Aktivierung der digitalen Signatur in Outlook 2003

Version 1.0
30. November 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

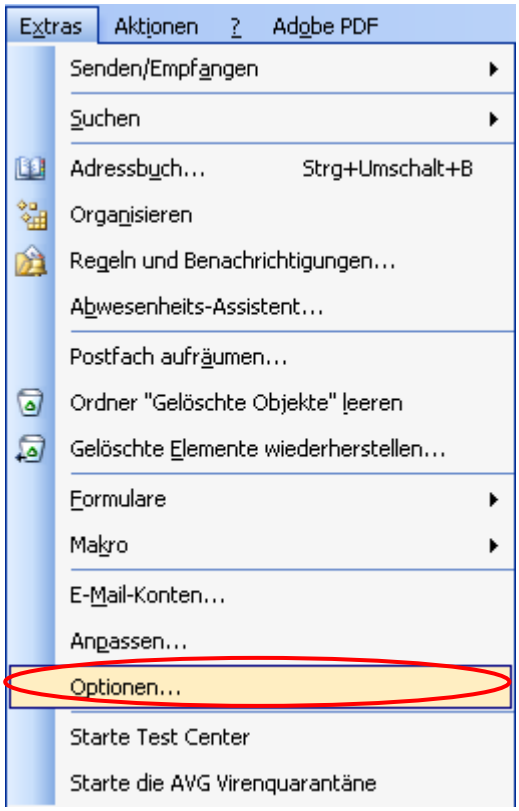
Voraussetzung

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

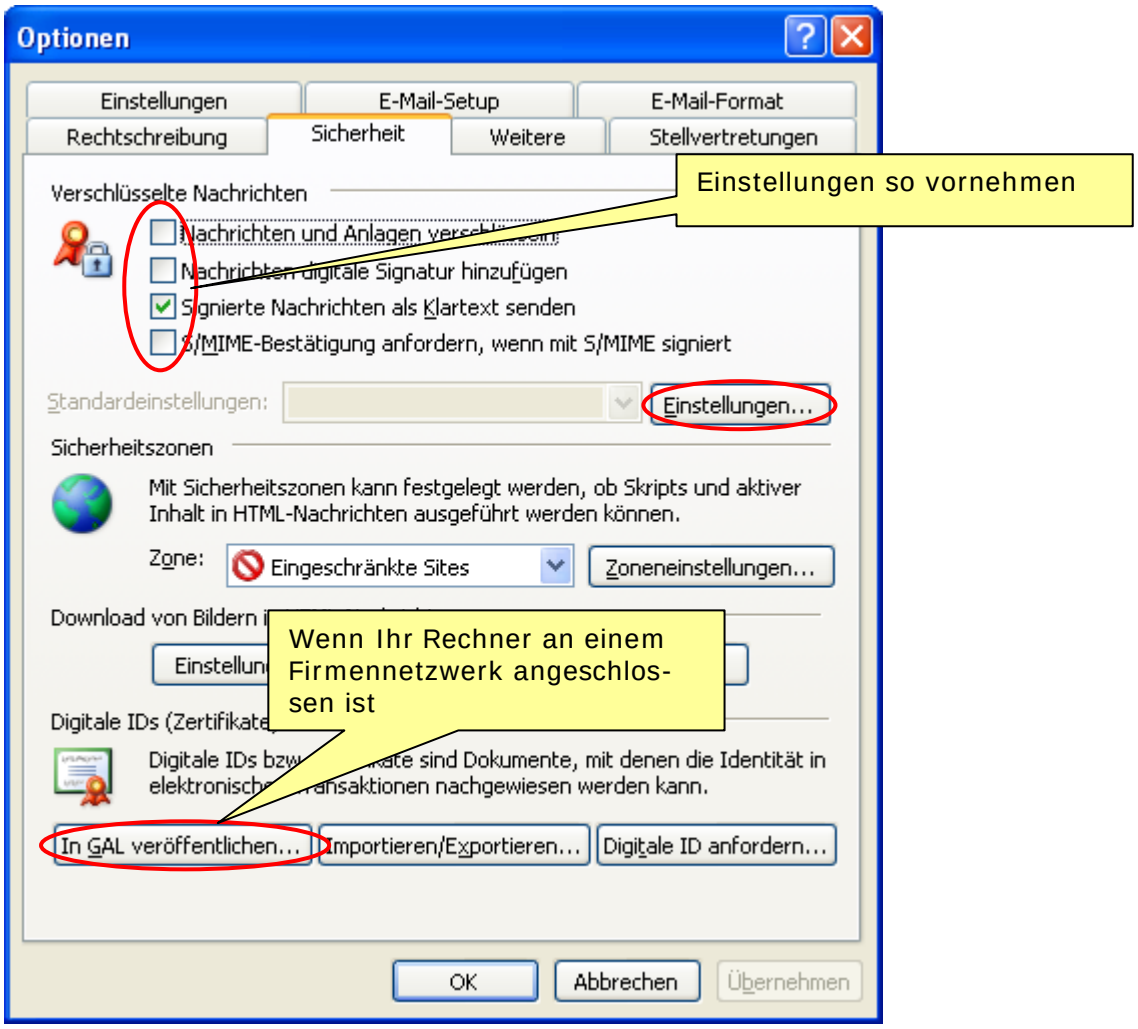
Stellen Sie sicher, dass sich die Smartcard im Smartcard-Leser befindet und dieser respektive der USB Token korrekt angeschlossen ist.

Einrichten

Rufen Sie die Optionen in Outlook auf:



Anschliessend wechseln Sie auf das Register „Sicherheit“:

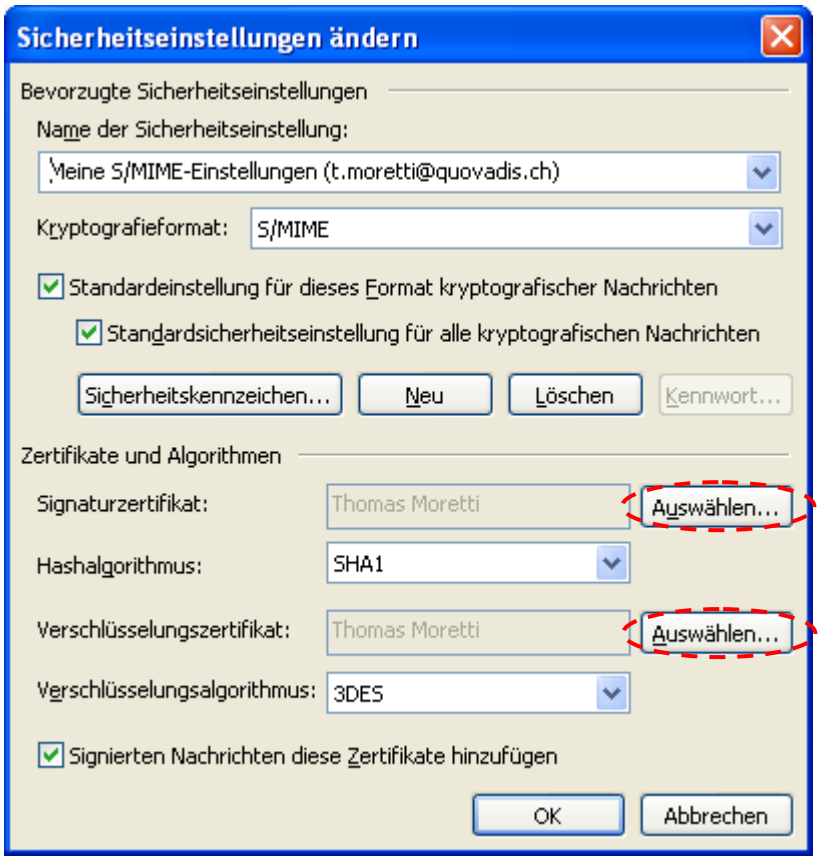


Stellen Sie sicher, dass die Einstellungen unter „Verschlüsselte Nachrichten“ wie markiert aktiviert sind. Daraufhin klicken Sie auf die Schaltfläche „Einstellungen…“

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 entsprechend wählen:

☑ Nachrichten und Anlagen verschlüsseln
☑ Nachrichten digitale Signatur hinzufügen

Outlook prüft, ob ein gültiges Zertifikat für die aktuelle e-Mail-Adresse vorhanden ist. Ist dies der Fall wird der folgende Dialog automatisch ausgefüllt:



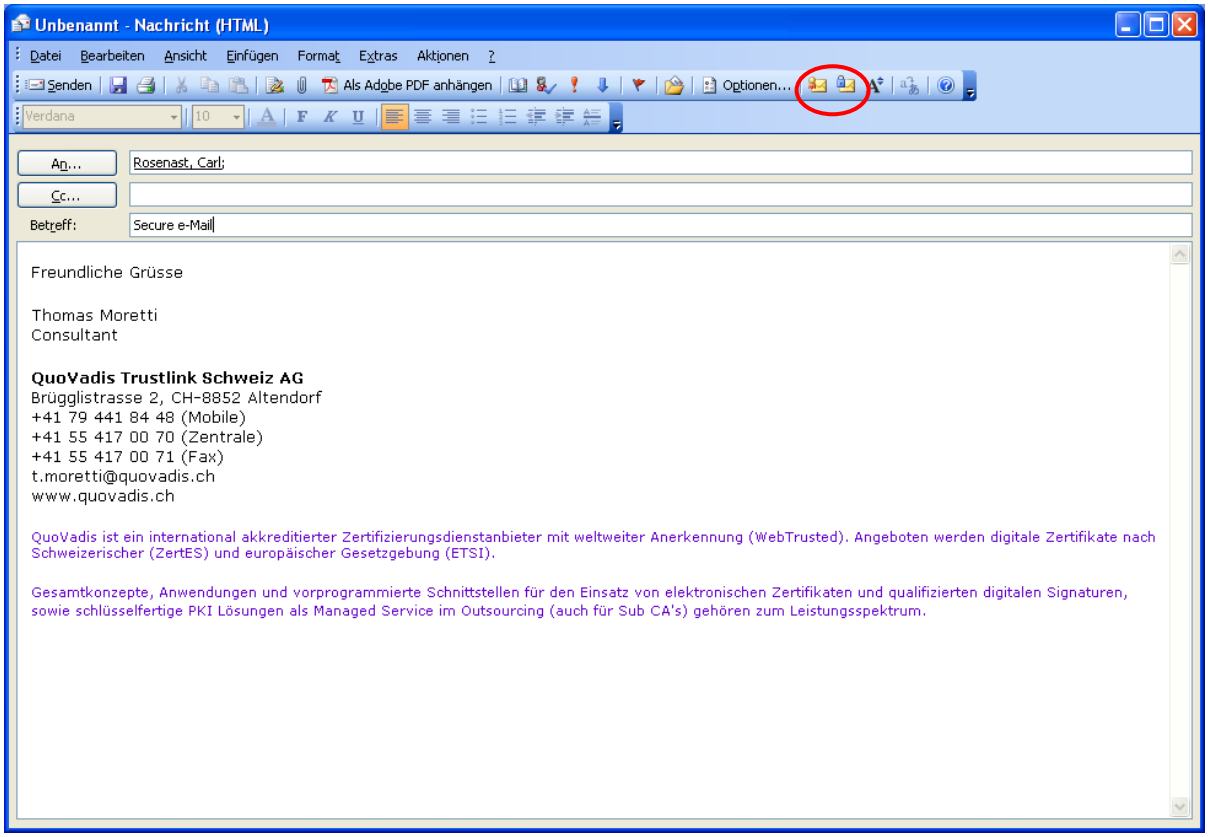
Wäre dies nicht der Fall kann das Zertifikat auch einzeln für die Signatur als auch für die Verschlüsselung über die Schaltflächen „Auswählen…“ selektiert werden.

Stellen Sie sicher, dass die Einstellungen wie oben aktiviert wurden und bestätigen Sie den Dialog mit Klicken auf die Schaltfläche „OK“.

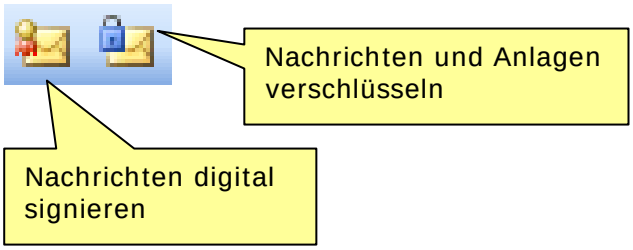
Hinweis
Falls sich Ihr Rechner in einem Firmennetzwerk befindet klicken Sie auf dem vorangegangenen Dialog auf die Schaltfläche „In GAL veröffentlichen…“ (GAL = Global Address List – globale Adressliste). Damit wird das Zertifikat in das Active Directory übertragen und jeder Benutzer kann Ihnen verschlüsselte Nachrichten senden.

Verfassen eines e-Mails

Öffnen Sie eine neue Nachricht in Outlook:



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 Outlook Kontakten, im Register Zertifikate, importieren.

Wird eine e-Mail-Adresse unter „An“, „CC“ oder „BCC“ ausgewählt, können diese aus dem GAL (Globale Adressliste – falls die Veröffentlichung bei der Aktivierung der Signatur in Outlook vorgenommen wurde) oder aus den eigenen Kontakten selektiert werden. Wurde da ein Zertifikat hinterlegt, wird dieses für die Verschlüsselung verwendet.

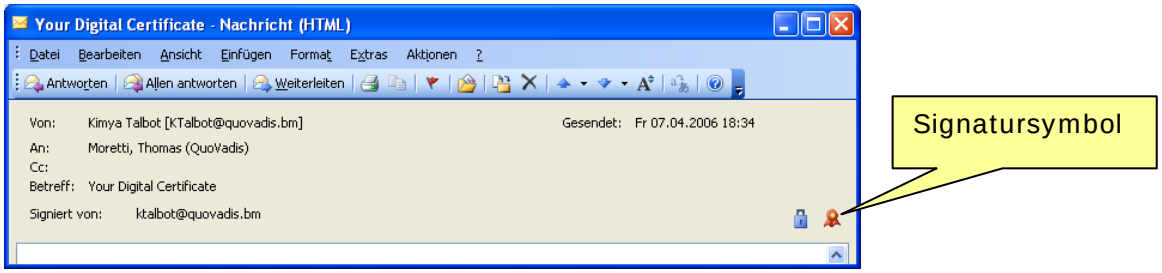
Beim Versenden der fertigen Nachricht werden Sie, vorausgesetzt Sie möchten Ihre Nachricht signieren, aufgefordert den PIN einzugeben (Dies ist ein Beispieldialog und muss nicht so aussehen. Der Dialog ist abhängig von der eingesetzten Client-Software):

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

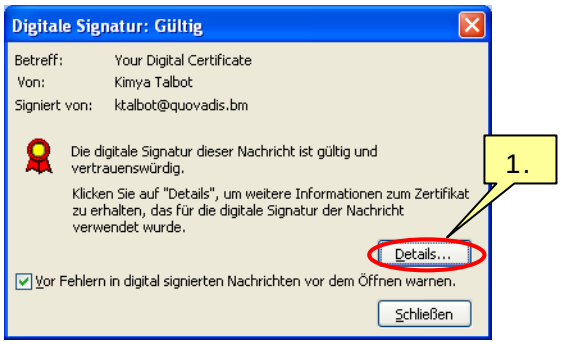
Prüfen einer e-Mail-Signatur

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

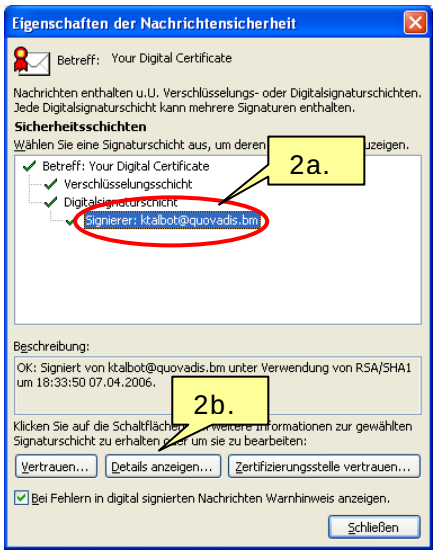
Klicken Sie hierzu auf das rote Signatursymbol, das bei einer geöffneten Nachricht am rechten oberen Rand erscheint:



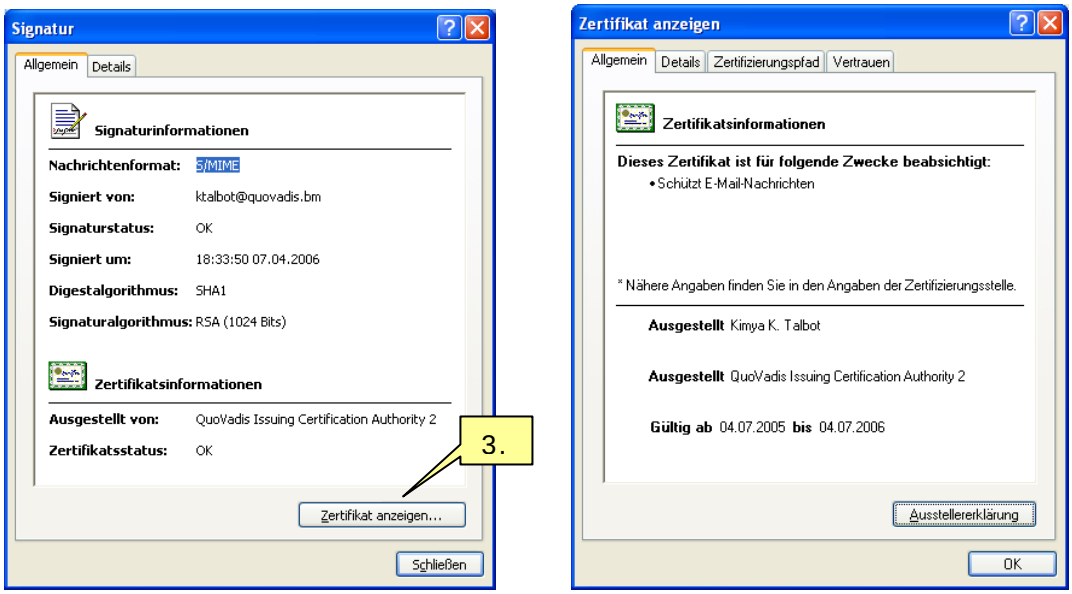
Outlook prüft anhand der Sperrliste, die im Hintergrund herunter geladen wird, ob das Zertifikat, mit welchem die Nachricht signiert wurde, gültig ist:



Details über die Signatur erhalten Sie über die Schaltfläche „Details…“.

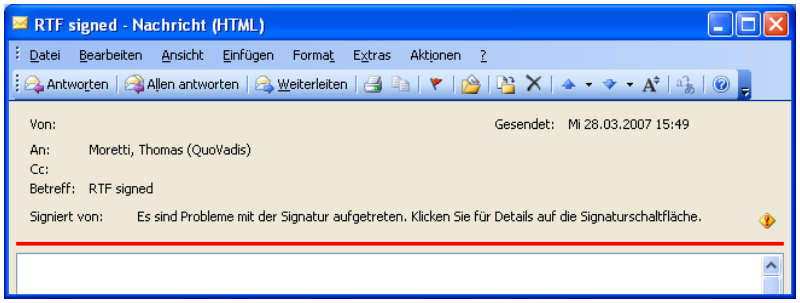


Das benutzte Zertifikat ist ersichtlich, wenn Sie auf die Schaltfläche „Zertifikat anzeigen…“ klicken.



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

Wurde eine Nachricht mit einem ungültigen Zertifikat signiert oder die Nachricht während der Übermittlung verändert erscheint beim Öffnen des e-Mails ein roter Balken:



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.

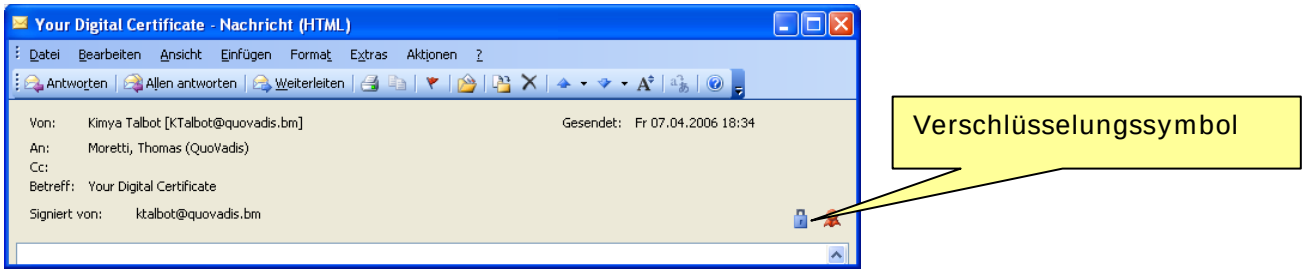
Prüfen eines verschlüsselten e-Mails

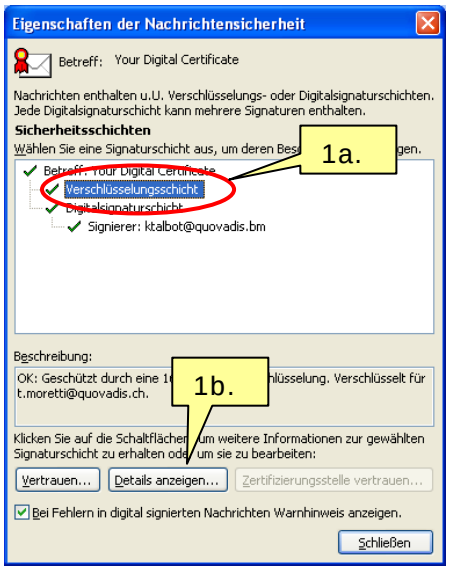
Wenn Sie eine verschlüsselte Nachricht erhalten hat der Absender Ihren öffentlichen Schlüssel dafür benutzt die Nachricht zu chiffrieren. Möchten Sie diese Nachricht öffnen bedarf es der eingesteckten Smartcard oder des USB Tokens mit dem entsprechenden privaten Schlüssel dazu.

Outlook prüft nun durch Aufforderung der PIN-Eingabe, ob Sie zum Lesen der Nachricht berechtigt sind:

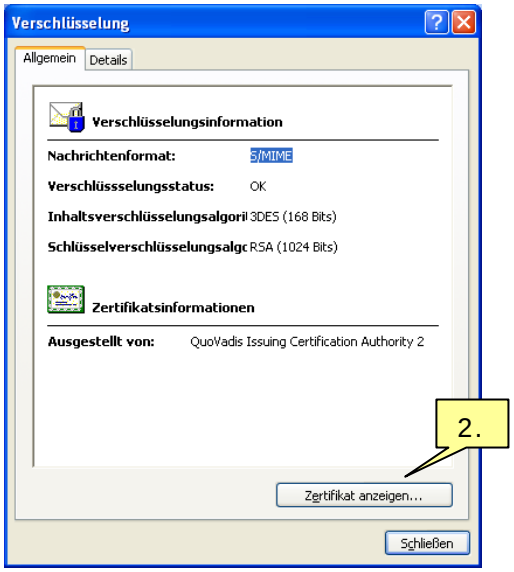
Hinweis
Fehlt Ihnen aufgrund eines Verlustes der zugehörige private Schlüssel auf einem USB Token oder der Smartcard lässt sich die Nachricht nicht mehr öffnen.

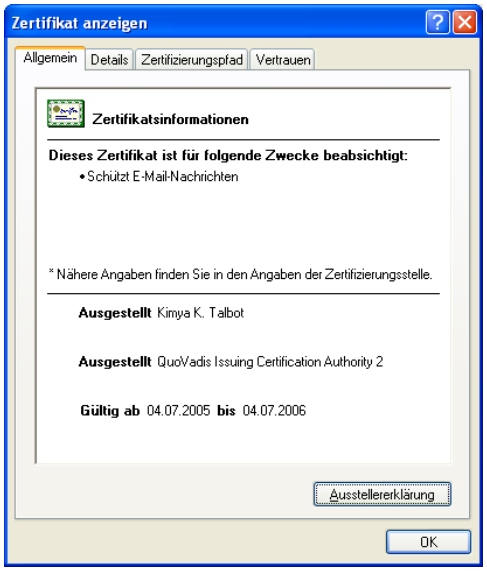
Zur Überprüfung der Verschlüsselung klicken Sie auf das blaue Verschlüsselungssymbol, das bei einer geöffneten Nachricht am rechten oberen Rand erscheint:





Das benutzte Zertifikat ist ersichtlich, wenn Sie auf die Schaltfläche „Zertifikat anzeigen…“ klicken.

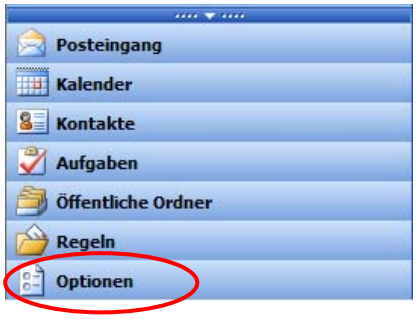




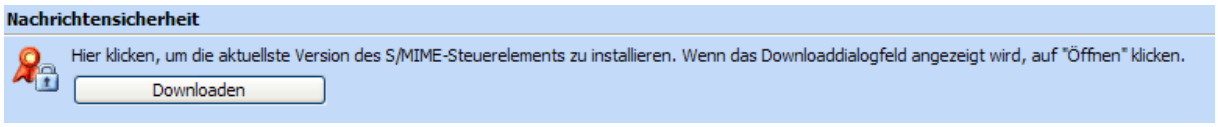
Nutzung der Signatur unter Outlook Web Access

Falls Sie neben dem gewöhnlichen Microsoft Outlook auch Outlook Web Access einsetzen, können Sie auch da die Signatur aktivieren, sofern Sie mindestens mit Microsoft Exchange 2003 oder höher arbeiten.

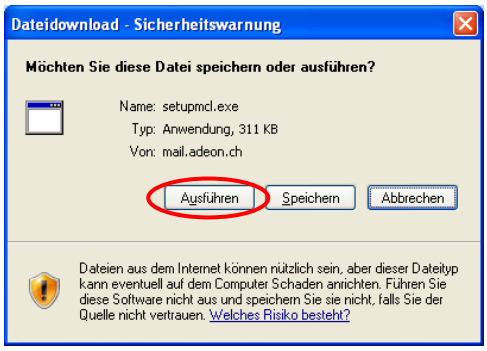
Wechseln Sie in die Optionen von Outlook Web Access, nachdem Sie sich angemeldet haben:

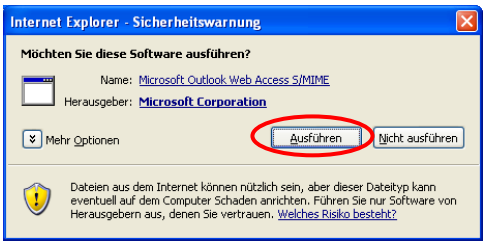


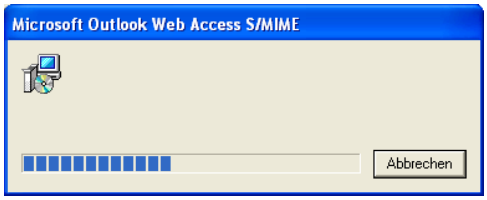
Suchen Sie in den Optionen den Abschnitt Nachrichtensicherheit und laden Sie sich das S/MIME Steuerelement herunter und installieren Sie es.



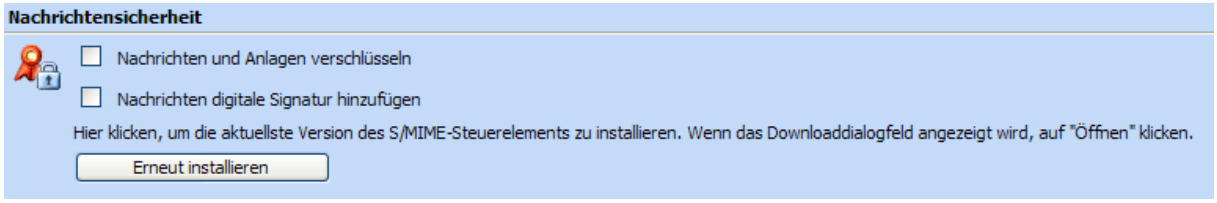
Führen Sie den Setup mittels „Ausführen“ aus:



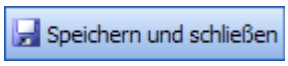




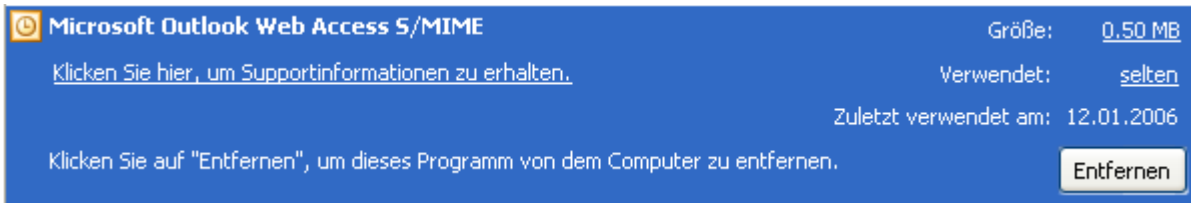
Nachdem die Komponente installiert wurde erscheint der Abschnitt wie folgt:



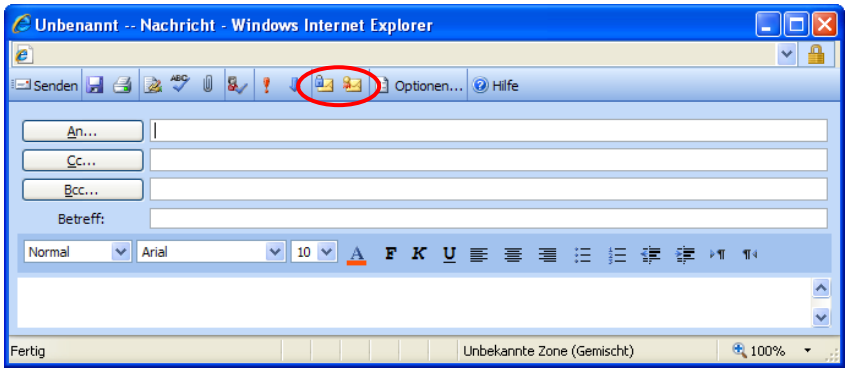
Speichern Sie die Einstellungen mit der folgenden Schaltfläche im oberen Bereich der Einstellungen.



Unter Software (in der Systemsteuerung) ist diese Komponente wie folgt ersichtlich:



Wenn Sie nun eine neue Nachricht öffnen sind die beiden bereits vorgestellten Schaltflächen auch hier ersichtlich:



Sie können gleich vorgehen wie beim installierten Outlook 2003.