QuoVadis Trustlink Schweiz AG

Aktivierung der digitalen Signatur in Windows Mail

Version 1.0
19. August 2007

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

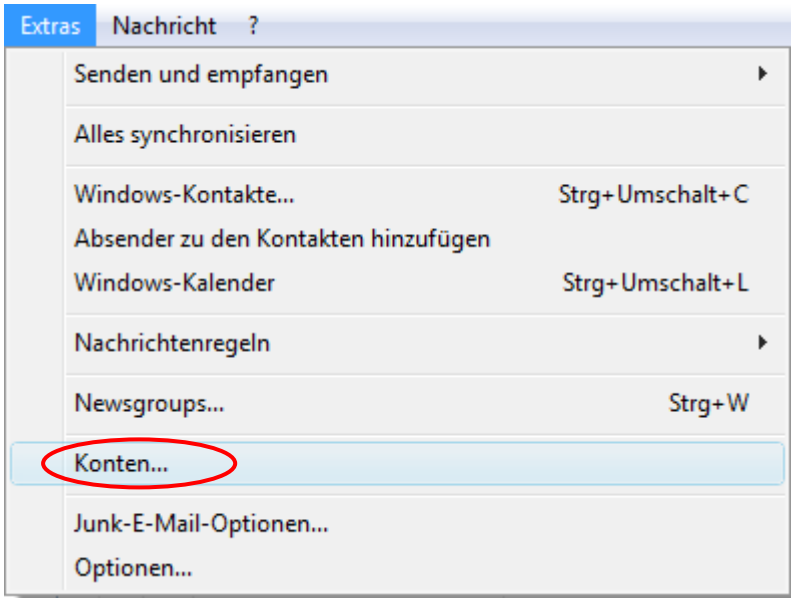
Damit die digitale Signatur in Windows Mail aktiviert werden kann müssen die entsprechenden Treiber und die Client-Software der Smartcard oder des USB Tokens installiert und lauffähig sein.

Stellen Sie sicher, dass sich die Smartcard im Smartcard-Leser befindet und dieser respektive der USB Token korrekt angeschlossen ist.

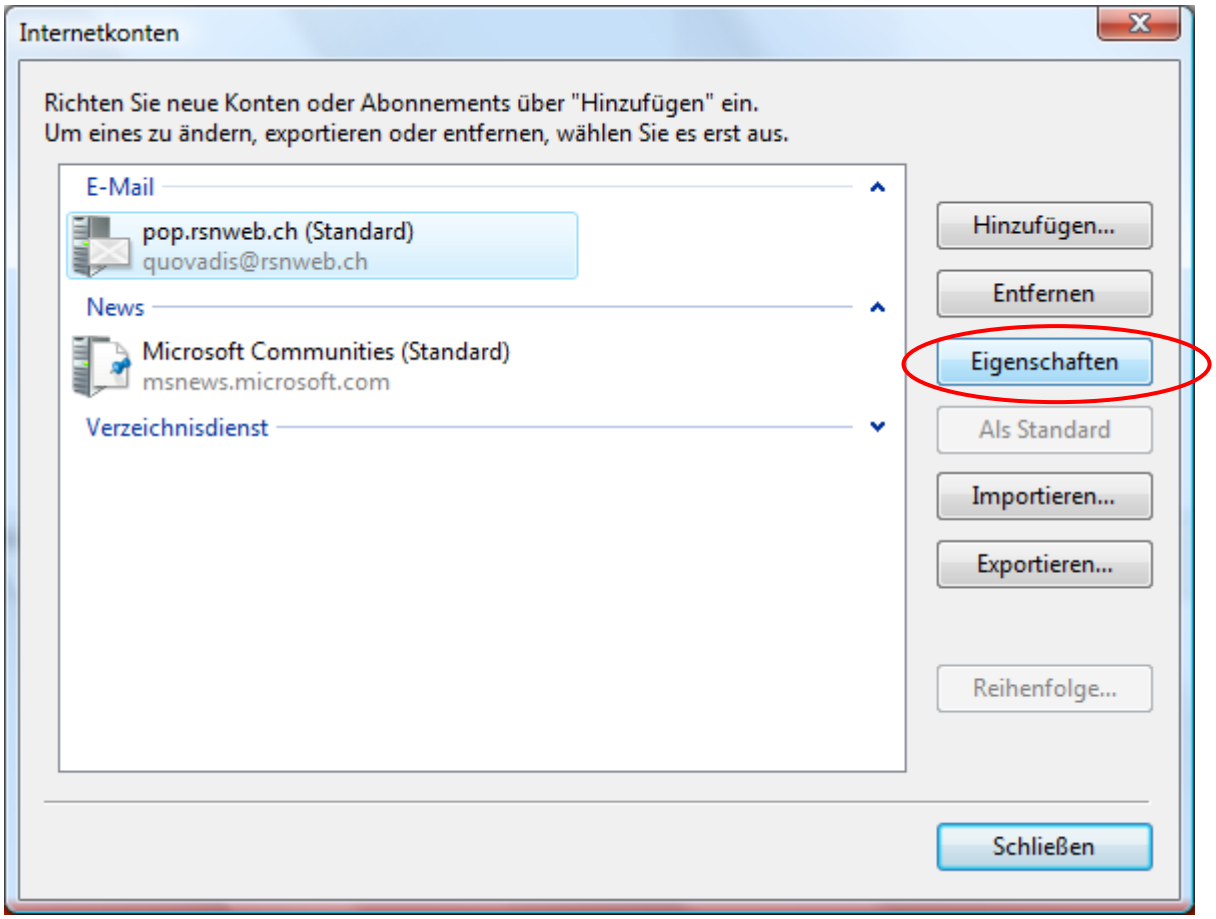
Wichtig ist, dass beim Einsetzen der Smartcard oder des USB Tokens die vorhandenen Zertifikate in den Windows Zertifikatsspeicher publiziert werden.

Einrichten

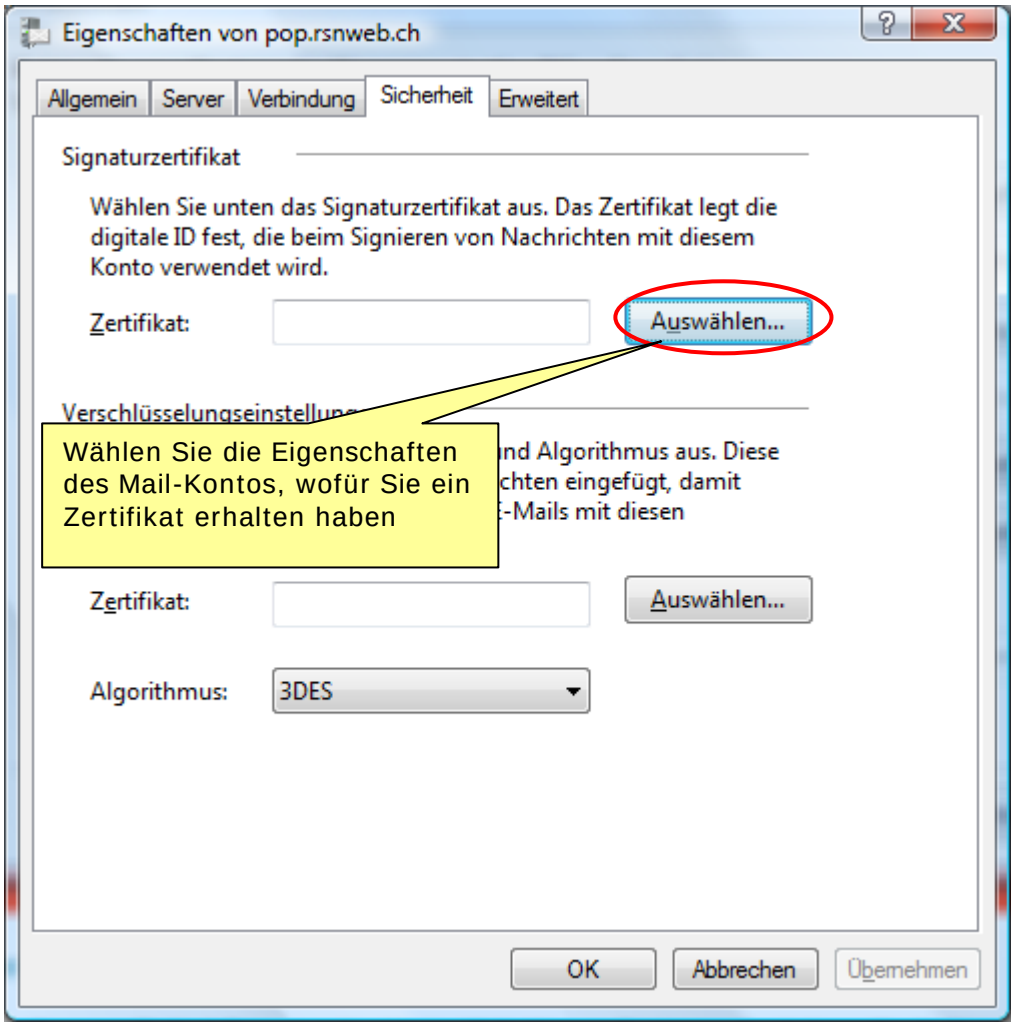
Rufen Sie „Konten…“ unter dem Menü „Extras“ in Windows Mail auf:



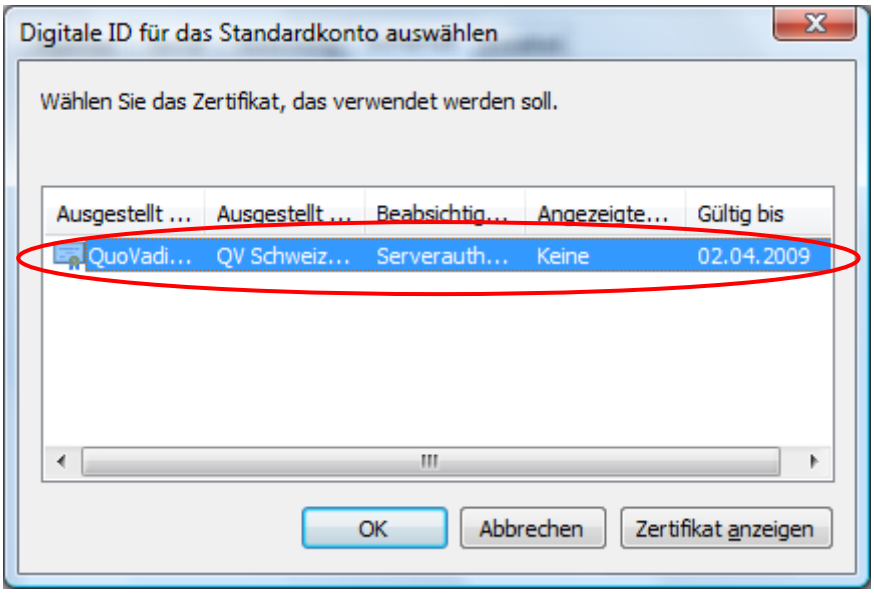
Wählen Sie jetzt das Mailkonto aus, das Sie mit dem Zertifikat verbinden möchten und klicken anschliessend auf die Schaltfläche „Eigenschaften“:



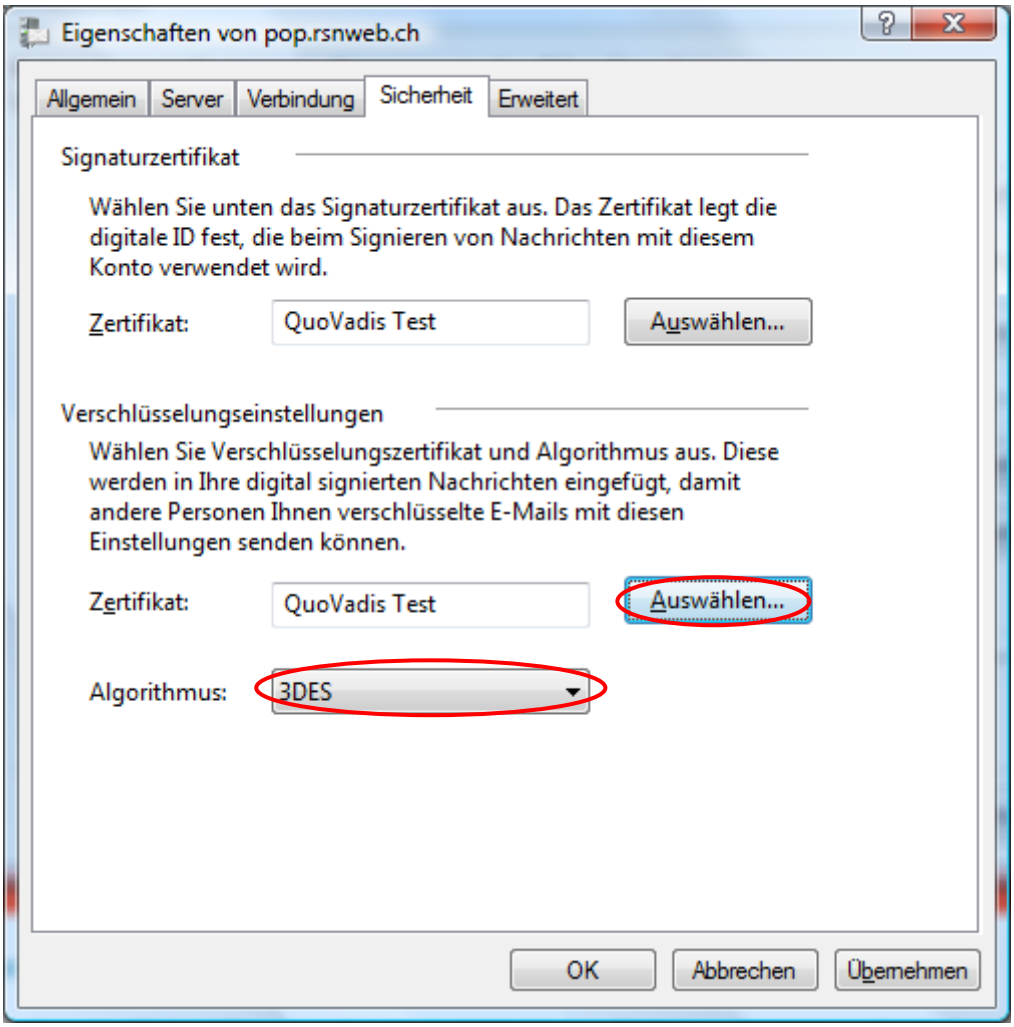
Wechseln im Eigenschaftsdialog auf das Register „Sicherheit“ und klicken Sie auf die Schaltfläche „Auswählen…“ im oberen Bereich Signaturzertifikat – zur Auswahl des Signaturzertifikats.



Wählen Sie nun das entsprechende Zertifikat aus und bestätigen Sie die Eingabe mit Klicken auf die Schaltfläche OK:



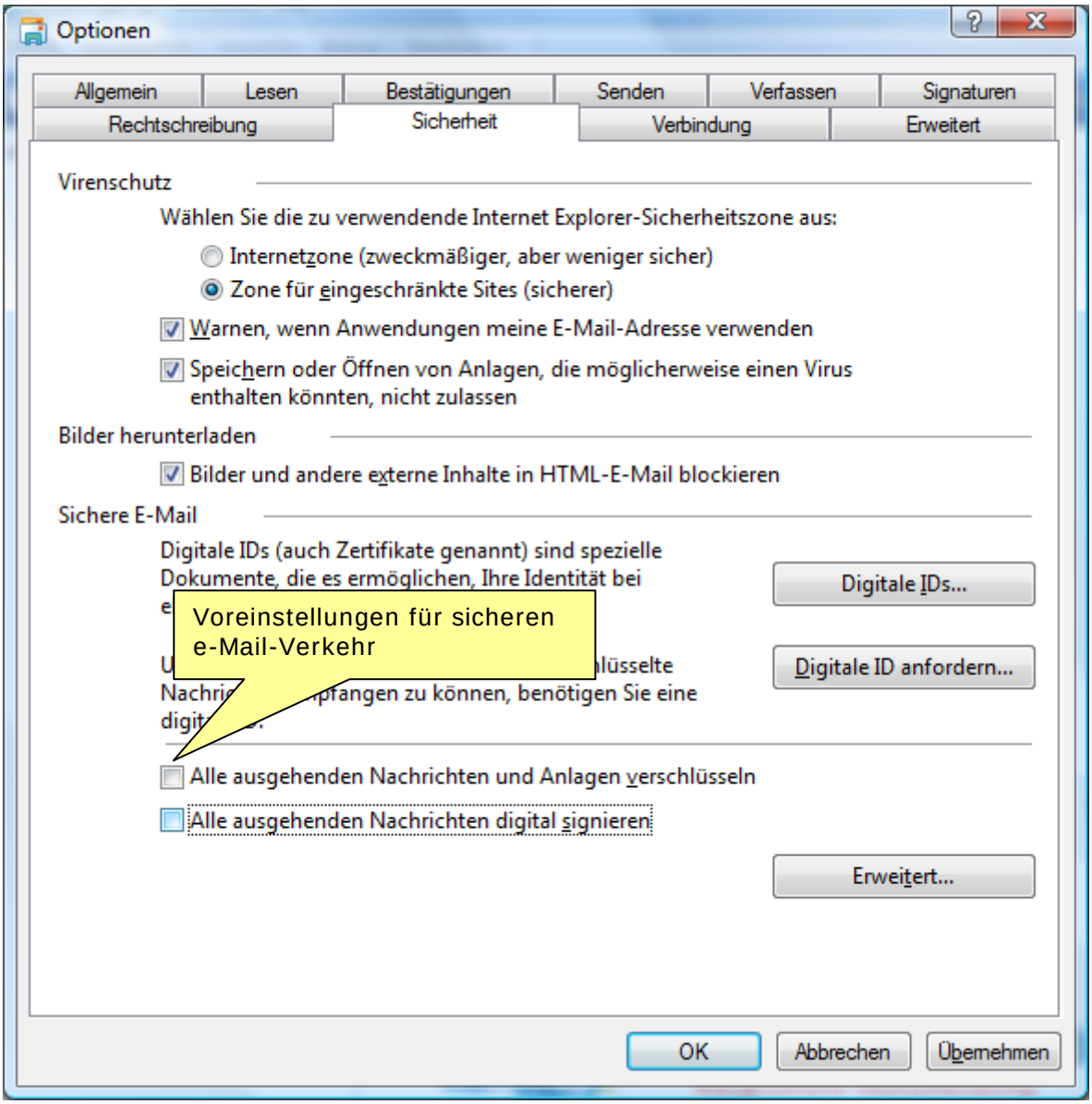
Wiederholen Sie nun die Auswahl für das Verschlüsselungszertifikat:



Belassen Sie den Algorithmus auf 3DES und bestätigen Sie mit einem Klick auf „OK“. Schliessen Sie anschliessend den Dialog „Internetkonten“, beenden Sie Windows Mail und starten Sie erneut, so dass die Einstellungen korrekt übernommen werden.

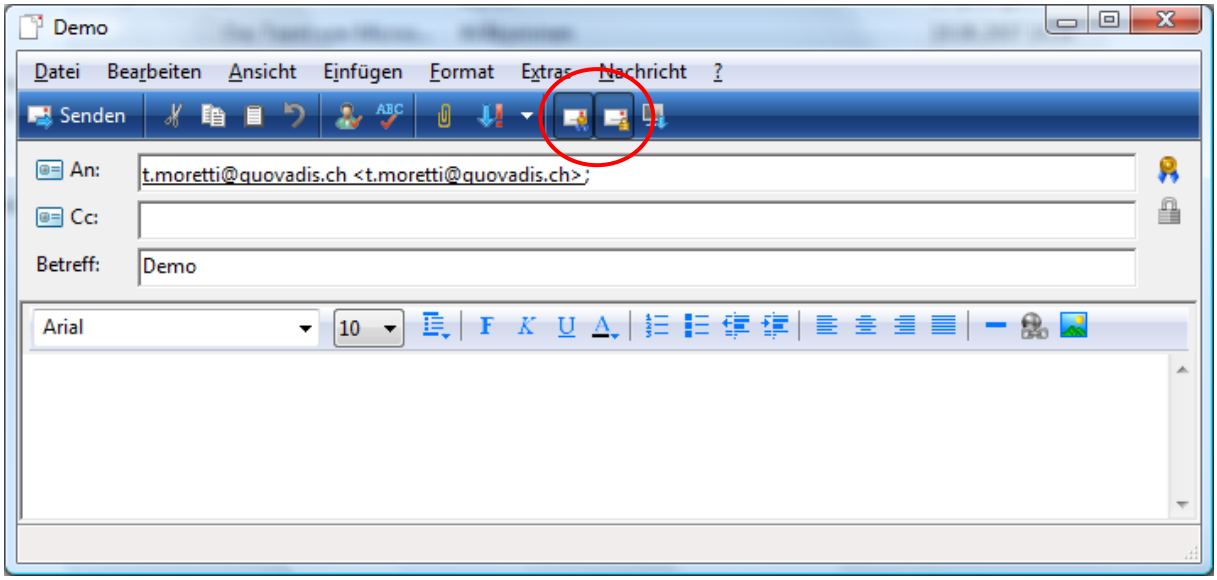
Hinweis
Falls Sie Ihre Nachrichten immer digital signieren oder grundsätzlich Mails verschlüsselt versenden möchten (vorausgesetzt die Empfänger besitzen alle ein Zertifikat), können Sie die Voreinstellungen unter den Optionen, Register Sicherheit wählen:

☑ Alle ausgehenden Nachrichten und Anlagen verschlüsseln
☑ Alle ausgehenden Nachrichten digital signieren

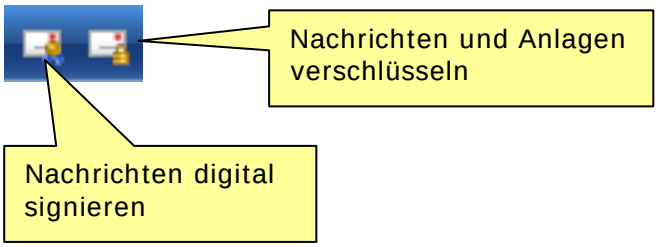

Optionen
Allgemein
Lesen
Bestätigungen
Senden
Verfassen
Signaturen
Rechtschreibung
Sicherheit
Verbindung
Erweitert
Virenschutz
Wählen Sie die zu verwendende Internet Explorer-Sicherheitszone aus:
Internetzone (zweckmäßiger, aber weniger sicher)
Zone für eingeschränkte Sites (sicherer)
Warnen, wenn Anwendungen meine E-Mail-Adresse verwenden
Speichern oder Öffnen von Anlagen, die möglicherweise einen Virus enthalten könnten, nicht zulassen
Bilder herunterladen
Bilder und andere externe Inhalte in HTML-E-Mail blockieren
Sichere E-Mail
Digitale IDs (auch Zertifikate genannt) sind spezielle Dokumente, die es ermöglichen, Ihre Identität bei
Digitale IDs...
Voreinstellungen für sicheren e-Mail-Verkehr
Digitale ID anfordern...
Alle ausgehenden Nachrichten und Anlagen verschlüsseln
Alle ausgehenden Nachrichten digital signieren
Erweitert...
OK
Abbrechen
Übernehmen

Verfassen eines e-Mails

Öffnen Sie eine neue Nachricht in Windows Mail:



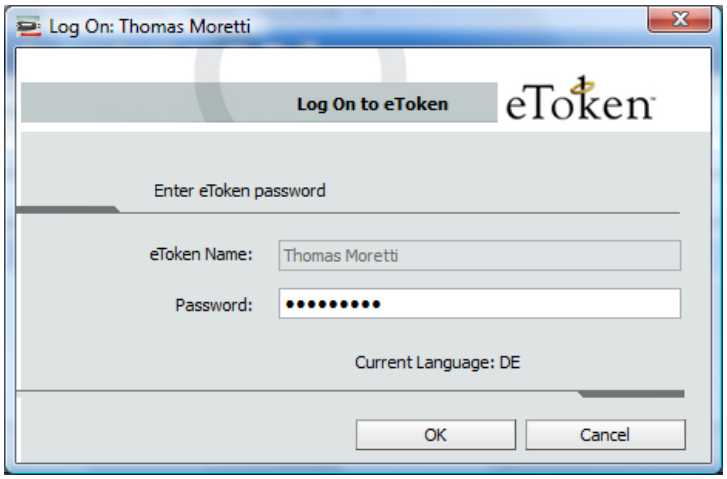
Es sind zwei neue Schaltflächen in der Symbolleiste sichtbar:



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 Zertifikat auch in den Windows Mail Kontakten, im Register IDs der Kontakteigenschaftn, importieren. Der Import entfällt, wenn Sie ein signiertes Mail erhalten. Dabei wird der Kontakt inklusive Zertifikat abgelegt und steht für künftige Mails zur Verfügung.

Beim Versenden der fertigen Nachricht werden Sie, vorausgesetzt Sie möchten Ihre Nachricht signieren, aufgefordert den PIN einzugeben (Dies ist ein Beispieldialog und muss nicht so aussehen. Der Dialog ist abhängig von der eingesetzten Client-Software):



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

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.

Beim Öffnen oder in der Voransicht des e-Mails zeigt Ihnen Windows Mail standardmässig den folgenden Hinweis an:

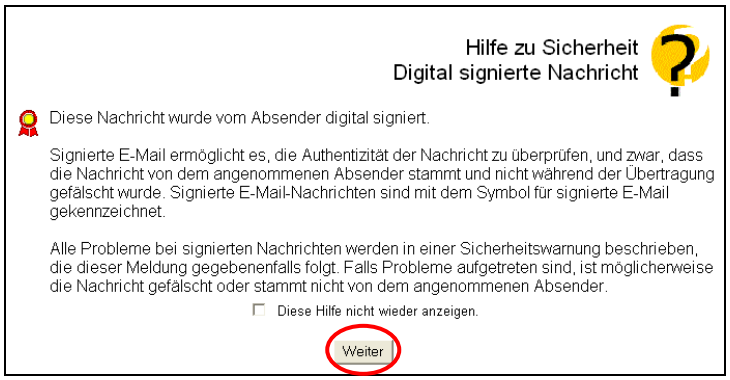


Abbildung 1 - signierte Nachricht

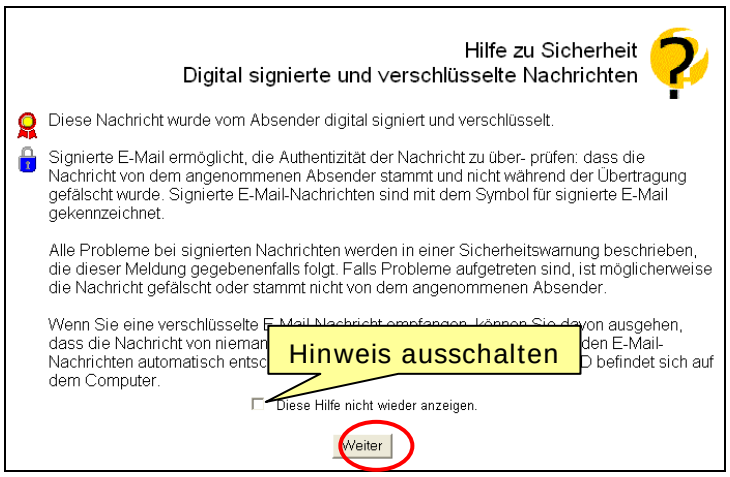
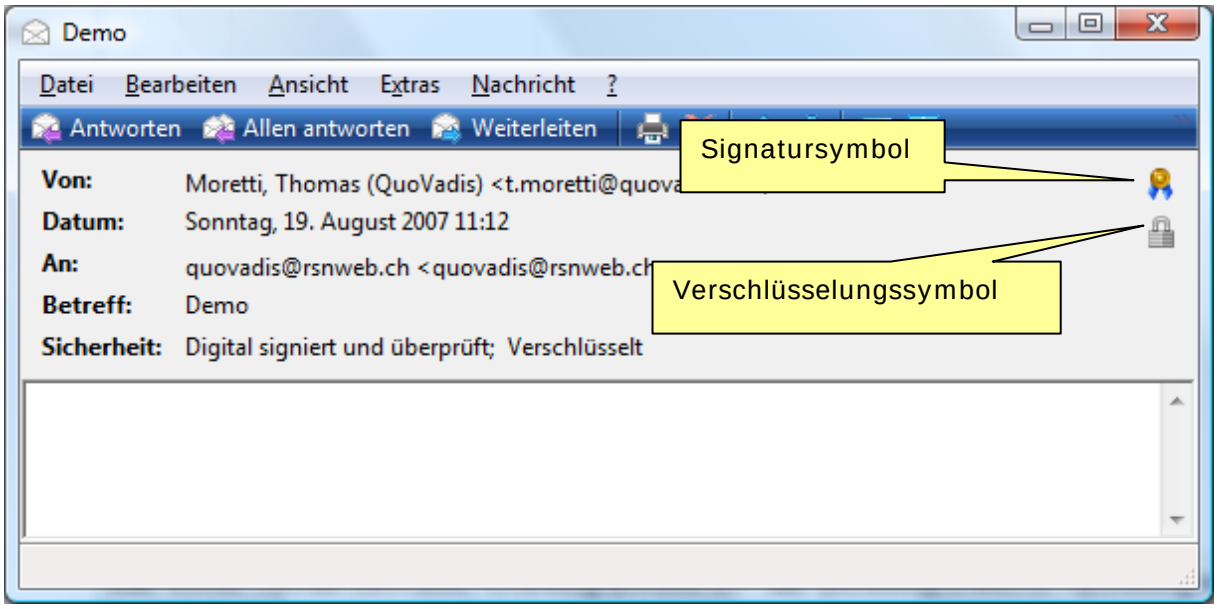


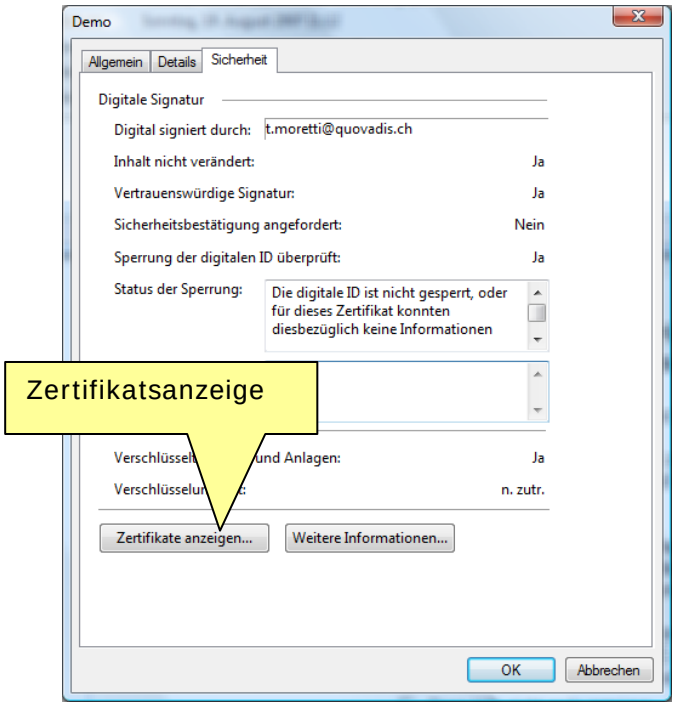
Abbildung 2 - signierte und verschlüsselte Nachricht

Klicken Sie auf die Schaltfläche „Weiter“. Sie können diesen Hinweis ausblenden, wenn Sie die Auswahl aktivieren und danach „Weiter“ wählen.

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 das Signatursymbol. Gehen Sie analog vor, wenn Sie die Verschlüsselung überprüfen möchten. Windows Mail prüft anhand der Sperrliste, die im Hintergrund herunter geladen wird, ob das Zertifikat, mit welchem die Nachricht signiert wurde, gültig ist:



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

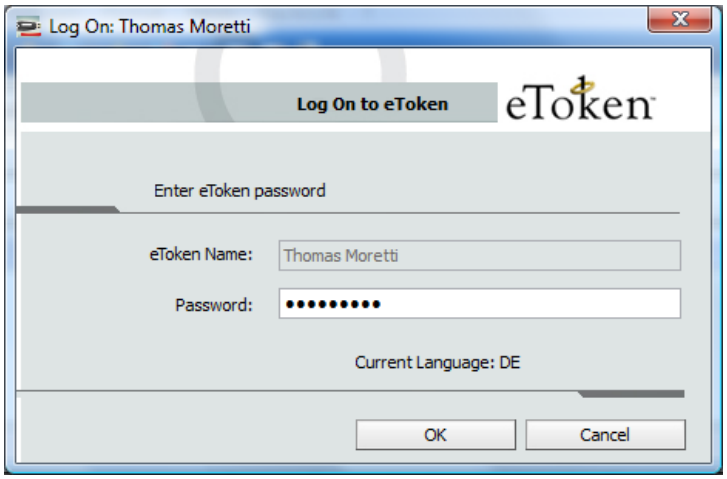
Achtung!
Nachrichten, die im HTML oder im Rich-Text (ohne so genanntes Encoding) Format übermittelt werden, können ungewollt verändert werden. Das heisst, dass der Empfänger eine Problemmeldung angezeigt erhält, obwohl an der Nachricht als solches nichts verändert wurde, jedoch an der Formatierung.

Nachrichten, die als reiner Text (Plain-Text) übermittelt werden, funktionieren erfahrungsgemäss ohne Probleme. Nachteilig ist dabei aber die fehlende Formatierung. Alternativ kann das Microsoft Rich-Text Format (jedoch mit Encoding) genutzt werden. Dabei sollten ebenfalls keine Probleme auftauchen.

Lesen eines verschlüsselten e-Mails

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 der eingesteckten Smartcard oder des USB Tokens mit dem entsprechenden privaten Schlüssel dazu.

Windows Mail prüft nun durch Aufforderung der PIN-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.

Die Überprüfung der Verschlüsselung wurde bereits zuvor beschrieben.