

Aktivierung der digitalen Signatur für Apple Mac

Version 1.1
30. Mai 2008

QuoVadis Trustlink Schweiz AG
Teufenerstrasse 11
9000 St. Gallen

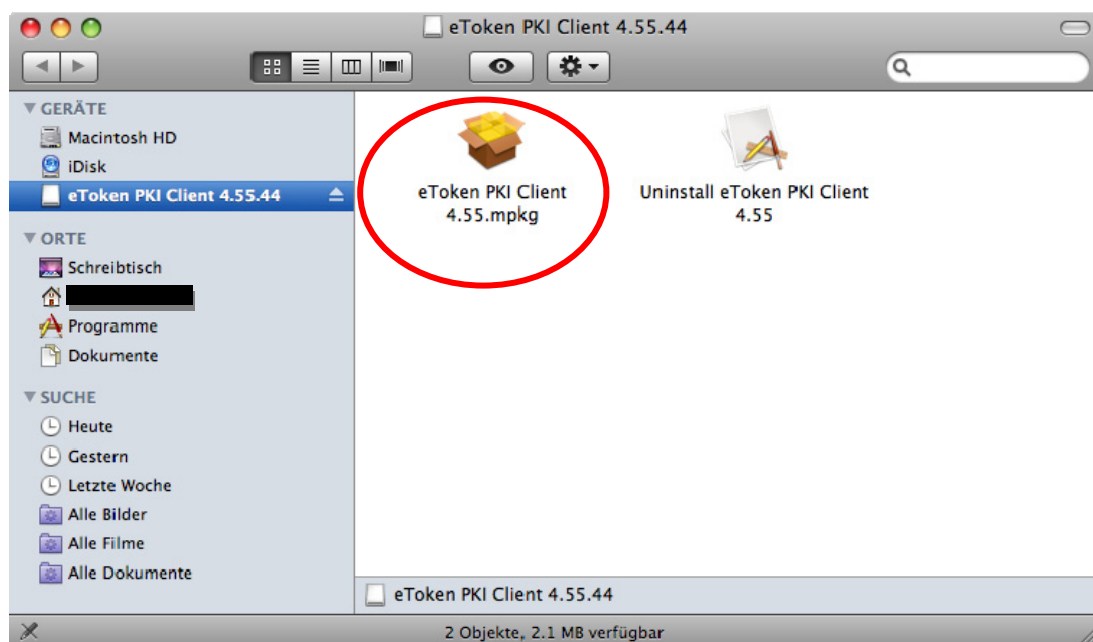
Phone +41 71 272 60 60
Fax +41 71 272 60 61
www.quovadis.ch

Voraussetzung

Damit die digitale Signatur in Mail oder Microsoft Entourage aktiviert werden kann müssen die entsprechenden Treiber und die Client-Software des USB Tokens installiert und lauffähig sein.

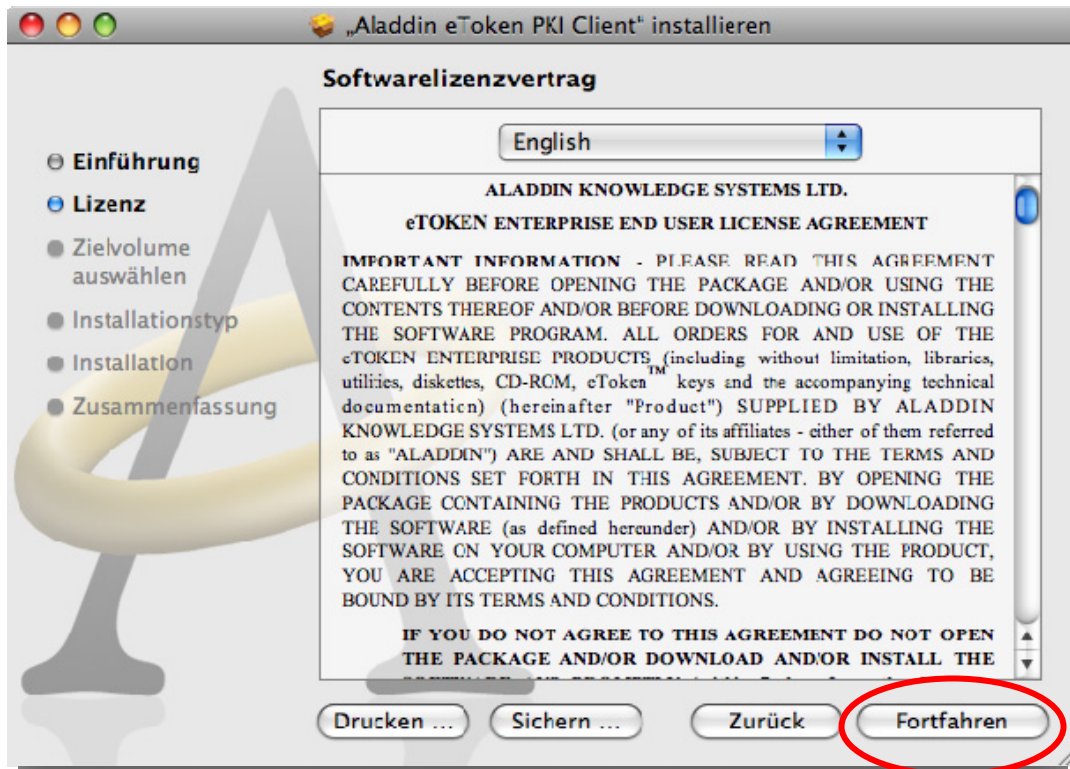
Installation des Aladdin PKI Clients

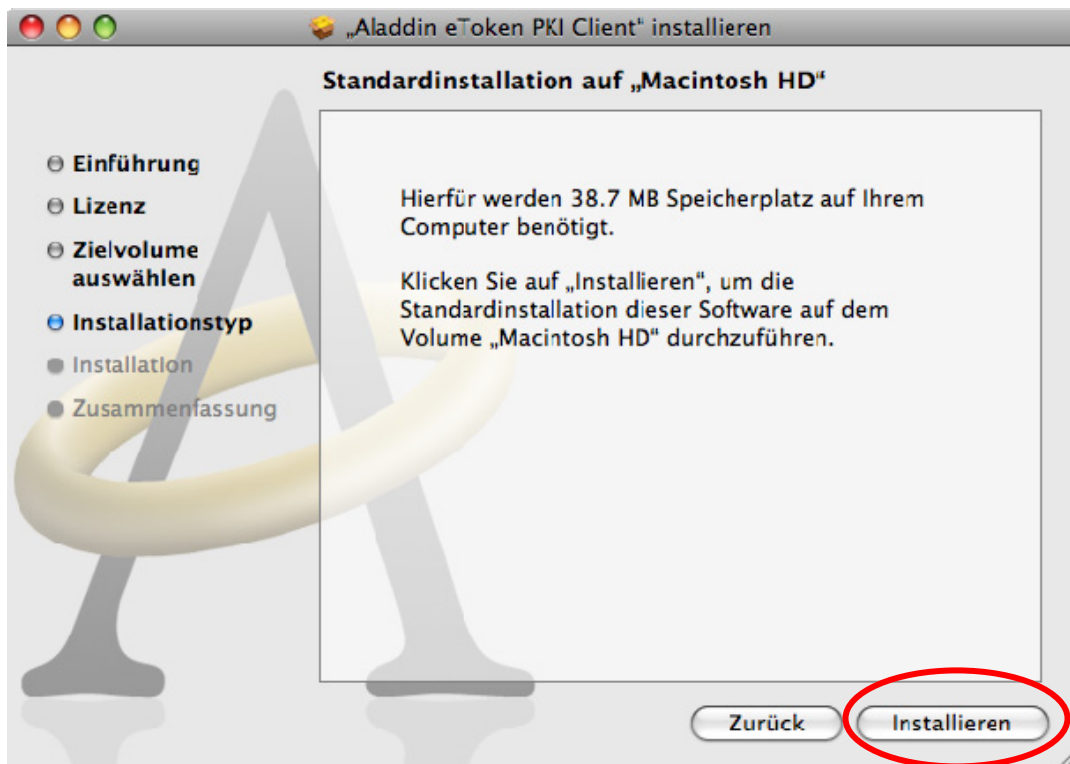
Entpacken Sie die Datei **pkiclient.4.55.44.dmg.zip**, doppelklicken Sie die Datei **PKI_Client_4.55.dmg** so dass Sie den folgenden Ordnerinhalt erhalten:



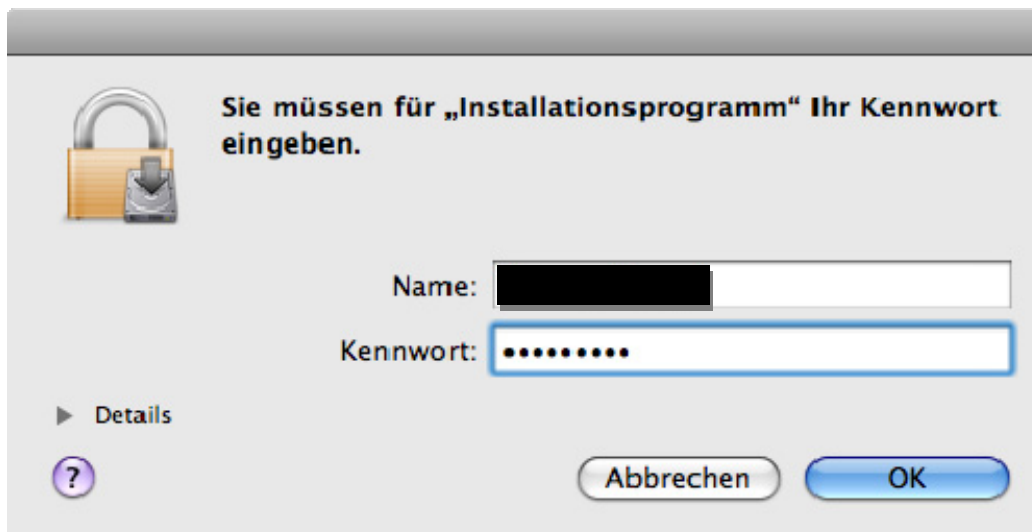
Starten Sie **eToken PKI Client 4.55.mpkg** und folgen Sie den Anweisungen des Installationsassistenten:







Damit die Installation ausgeführt werden kann müssen Sie die Administratorrechte aktivieren indem Sie auf das Schlosssymbol klicken. Sie werden aufgefordert das Kennwort einzugeben. Bestätigen Sie die Eingabe mit Klicken auf OK.



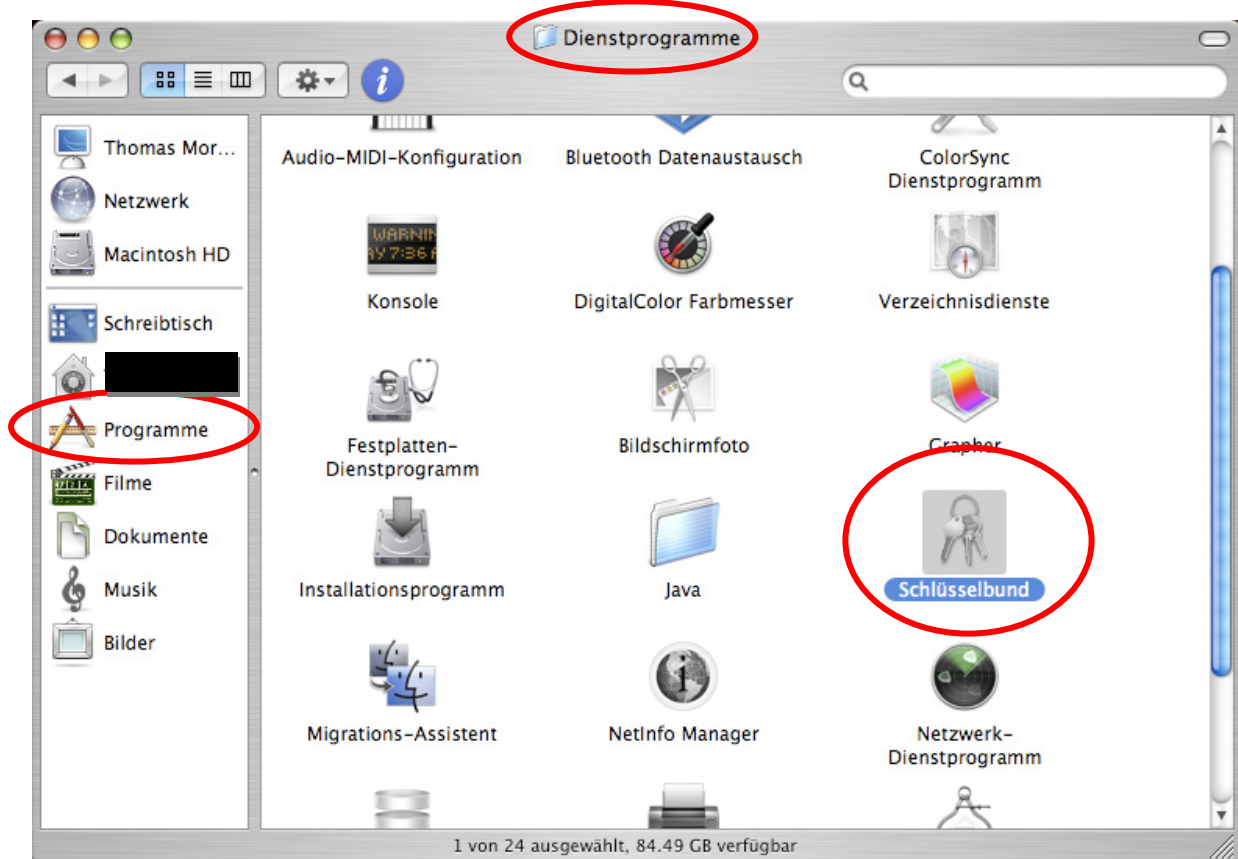
Aktivierung der digitalen Signatur für Apple Mac



Nach erfolgreicher Installation werden Sie unter Umständen aufgefordert Ihren Rechner neu zu starten oder sich abzumelden. Bitte führen Sie diese jeweilige Anweisung jetzt aus, damit die Einrichtung korrekt vorgenommen werden kann.

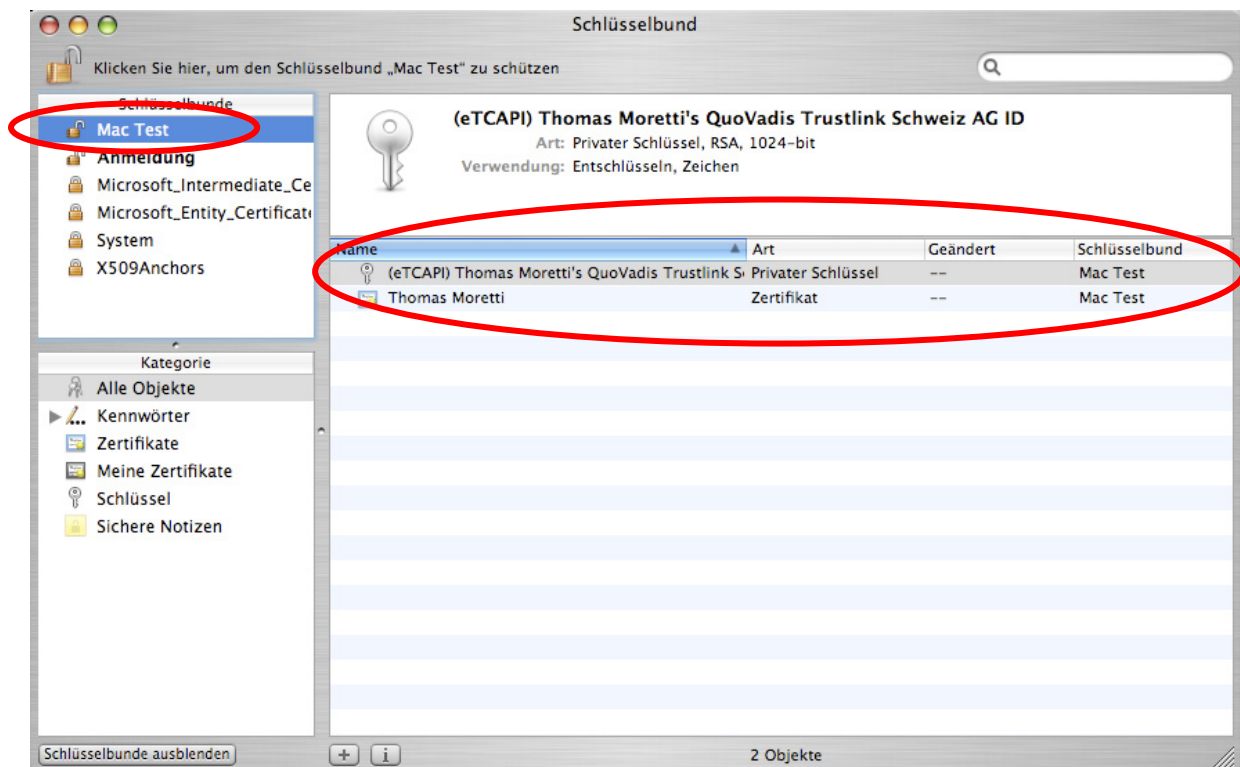
Überprüfung des Schlüsselbunds

Mac OS X verwaltet Zertifikate in so genannten Schlüsselbunden. Das entsprechende Programm kann unter den Dienstprogrammen aufgerufen werden:



Aktivierung der digitalen Signatur für Apple Mac

Wurde der Token zuvor eingesteckt oder während der Ausführung des Programms eingesteckt erscheint ein neuer „Schlüsselbund“ der den Inhalt des USB Tokens zeigt:



Sobald der USB Token im Schlüsselbund sichtbar ist, kann mit der Einrichtung des Mail Clients begonnen werden.

Einrichten des Mozilla Thunderbird Mail Clients

Für die Aktivierung der Signatur unter Mozilla Thunderbird gibt es ein eigenes Dokument, weshalb hier nicht weiter darauf eingegangen wird.

Da das erwähnte Dokument für eine Windows Installation geschrieben wurde, wird hier noch speziell darauf eingegangen, wo sich die PKCS#11 Datei auf dem Mac Rechner befindet.

Unter dem Menü **Thunderbird, Einstellungen, Bereich „Erweitert“, im Register Zertifikate** können Sie die notwendigen **Kryptographie-Module** laden.

Für das Laden der PKCS#11 Datei müssen Sie im Pfad manuell folgenden Dateipfad angeben:

`/usr/local/lib/libeTPkcs11.dylib`

Die restlichen Einstellungen entsprechen im Grossen und Ganzen denjenigen der Windows Installation.

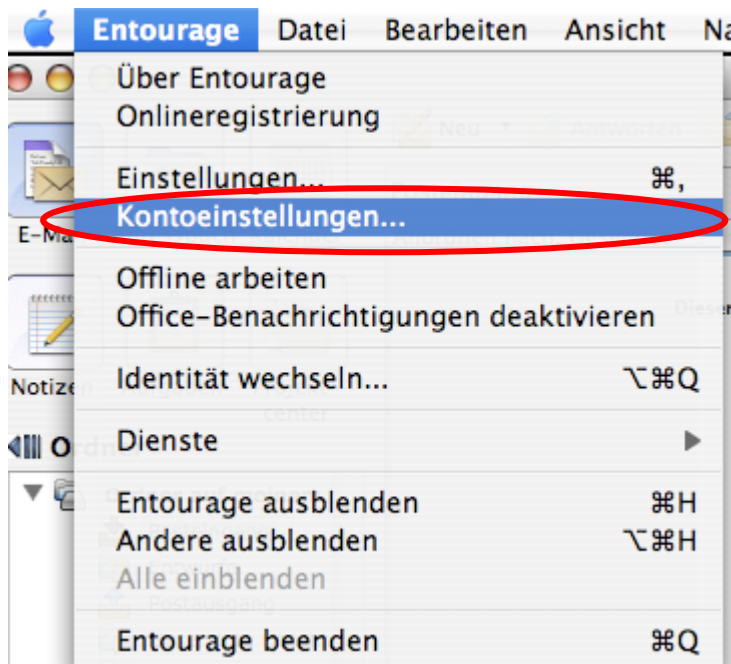
Einrichten des Entourage Mail Client

Starten Sie das Programm Entourage aus dem Paket Microsoft Office for Mac:



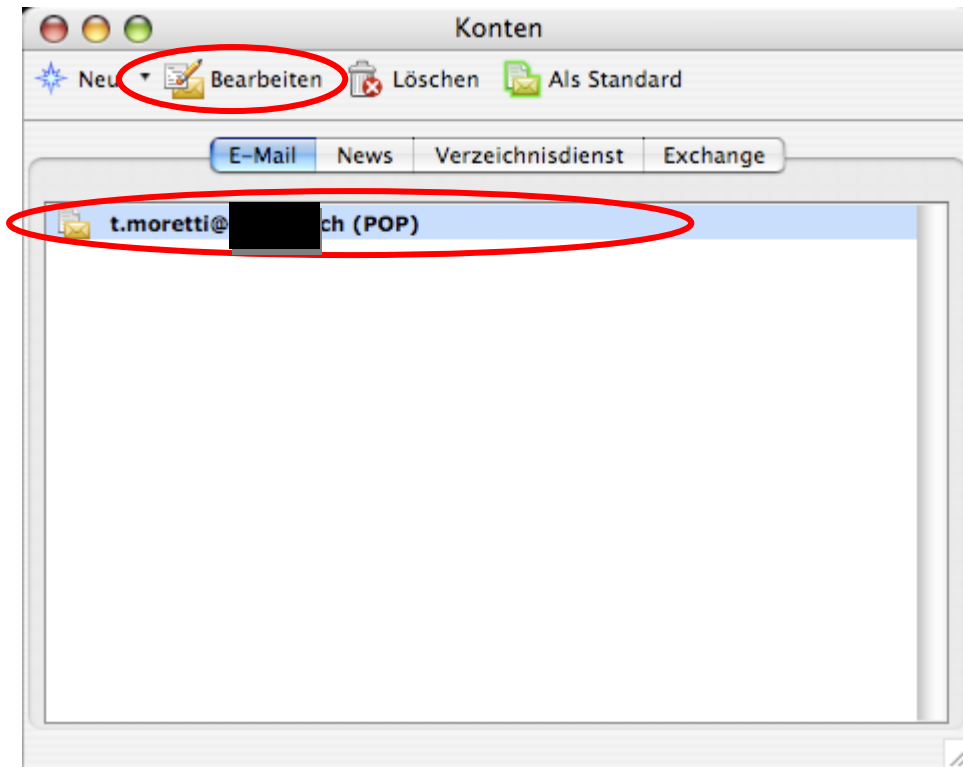
Microsoft Entourage

Rufen Sie „Kontoeinstellungen...“ unter dem Menü „Entourage“ auf:



Aktivierung der digitalen Signatur für Apple Mac

Wählen Sie jetzt das Mailkonto aus, das Sie mit dem Zertifikat verbinden möchten und klicken anschliessend auf die Schaltfläche „Bearbeiten“:



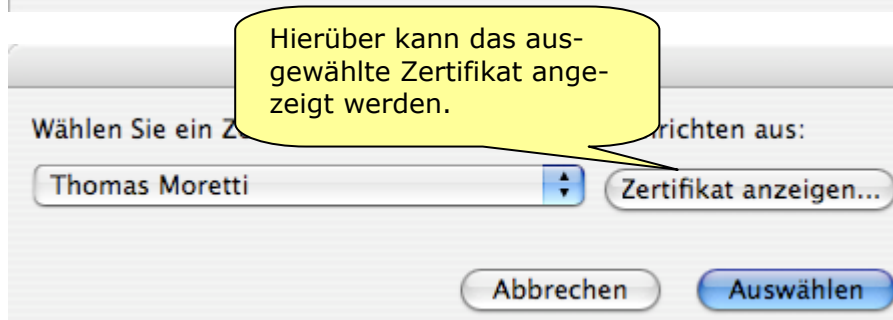
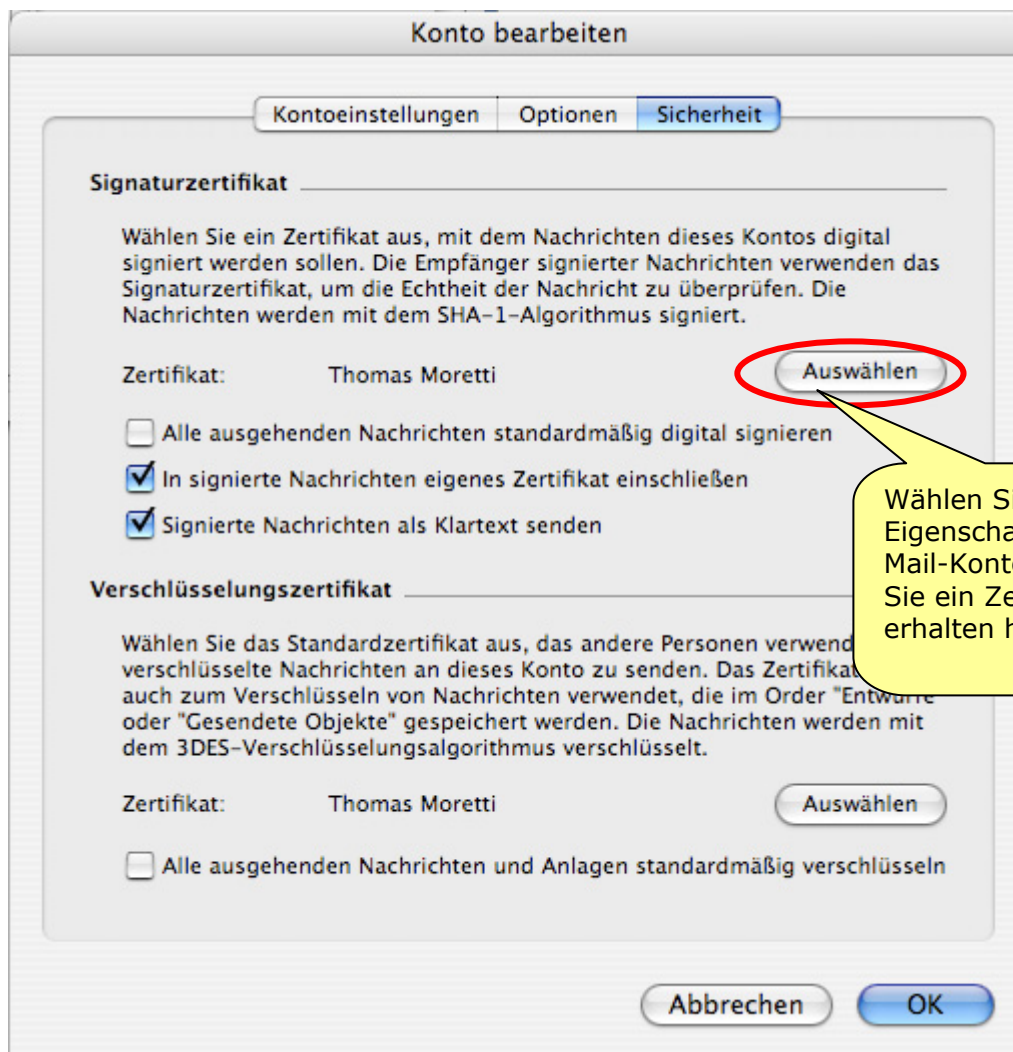
Wechseln Sie anschliessend in den Bereich Sicherheit und wählen Sie das entsprechende Zertifikat aus, das Sie für das Signieren und/oder Verschlüsseln verwenden möchten. Ist der USB Token eingesteckt müssten Sie das/die Zertifikat/e sehen, die für diesen Mail-Account auswählbar sind.



Hinweis

Es können nur Zertifikate ausgewählt werden bei denen die Mail-Adresse der Mail-Adresse im Mail-Konto entspricht.

Aktivierung der digitalen Signatur für Apple Mac





Wiederholen Sie nun die Auswahl für das Verschlüsselungszertifikat.



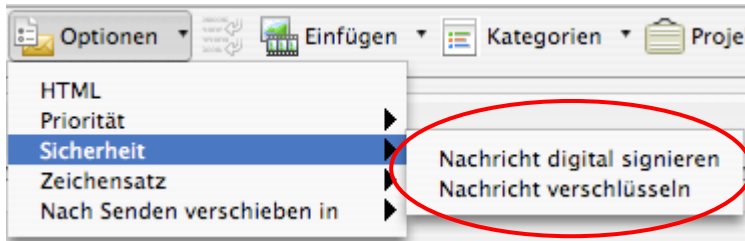
Hinweis

Falls Sie Ihre Nachrichten immer digital signieren oder grundsätzlich Mails verschlüsselt versenden möchten (vorausgesetzt die Empfänger besitzen alle ein Zertifikat), können Sie die Voreinstellungen unter „Konten bearbeiten“, Bereich „Sicherheit“ wählen:

- Alle ausgehenden Nachrichten standardmässig digital signieren
- Alle ausgehenden Nachrichten und Anlagen standardmässig verschlüsseln

Verfassen eines e-Mails in Entourage

Öffnen Sie eine neue Nachricht in Entourage. Unter der Schaltfläche „Optionen“ finden Sie unter Sicherheit die beiden Menüpunkte um Mail zu signieren und/oder zu verschlüsseln.

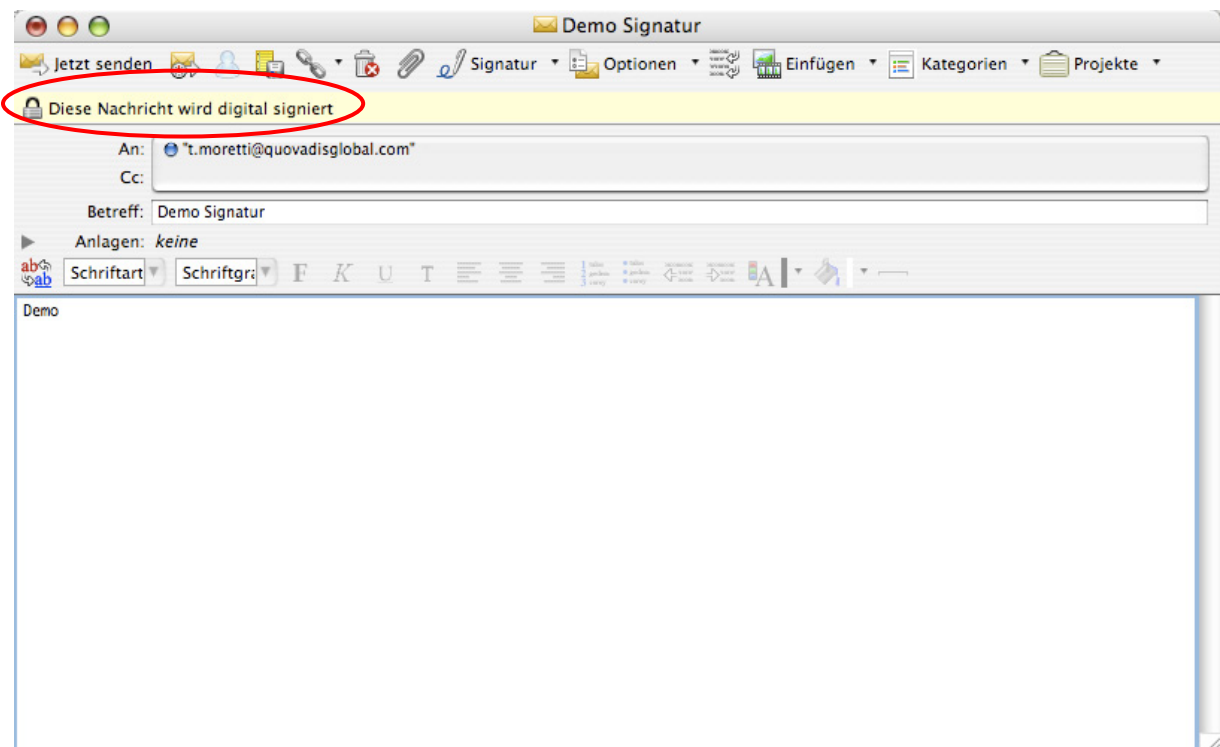


Hinweis

Damit eine Nachricht verschlüsselt werden kann ist es notwendig, dass Sie den öffentlichen Schlüssel respektive das Zertifikat des Empfängers besitzen.

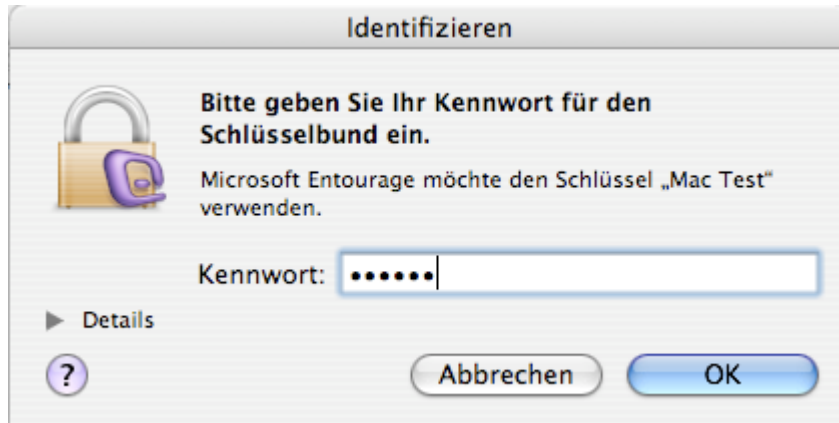
Das Zertifikat erhalten Sie, wenn Sie vom Empfänger eine signierte Nachricht erhalten oder es aus einem öffentlichen Verzeichnis herunterladen. Sie können sich das Verschlüsselungszertifikat des Empfängers auch im Adressbuch, im Bereich Zertifikate, importieren (bei geöffnetem Kontakt). Der Import entfällt, wenn Sie ein signiertes Mail erhalten. Dabei wird der Kontakt inklusive Zertifikat abgelegt und steht für künftige Mails zur Verfügung.

Entourage zeigt an, wenn ein ausgehendes Mail signiert werden soll.



Aktivierung der digitalen Signatur für Apple Mac

Beim Versenden der fertigen Nachricht werden Sie, vorausgesetzt Sie möchten Ihre Nachricht signieren, aufgefordert den PIN einzugeben:



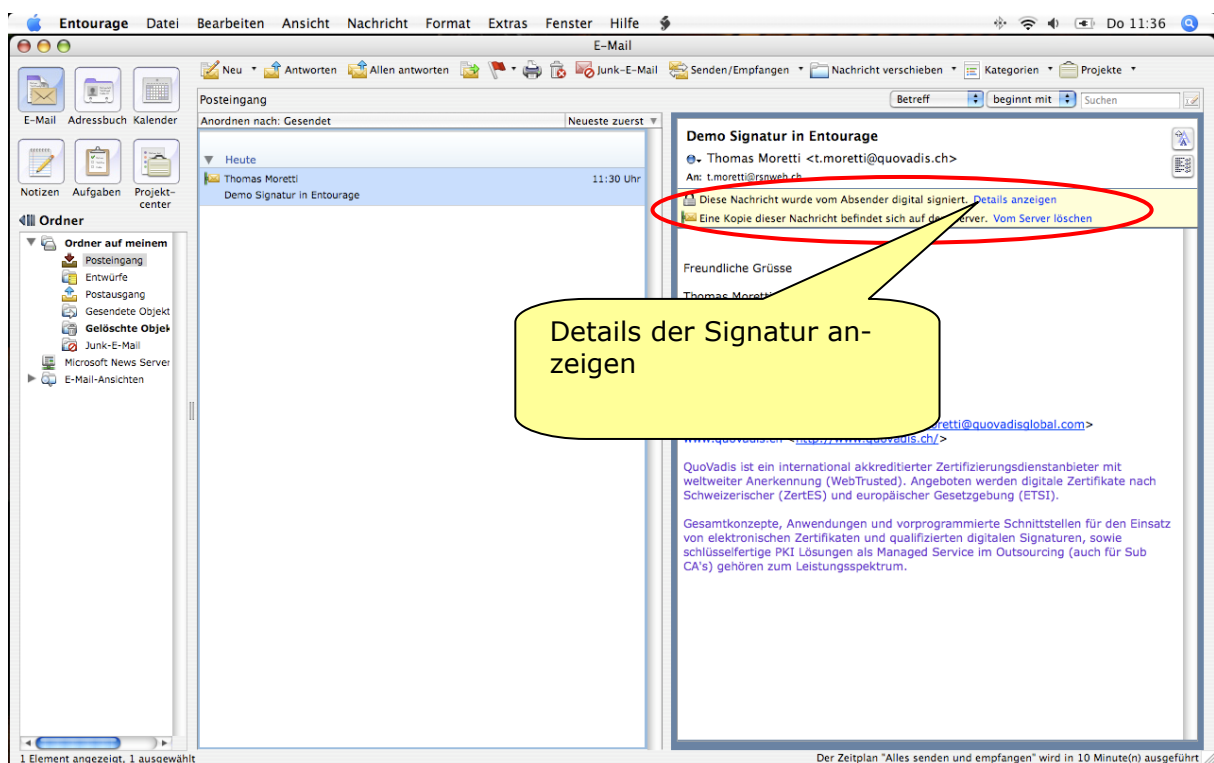
Hinweis

Beim reinen Verschlüsseln von Nachrichten wird die Eingabe des PINs nicht benötigt, da die Nachricht nicht signiert wurde.

Prüfen einer e-Mail-Signatur und -Verschlüsselung in Entourage

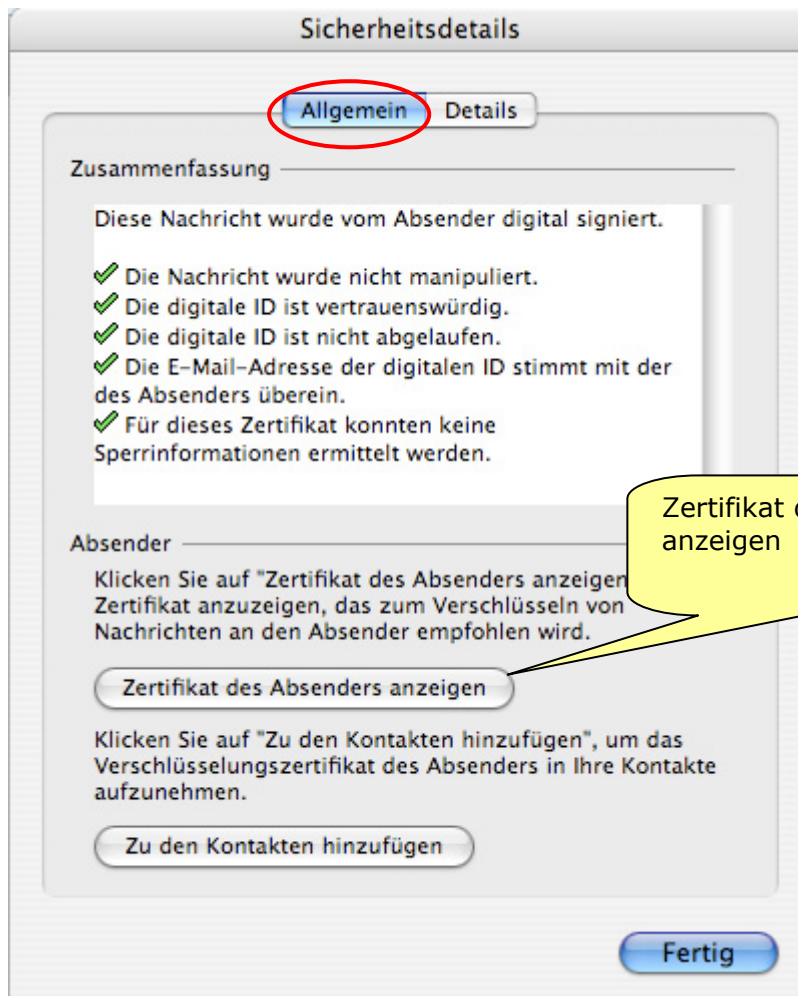
Wenn Sie eine signierte und/oder verschlüsselte Nachricht erhalten sollten Sie die Signatur/Verschlüsselung überprüfen um sicher zu gehen, dass die Nachricht auch wirklich vom Absender stammt und/oder während der Übermittlung nicht verändert wurde.

Wenn Sie die Nachricht öffnen sehen Sie, je nach dem ob Sie die Nachricht signiert und/oder verschlüsselt erhalten die eines oder beide Symbole auf der rechten Seite in den Kopfinformationen des Mails angezeigt:



Klicken Sie zur Überprüfung der Signatur auf den Link „Details anzeigen“. Das System prüft automatisch, ob das Zertifikat, mit welchem das Mail signiert wurde, nach wie vor gültig ist:

Aktivierung der digitalen Signatur für Apple Mac



Aktivierung der digitalen Signatur für Apple Mac



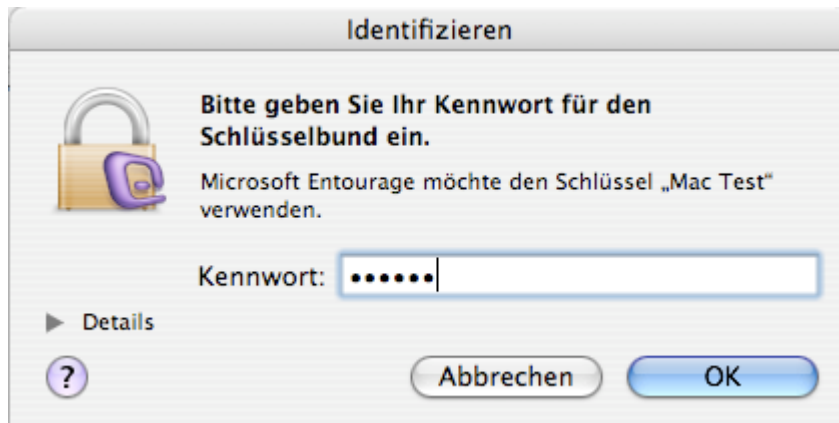
Hinweis

Bei einer signierten oder verschlüsselten Nachricht, einer so genannten S/MIME Nachricht, wird das verwendete Benutzerzertifikat immer auch beigelegt.

Lesen eines verschlüsselten e-Mails in Entourage

Wenn Sie eine verschlüsselte Nachricht erhalten hat der Absender Ihren öffentlichen Schlüssel dafür benutzt die Nachricht zu chiffrieren. Möchten Sie diese Nachricht öffnen bedarf es des USB Tokens mit dem entsprechenden privaten Schlüssel dazu.

Entourage prüft nun durch Aufforderung der Passwort Eingabe, ob Sie zum Lesen der Nachricht berechtigt sind:



Hinweis

Fehlt Ihnen aufgrund eines Verlustes der zugehörige private Schlüssel auf einem USB Token oder der Smartcard lässt sich die Nachricht nicht mehr öffnen.

HAFTUNGSHINWEIS:

Die Angaben in diesem Dokument können jederzeit geändert werden. Für fehlerhafte Angaben und deren Folgen kann weder eine juristische Verantwortung noch irgendeine Haftung übernommen werden. Alle Teile dieses Dokuments unterliegen dem Urheberrecht (Copyright). Alle Rechte sind geschützt. Jegliche Vervielfältigung oder Verbreitung, ganz oder teilweise, ist verboten. Kein Teil des Dokuments darf kopiert werden, fototechnisch übertragen, reproduziert, übersetzt, auf einem anderen elektronischen Medium gespeichert oder in maschinell lesbare Form gebracht werden. Hierzu ist in jedem Fall die ausdrückliche Erlaubnis des Herstellers einzuholen. Für den Inhalt von verlinkten Seiten sind ausschliesslich deren Betreiber verantwortlich. Alle in diesem Dokument erwähnten Hersteller- oder Produktnamen sowie die verwendeten Software- und Hardwarebezeichnungen sind eingetragene Warenzeichen ihrer Hersteller und unterliegen als solche dem Schutz durch die gesetzlichen Bestimmungen. Warennamen werden ohne Gewährleistung der freien Verwendbarkeit benutzt.