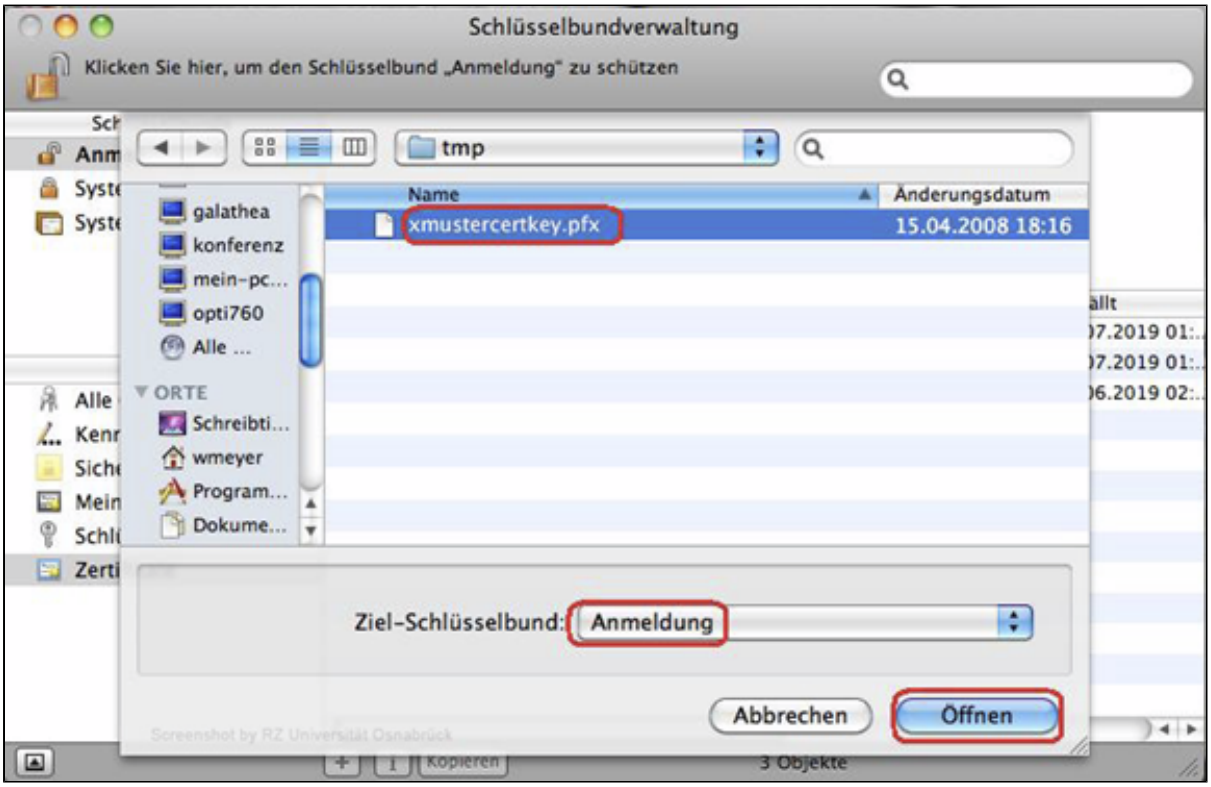
Zertifikat MacOS

Zertifikatsinstallation

Das über die Zertifizierungsinstanz der Hochschule Magdeburg-Stendal beantragte persönliche Zertifikat (Benutzerzertifikat) wird standardmäßig in den **Zertifikatsspeicher des Browsers** abgelegt, **mit dem es beantragt** wurde. Um das persönliche Zertifikat in **Apple Mail** zum **Signieren** und **Ver schlüsseln** zu nutzen, muss es in die **Schlüsselbundverwaltung** importiert werden. Damit dies möglich ist, wird das persönliche Zertifikat als Datei im **PKCS#12-Format**, dies entspricht den Dateitypen **pfx** beziehungsweise **p12,** benötigt. Die geforderte Datei erhält man, indem das persönliche Zertifikat aus dem Browser **exportiert** wird, **mit dem es beantragt** wurde.
Hinweis: Es empfiehlt sich zum Beantragen und Exportieren des persönlichen Zertifikates den **Firefox**- Browser zu verwenden, da mit **Safari** kein Zertifikatexport möglich ist.

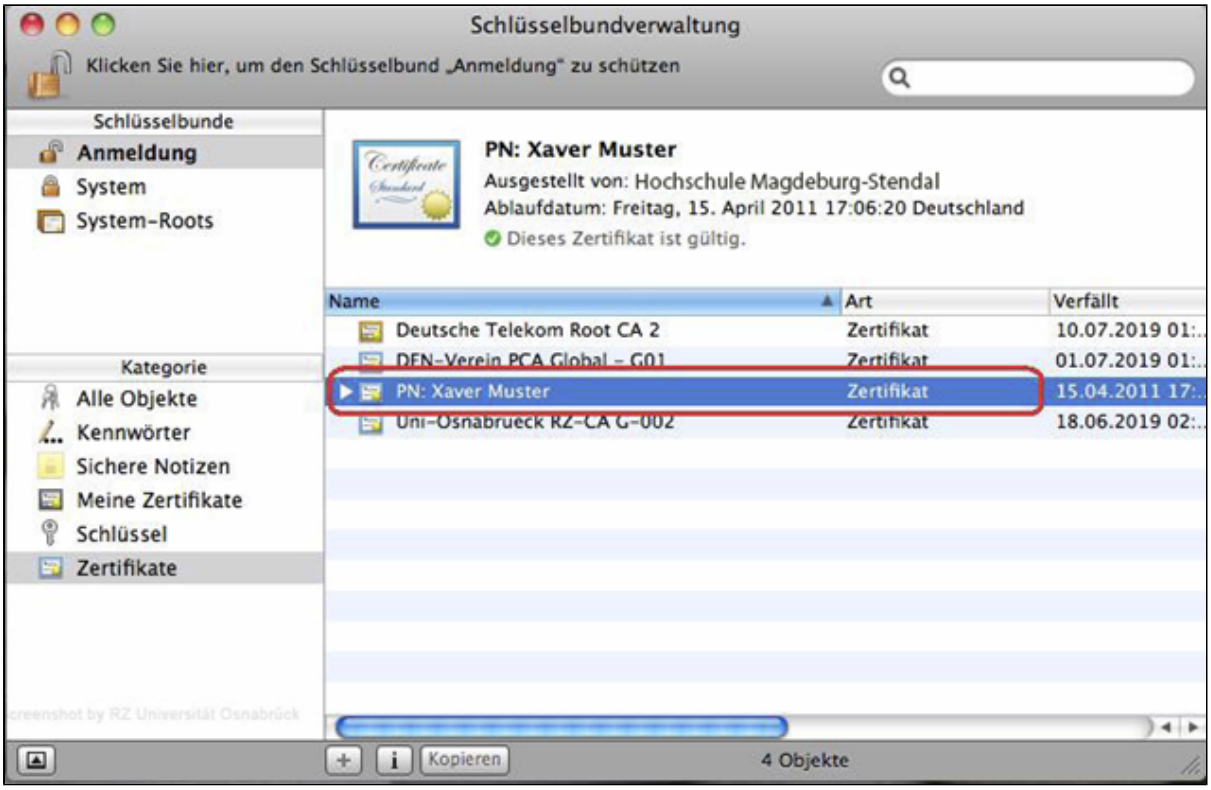
Die Installation des persönlichen Zertifikates über eine Zertifikatsdatei (hier: **xmustercertkey.pem**) erfolgt in 3 Arbeitsschritten:

1. Starten der **Schlüsselbundverwaltung**.
2. Im Menü **Ablage** das Untermenü **Objekte importieren...** auswählen.
3. Jetzt wird in das Verzeichnis gewechselt, in dem die zuvor aus dem Browser exportierte Zertifikatsdatei liegt. Die Datei (hier: **xmustercertke y.pfx**) wird selektiert; als **Ziel-Schlüsselbund** wird **Anmeldung** ausgewählt und über die Schaltfläche **Öffnen** startet der Importdialog.



Beim Öffnen der persönlichen Zertifikatsdatei wird das Kennwort verlangt, das beim Export angegeben wurde.

Die **Schlüsselbundverwaltung** zeigt jetzt das erfolgreich importierte persönliche Zertifikat an.



Verschlüsseln von E-Mails mit Apple Mail

E-Mails werden immer mit dem **öffentlichen Schlüssel** aus dem **persönlichen Zertifikat des Empfängers** verschlüsselt. Wenn beispielsweise **Xaver Muster** eine **verschlüsselte E-Mail an Yvonne Muster senden** will, benötigt er dazu den **öffentlichen Schlüssel** des persönlichen Zertifikates von Yvonne Muster.

1. Öffentlichen Schlüssel des Empfängers verfügbar machen

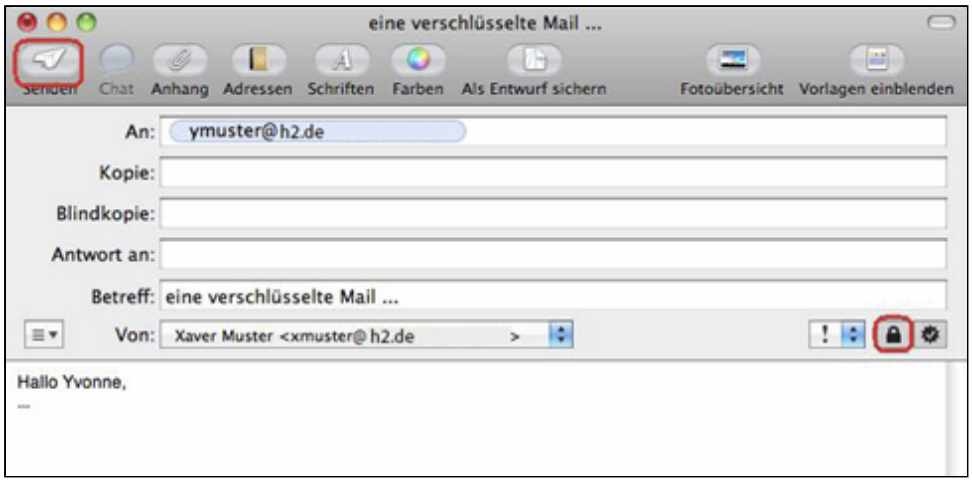
   Wie kommt Xaver Muster an den **öffentlichen Schlüssel** aus dem persönlichen Zertifikat von Yvonne Muster? Es gibt verschiedene Methoden **öffentliche Schlüssel** verfügbar zu machen.

   Im Folgenden wird ein möglicher Weg für **Apple Mail** beschrieben:

   Xaver lässt sich eine **signierte** E-Mail von Yvonne **zusenden**. Durch das Öffnen der signierten E-Mail wird der **öffentliche Schlüssel** von Yvonnes persönlichem Zertifikat **automatisch** in den Schlüsselbund von **Apple Mail** übernommen. Xaver Muster kann den **öffentlichen Schlüssel** von Yvonne jetzt nutzen, um ihr **verschlüsselte** E-Mails zuzusenden.
2. Erzeugen einer verschlüsselten Mail

   Nachdem Xaver Muster den **öffentlichen Schlüssel** des persönlichen Zertifikates von Yvonne Muster besitzt, kann er diesen nutzen, um eine **verschlüsselte** E-Mail an Yvonne **zu schicken**.
   Die E-Mail an Yvonne Muster wird geschrieben und anschließend **verschlüsselt**, indem mit der Maus auf das **Verschlüsselungs-Symbol** (hier: rot eingekreist) geklickt wird. Über Senden wird die E-Mail versendet.

Hinweis:
Die E-Mail-Adresse des Empfängers muss **exakt** so geschrieben werden, wie sie im persönlichen Zertifikat des Empfängers **enthalten** ist. Ansonsten funktioniert das Verschlüsseln **nicht**.



3. Lesen einer verschlüsselten Mail

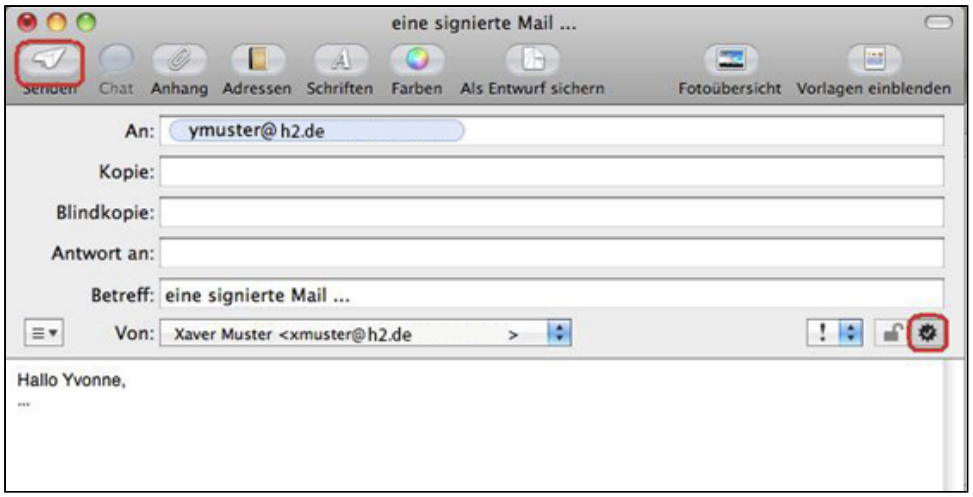
   Öffnet Yvonne die E-Mail von Xaver, wird sie **automatisch** entschlüsselt. Dazu benutzt Apple Mail den **privaten Schlüssel** des persönlichen Zertifikates von Yvonne Muster. Das **Schloss-Symbol** zeigt an, dass die E-Mail vom Absender (hier: **Xaver Muster**) verschlüsselt wurde.

Signieren von E-Mails

Nachdem das **persönliche Zertifikat** in der Schlüsselbundverwaltung vorliegt, können **E-Mails** beim **Versenden** mit einer **Signatur** versehen werden. Das folgende Beispiel beschreibt, wie der fiktive Benutzer **Xaver Muster** der fiktiven Benutzerin **Yvonne Muster** eine **signierte E-Mail** zusendet.

1. Erzeugen einer E-Mail mit persönlicher Signatur

   Nach dem Starten von **Apple Mail** wird eine Nachricht geschrieben, die signiert werden soll.
   Zum Signieren wird das **Signatur-Symbol** (hier rot eingekreist) benutzt.
   Über die Schaltfläche **Senden** wird dann die **signierte E-Mail** verschickt.



2. Prüfen der Signatur einer empfangenen E-Mail

   Das folgende Beispiel beschreibt, wie die fiktive Benutzerin **Yvonne Muster die Signatur einer E-Mail prüft**, die sie von **Xaver Muster** erhalten hat. Nach dem Start von **Apple Mail** wird im **Posteingang** von **Yvonne Muster** die **E-Mail** von **Xaver Muster** geöffnet. In der E-Mail befindet sich ein Symbol (**hier:** rot eingekreist), das anzeigt, dass die **E-Mail signiert** wurde.
   Durch Klicken auf das **Signatur-Symbol** werden die Informationen zur Signatur des Absenders (hier: **Xaver Muster**) angezeigt.