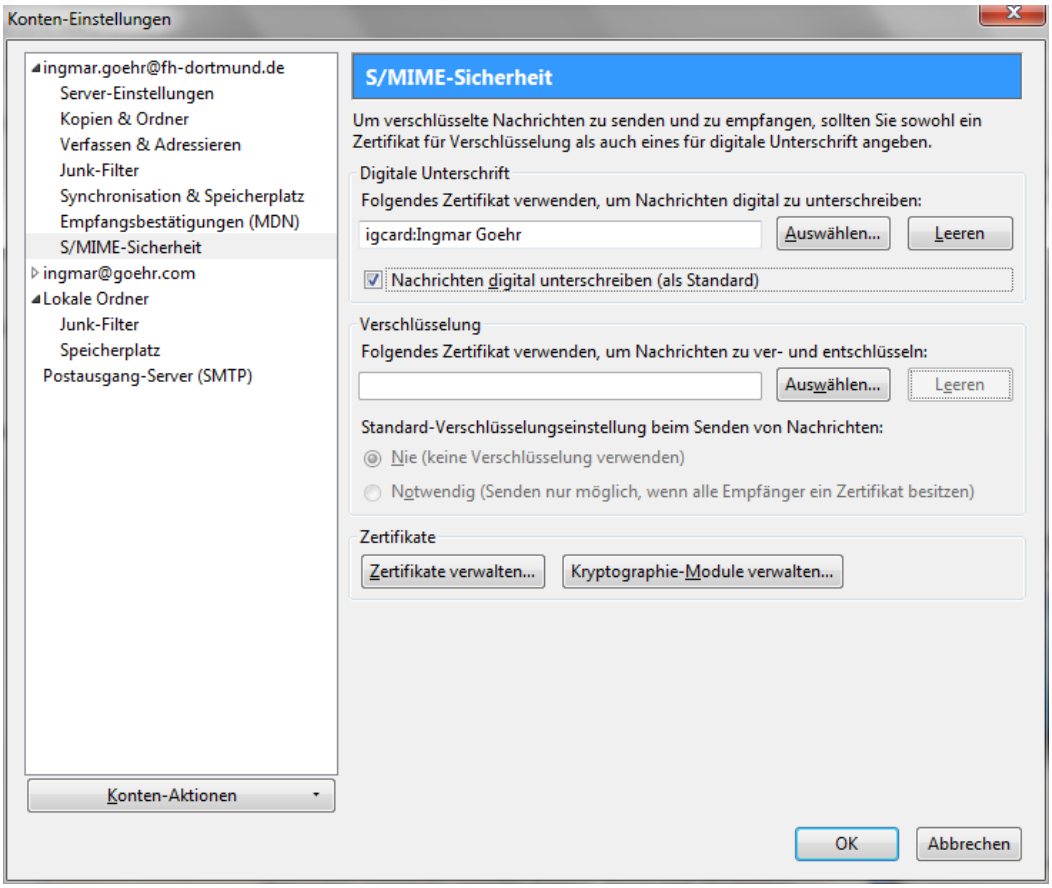

Abbildung: Sicherheitseinstellungen

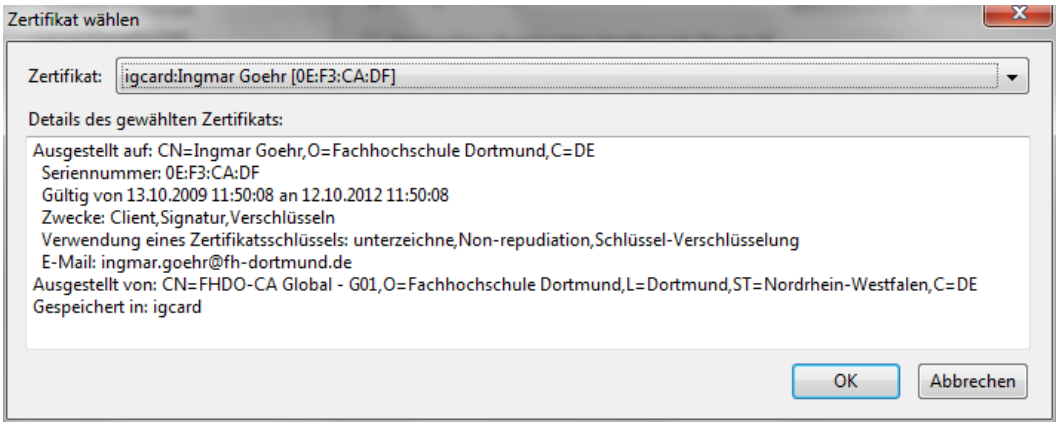

Abbildung: Zertifikatsauswahl

Abschließend können Sie noch Standardeinstellungen festlegen, z.B. ob Ihr Mailclient jede ausgehende E-Mail standardmäßig signieren und/oder verschlüsseln soll.

Versenden und Empfangen signierter E-Mail

Wenn Sie Ihre Standardeinstellung nicht so eingestellt haben, jede E-Mail zu signieren, können Sie die Signaturfunktion beim Verfassen der E-Mail über den Button "S/MIME" auswählen.

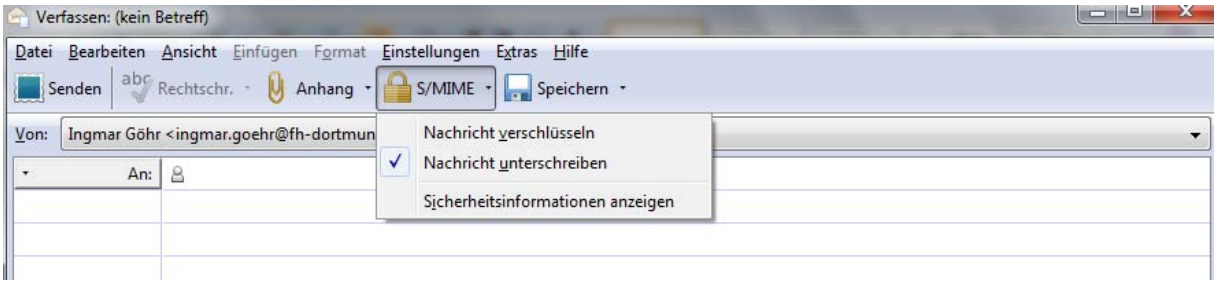

Abbildung: E-Mail signieren

Nach klicken auf den Sendebutton werden Sie zur Eingabe Ihrer PIN aufgefordert, sofern Sie nicht schon an Ihrer Smartcard angemeldet sind, und es wird unter Verwendung Ihres privaten Schlüssels eine Signatur erzeugt.

Ihre signierte E-Mail erhält daraufhin in der Kopfzeile bei Ihrem Empfänger einen Umschlag. Bei einem Klick darauf werden Informationen zur Signatur angezeigt. Zur Überprüfung kann man sich auch Detailinformationen anzeigen lassen, indem das Unterschriftszertifikat aufgerufen wird.

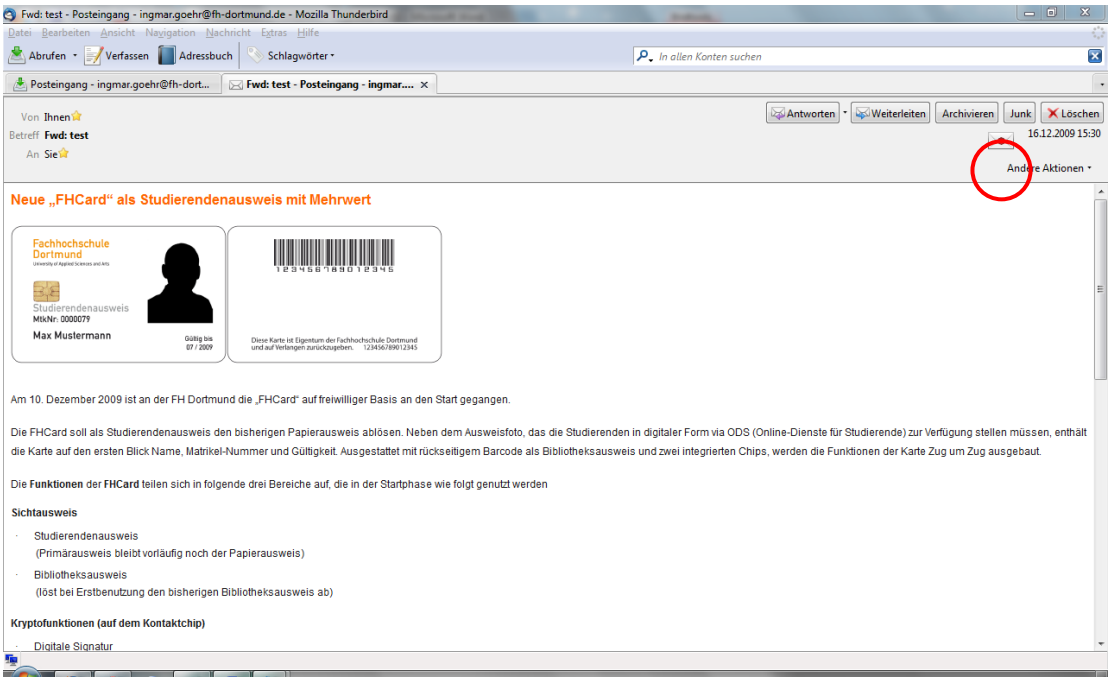

Abbildung: Signaturinformationen

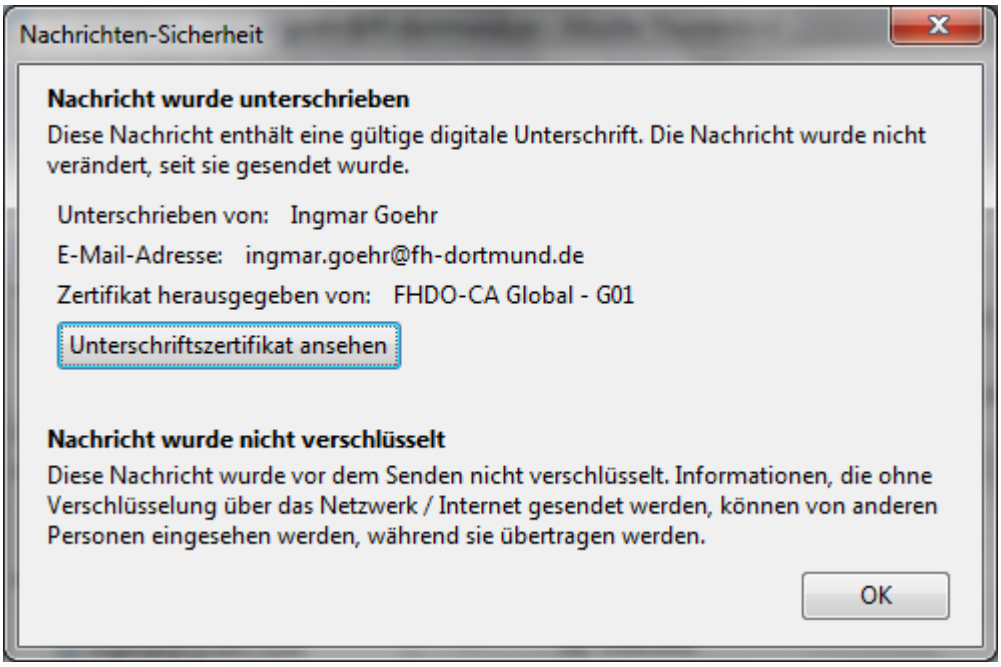

Abbildung: Detailinformationen