



Verwendung eines persönlichen Zertifikats der UHH-CA mit dem Apple-Mail-Programm unter MacOS-X 10.6 Version 0.2



Das zuvor über die Internetseiten der UHH-CA erstellte persönliche Zertifikat muss zur Verwendung im Apple-Mail-Programm in das Schlüsselbundverwaltungsprogramm des Apple Betriebssystems importiert werden. Hierzu muss die Zertifikatdatei (im Beispiel zertifikat.p12) durch Doppelklick ausgewählt werden (Abb. 1).

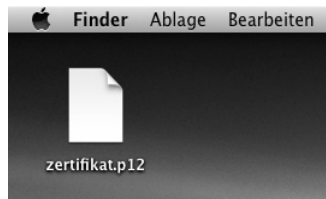


Abb. 1: Persönliches Zertifikat

Sollte die Datei durch ein Passwort geschützt sein, so wird dieses abgefragt (Abb. 2).

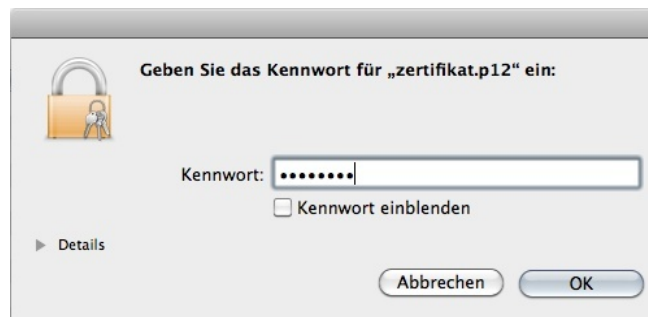


Abb. 2: Evtl. vorhandenes Passwort eingeben.

Es folgen keine weiteren Abfragen. Nach dem erfolgreichen Import des Zertifikats erscheinen in der "Schlüsselbundverwaltung" einige neue Einträge. Neben dem eigenen Zertifikat sind dies die weiteren Zertifikate der Zertifizierungskette, sowie ein Eintrag für den persönlichen Schlüssel (Abb. 3a und 3b).



Abb. 3a: Schlüsselbundverwaltung vor dem Zertifikatimport



Abb. 3a: Schlüsselbundverwaltung nach dem Zertifikatimport

Liegt in der Apple MacOS-X Schlüsselbundverwaltung ein Zertifikat für einen im Apple-Mail-Programm angelegten Account vor, so bietet das Apple-Mail-Programm, ohne weitere Konfiguration, die Möglichkeit zum Signieren und Verschlüsseln an. Hierfür erscheinen zwei zusätzliche Buttons rechts unterhalb der Betreffzeile in der Eingabemaske zum Erstellen einer neuen E-Mail (Abb. 4a und 4b).



Abb. 4a: Apple-Mail-Eingabemaske für neue E-Mail ohne passendes Zertifikat

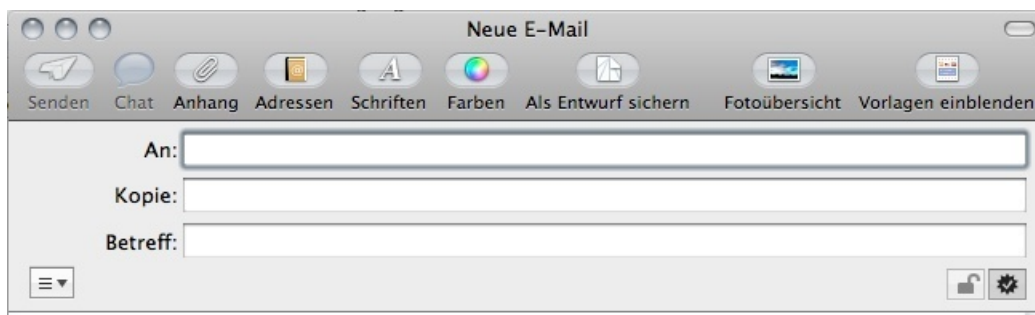


Abb. 4a: Apple-Mail-Eingabemaske für neue E-Mail mit passendem Zertifikat

Hierbei ist jedoch zu beachten, dass die im Zertifikat hinterlegte E-Mail-Adresse exakt mit der E-Mail-Adresse des im Apple-Mail-Programm angelegten Account übereinstimmen muss.

Zum Verschlüsseln einer E-Mail muss dem Apple-Mail-Programm das Zertifikat des Empfängers vorliegen. Dies ist der Fall, wenn man dieses entweder importiert hat, bereits eine signierte E-Mail von dem Adressaten erhalten hat oder das Apple-Mail-Programm so konfiguriert wurde, dass es einen LDAP-Server abfragt auf dem das Empfänger-Zertifikat hinterlegt wurde.