

Elektronische Unterschriften mit Adobe Acrobat 8

Version 1.0
7. Mai 2007

QuoVadis Trustlink Schweiz AG
Brügglistrasse 2
CH-8852 Altendorf

Phone +41 55 417 00 70
Fax +41 55 417 00 71
www.quovadis.ch

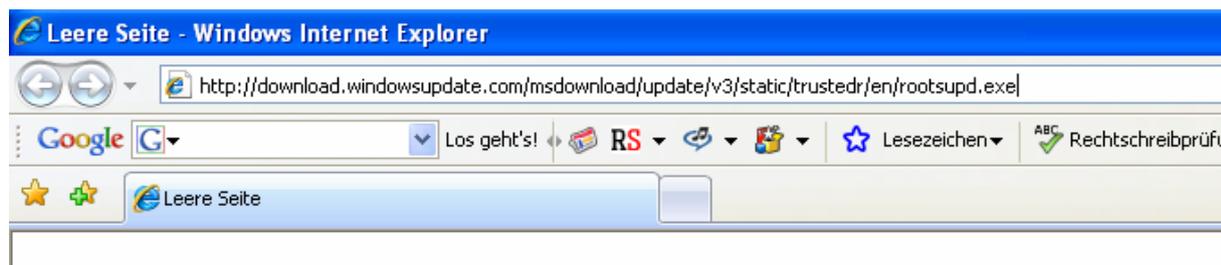
Einleitung

Diese Anleitung beschreibt in Kurzform wie mit Adobe Acrobat 8 (Standard oder Professional) PDF Dokumente signiert oder zertifiziert respektive die Signatur(en) geprüft werden können.

Voraussetzungen

Aktualisierung der Stammzertifikate

Eines der Ursachen, weshalb eine Signatur unbekannt oder gar ungültig angezeigt wird, ist die fehlende Aktualisierung der Stammzertifikate. Um die manuell nachzuholen kann über Microsoft ein kleines Programm heruntergeladen werden, das die Stammzertifikate, die von Microsoft unterstützt werden, auf dem lokalen Windows® Rechner aktualisiert.



Der Link lautet:

<http://download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/rootupd.exe>

Anschliessend erscheint folgender Dialog, denn Sie mit „Ausführen“ bestätigen.



Der anschliessende Sicherheitshinweis kann ebenfalls mit „Ausführen“ beantwortet werden:



Die Ausführung des Programms wird nicht explizit quittiert.

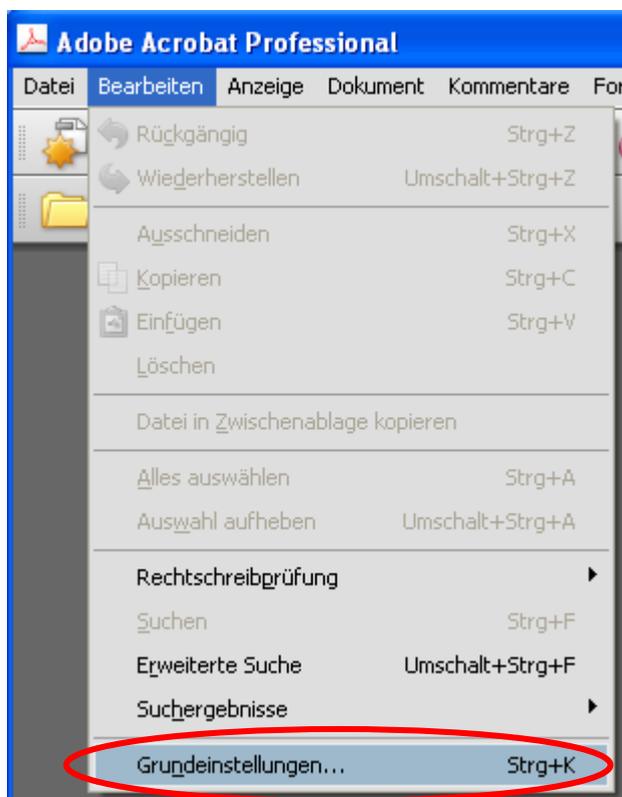
Einstellungen in Adobe Acrobat 8

Adobe Acrobat 8 wird standardmässig so installiert, dass Zertifikate, die im Windows-Speicher abgelegt sind, nicht berücksichtigt werden.

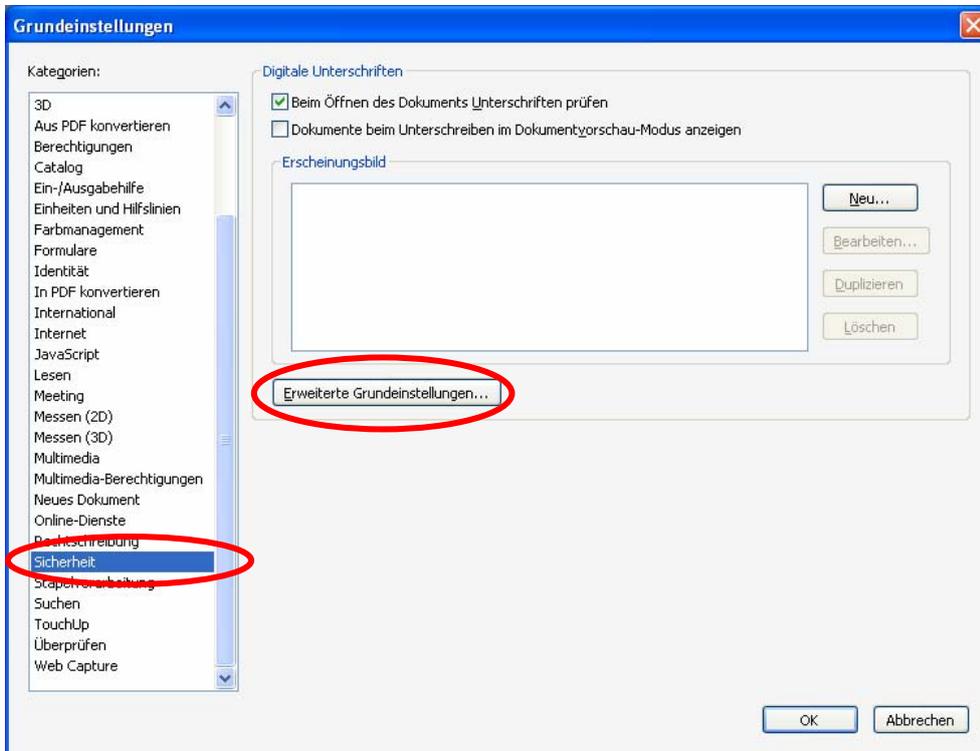
Anstelle des Imports jedes einzelnen vertrauenswürdigen Stammzertifikates muss Adobe Acrobat 8 so eingestellt werden, dass auch Windows-Zertifikate berücksichtigt werden.

Des Weiteren müssen noch wenige weitere Einstellungen angepasst werden. Gehen Sie nun wie folgt vor:

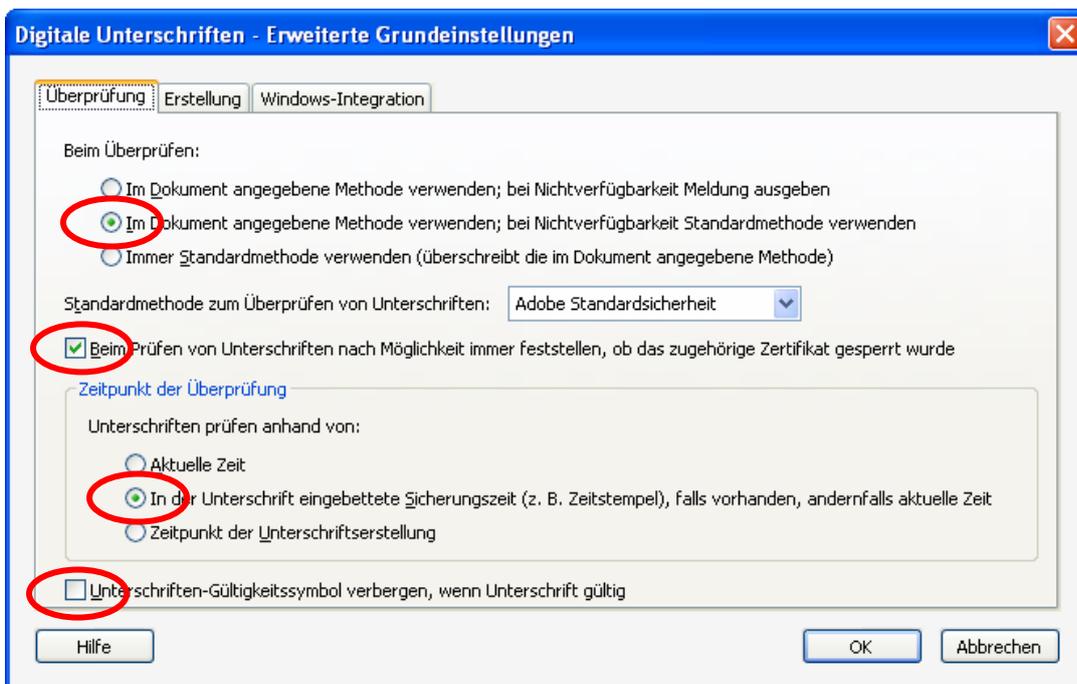
Rufen Sie das Menü **Bearbeiten | Grundeinstellungen...** auf:



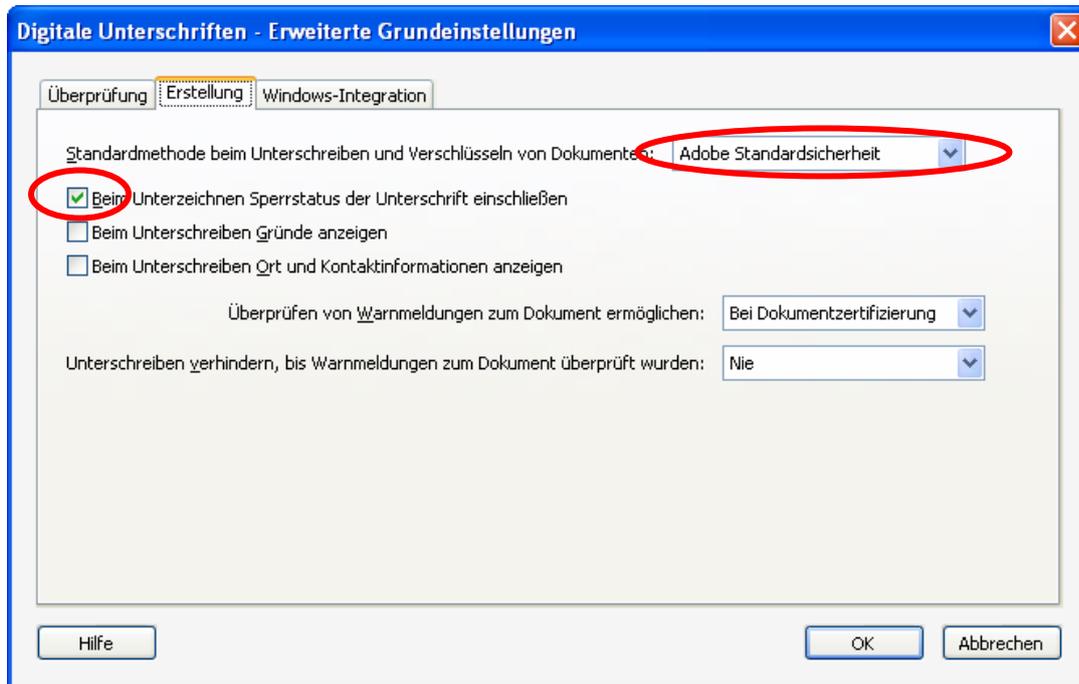
Sie erhalten folgenden Dialog zur Ansicht. Wählen in den Grundeinstellungen die Kategorie „Sicherheit“ und klicken Sie dann im rechten Teil auf die Schaltfläche „Erweiterte Sicherheitseinstellungen“.



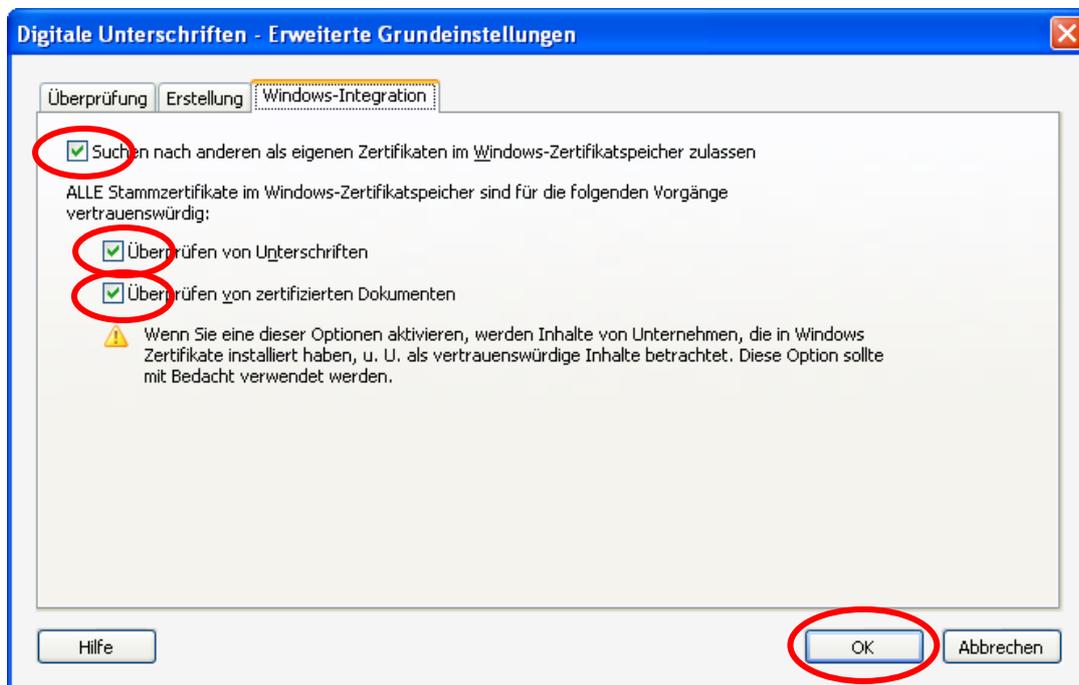
Es erscheint ein Dialog, in dem Sie anschliessend die Einstellungen gemäss den nachfolgenden Abbildungen vornehmen:



Klicken anschliessend auf das Register „Erstellung“



Danach muss noch das Register „Windows-Integration“ aufgerufen werden:



Schliessen die Einstellungen mit „OK“ ab und schliessend daraufhin auch das Fenster mit den Grundeinstellungen.



Hinweis

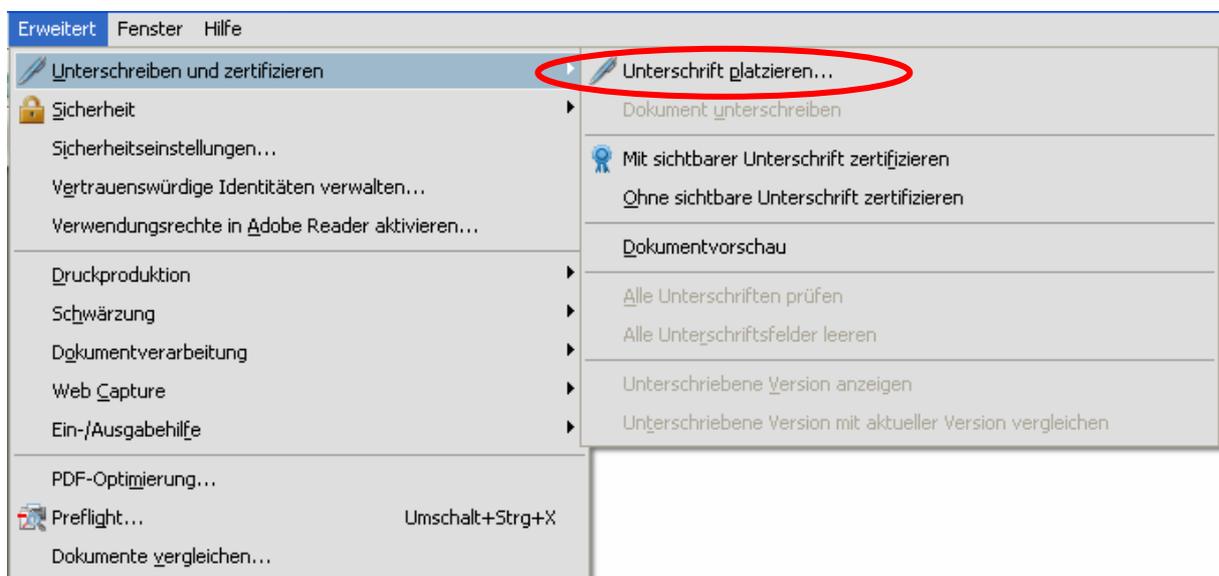
Für die Nutzung des qualifizierten Zeitstempels von QuoVadis bitten wir Sie mit uns Kontakt aufzunehmen.

Anbringen einer Signatur

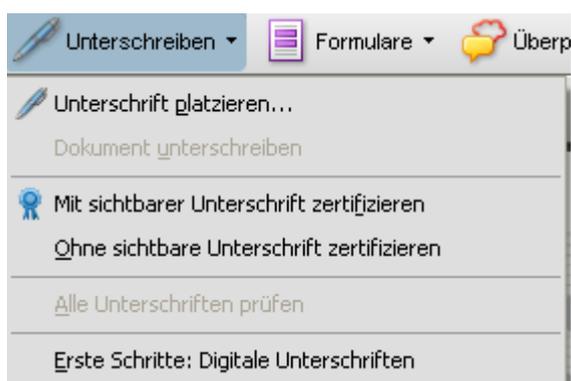
Es gibt zwei Arten Signaturen an PDF Dateien anzubringen: **sichtbar** oder **verdeckt** (unsichtbar).

Sichtbare Signatur

Wählen Sie über das Menü **Erweitert | Unterschreiben und zertifizieren** den Punkt **Unterschrift platzieren...** aus:



Dasselbe erreichen Sie auch über die Symbolleiste:



Nachfolgende Dialoge bestätigen Sie entsprechend Ihren Vorgaben und ziehen anschließend mit dem erscheinenden Fadenkreuz (der Mauszeiger wird damit kurzfristig ersetzt) ein genügend grosses Feld auf das Dokument:

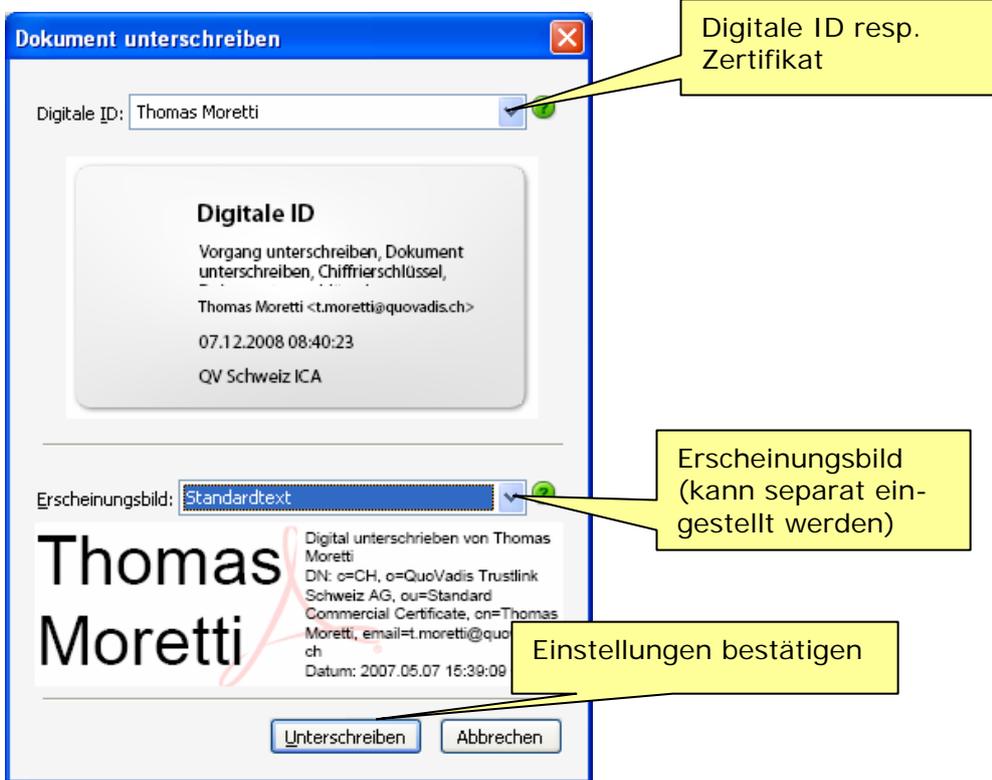
Thema **Signaturprüfung**

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Maecenas congue dapibus ipsum. Sed arcu magna, bibendum in, aliquet ac, adipiscing luctus, lorem. Proin nec nulla non felis adipiscing fringilla. Suspendisse condimentum lacus a metus. Cras eleifend, nisl at dignissim pellentesque, urna, nec rutrum felis leo eu diam. Nulla blandit dui. Nulla facilis elit ut felis. In elementum mi id quam. dolor. Etiam consectetur metus. Sed ante eros, pulv accumsan vel, sapien. Nulla aliquet lacinia ante. Nam commodo id, elementum at, nisl. Pellentesque egesta lectus vitae nulla accumsan fringilla. Phasellus a velit non Sed consectetur fringilla mi. Fusce id lectus a metus he Phasellus malesuada mauris et diam.

genügend grosser Rahmen für die Signatur aufziehen

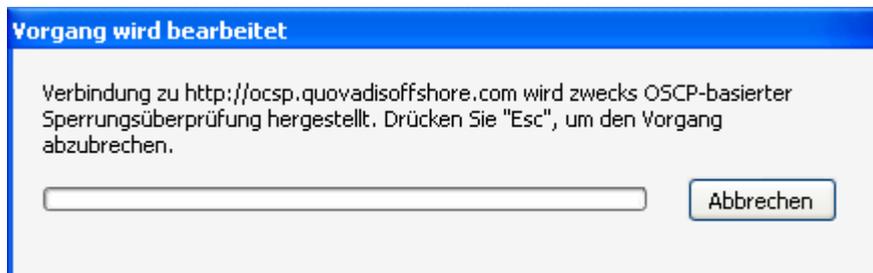


Anschliessend erscheint ein Fenster, in dem Sie die gewünschte digitale ID, also das entsprechende Zertifikat, mit welchem Sie die Unterschrift leisten möchten, auswählen können:

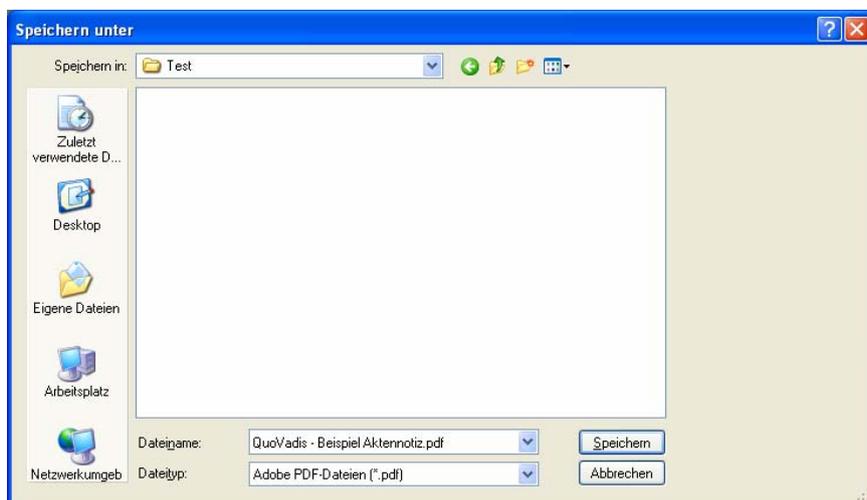


Bestätigen Sie die Auswahl und des Erscheinungsbilds mit Klicks auf die Schaltfläche „Unterschreiben“.

Das Zertifikat wird sogleich über OSCP (Online Certificate Status Protocol) geprüft, ob dieses für eine Signatur verwendet werden darf oder es unter Umständen vorgängig revoziert wurde. Die URL (Internetadresse), worüber dies erfolgen soll, entnimmt Adobe automatisch dem Zertifikat:



Ist das Zertifikat gültig, muss als nächstes die PDF Datei mit der Signatur gespeichert werden.



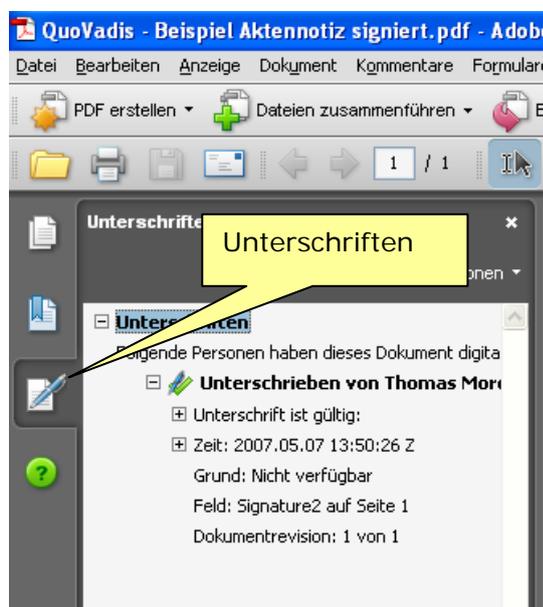
Befindet sich das Zertifikat auf einem USB Token oder einer Smartcard wird jetzt nach dem Passwort respektive PIN gefragt (der Dialog kann je nach eingesetztem Token oder Smartcard ändern):



Die Signatur des Dokuments wird abgeschlossen und erneut überprüft. Ist alles in Ordnung wird die Signatur mit einem grünen Haken angezeigt:



Am rechten Rand wird ersichtlich, dass das Dokument eine Signatur trägt. Klickt man auf das Symbol erhält man nähere Informationen darüber.

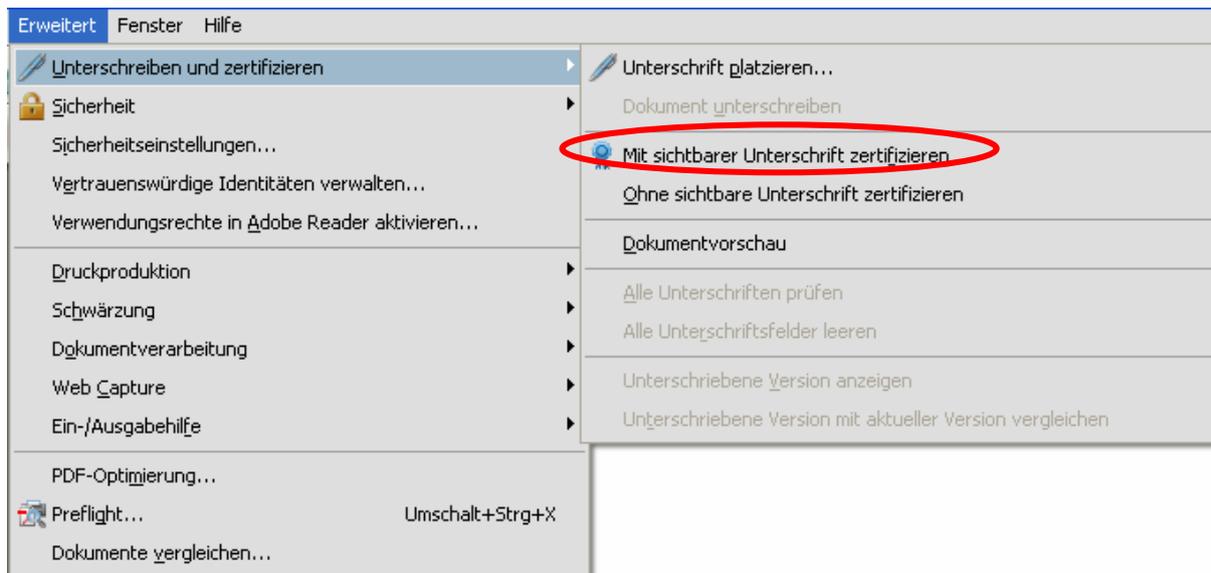


Hinweis

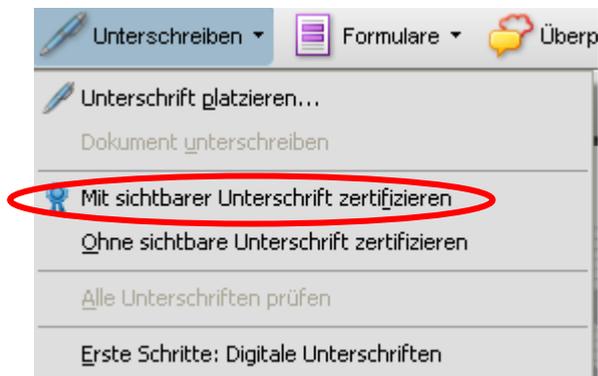
Ein Dokument, kann mehrere Unterschriften erhalten, solange es nicht zertifiziert wurde und darin diese Änderungsmöglichkeit nicht zugelassen wird.

Mit sichtbarer Unterschrift zertifizieren

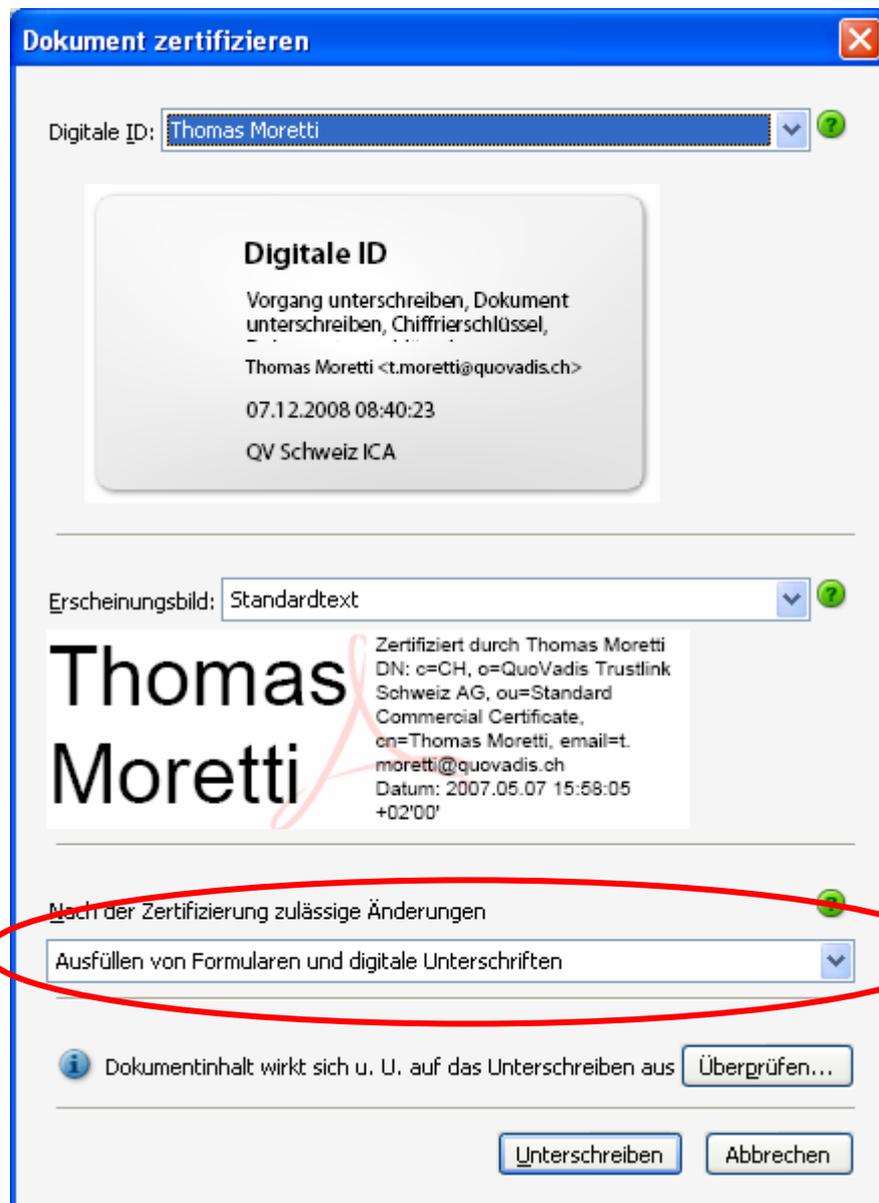
Die Zertifizierung eines Dokuments geht über die reine Unterschrift hinaus. Mit der Unterschrift genehmigen Sie den Inhalt. Die Zertifizierung geht einen Schritt weiter und legt die zulässigen Änderungen fest, die die Zertifizierung nach wie vor gewährleisten.



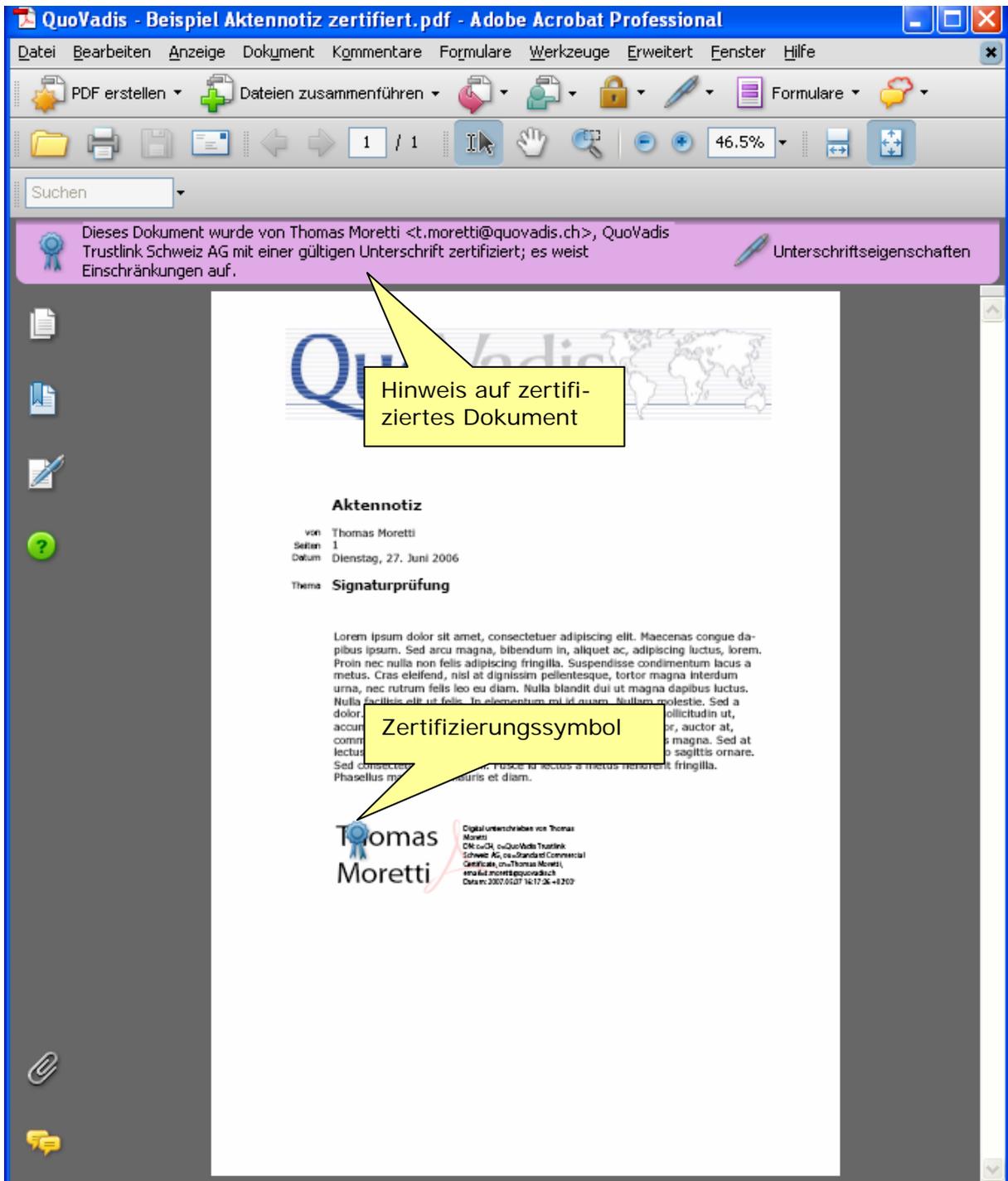
oder



Das Vorgehen ist dasselbe wie bei der Unterschrift, nur dass beim folgenden Dialog die Änderungen festgelegt werden:

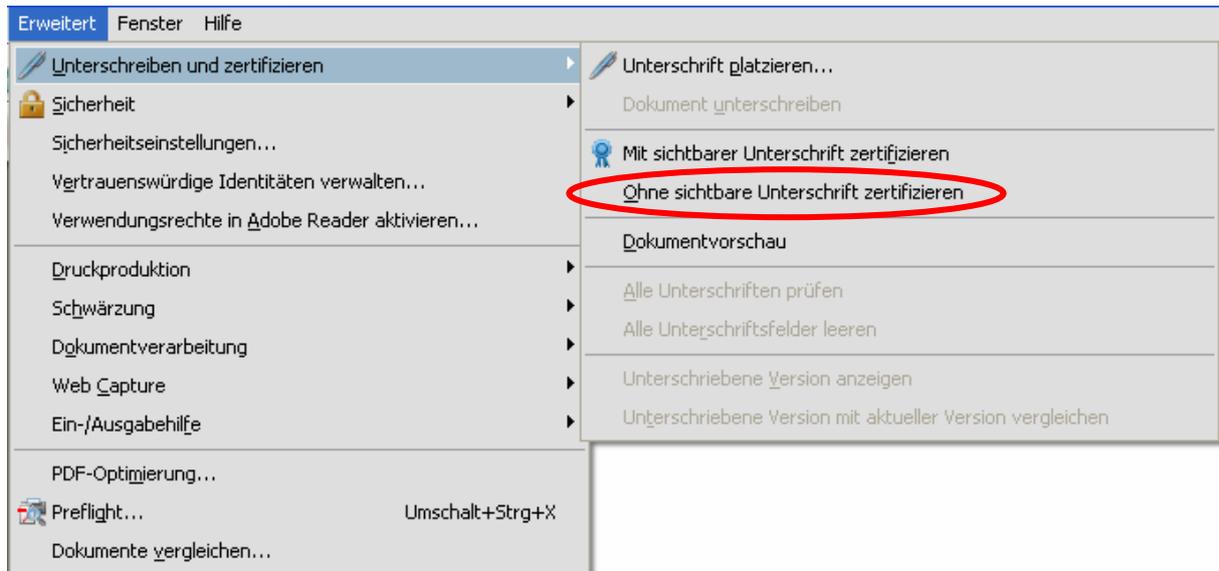


Bei einem zertifizierten Dokument erscheint ein violetter Hinweis im oberen Bereich von Adobe Acrobat. Zudem zeigt sich das Signet bei der Signatur nicht als grüner Haken, sondern als blaues Siegel:

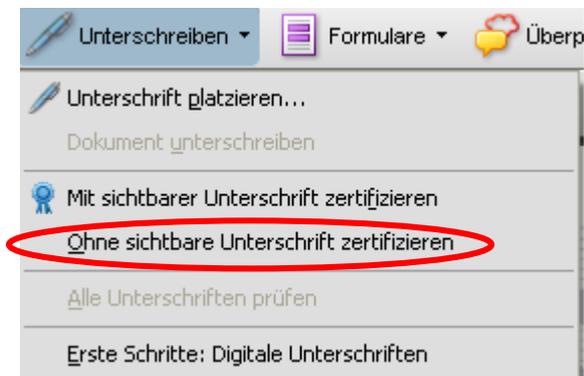


Mit unsichtbarer Unterschrift zertifizieren

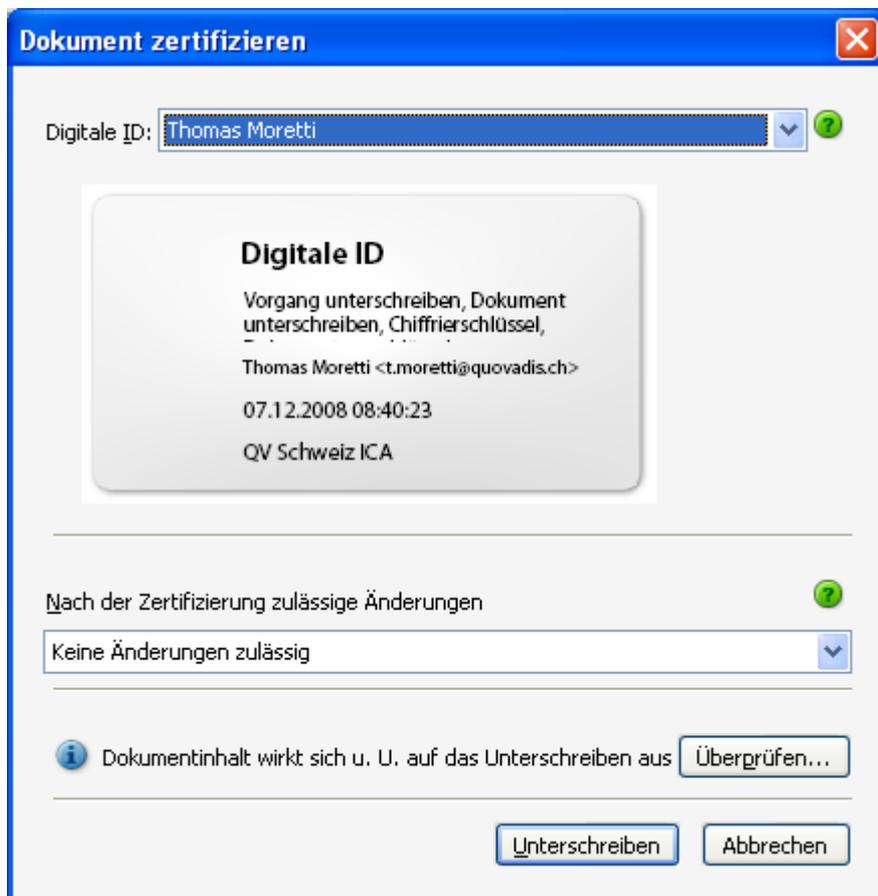
Soll die Unterschrift nicht unmittelbar auf dem Dokument, sondern im Hintergrund angebracht werden, kann dies über diese Auswahl erreicht werden:



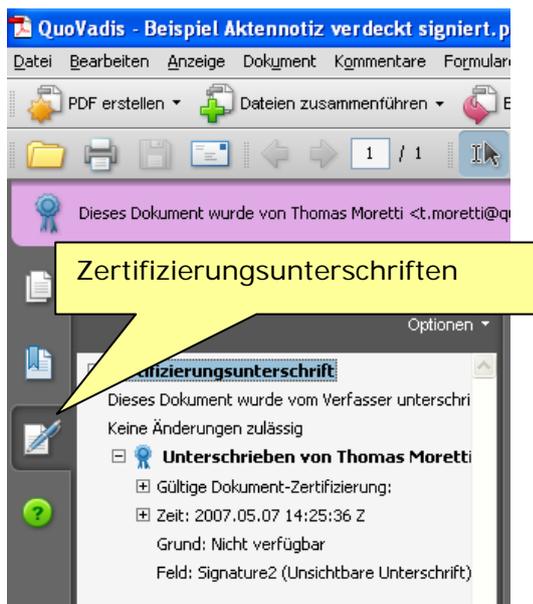
oder



Der Auswahldialog für die digitale ID respektive das Zertifikat sieht in diesem Fall ein wenig anders aus, da das Erscheinungsbild der Unterschrift obsolet wird:

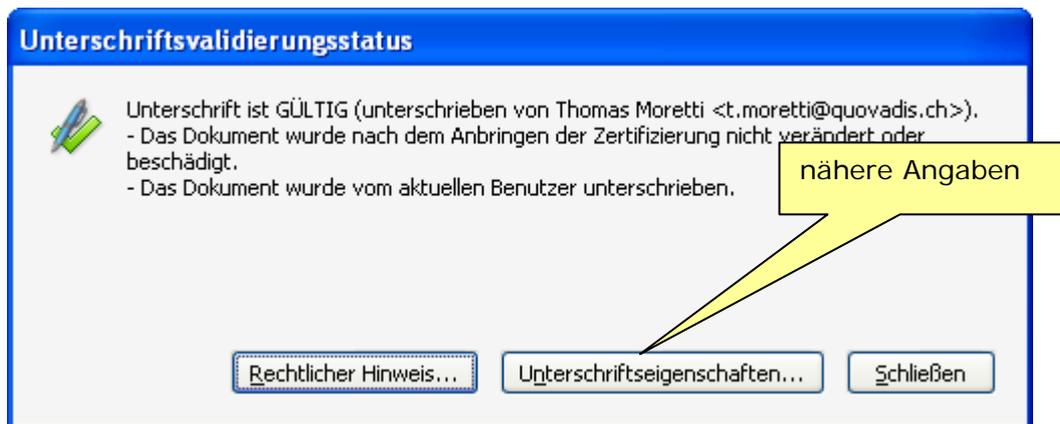


Die Unterschrift wird wiederum auf das entsprechende Symbol am linken Rand sichtbar:

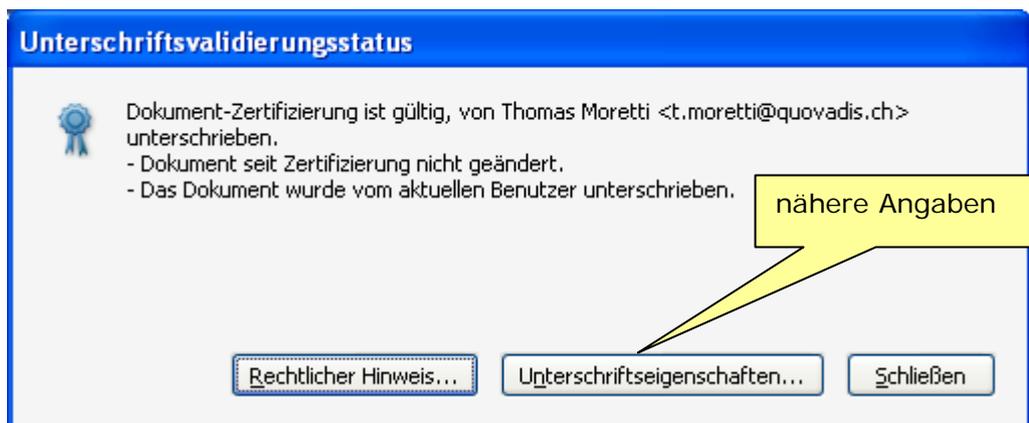


Prüfung einer fortgeschrittenen Signatur

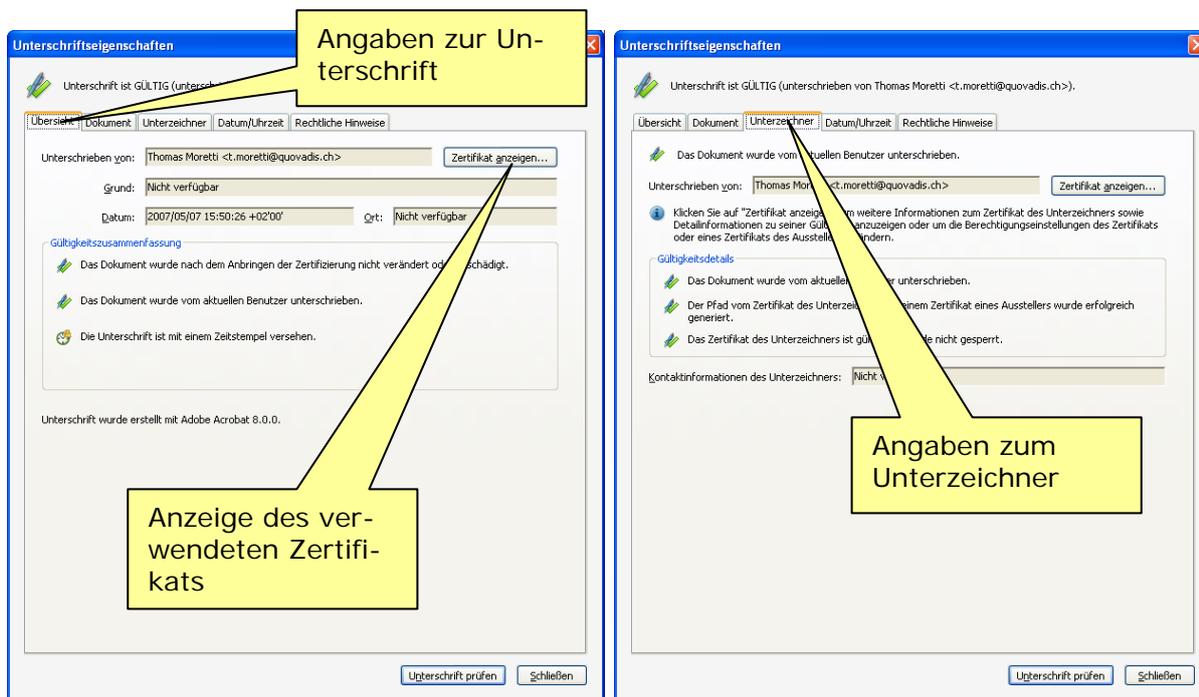
Eine Signatur kann jederzeit mittels Klicken auf die sichtbare Signatur oder durch die Auswahl des Kontextmenüs „Signatur prüfen“ (rechte Maustaste) auf der verdeckten Signatur erreicht werden:



respektive



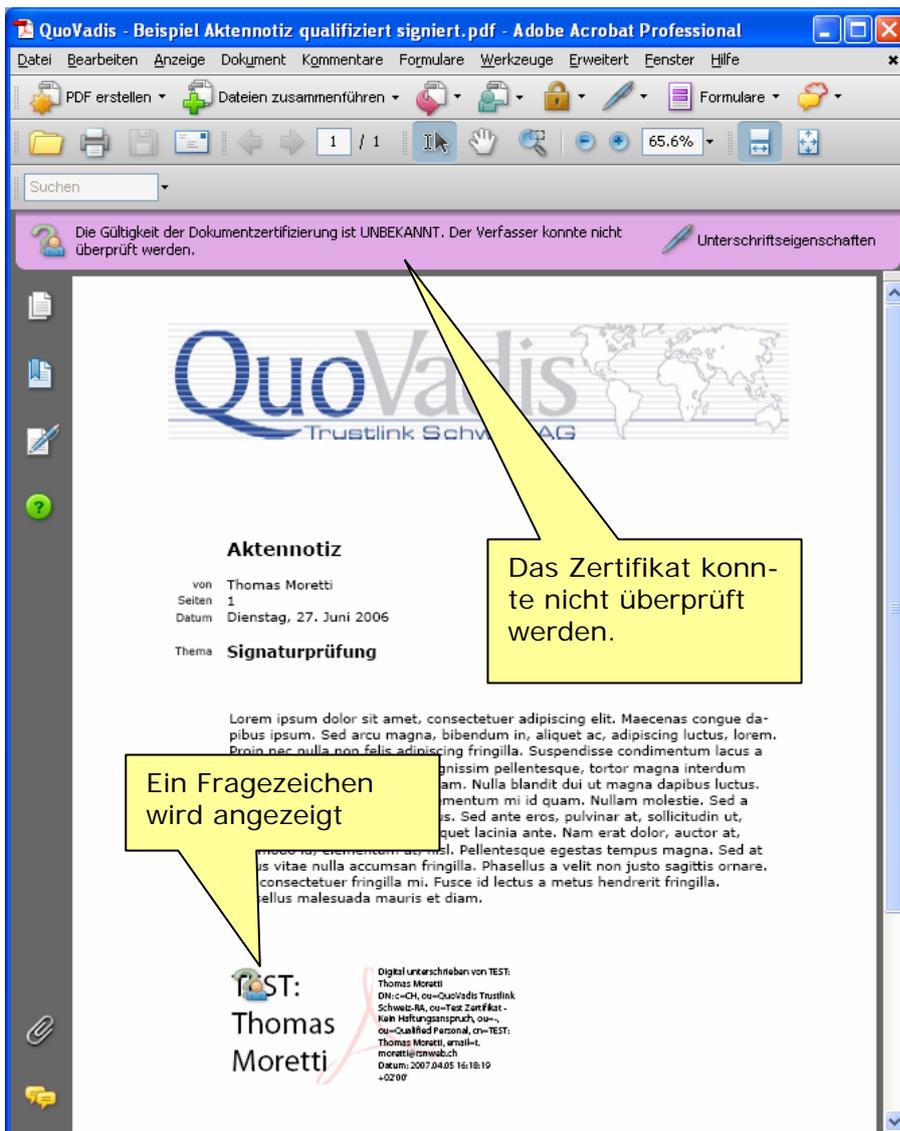
Über die Schaltfläche Unterschriftseigenschaften... erhalten Sie nähere Angaben zur Signatur als auch zum verwendeten Zertifikat selbst:



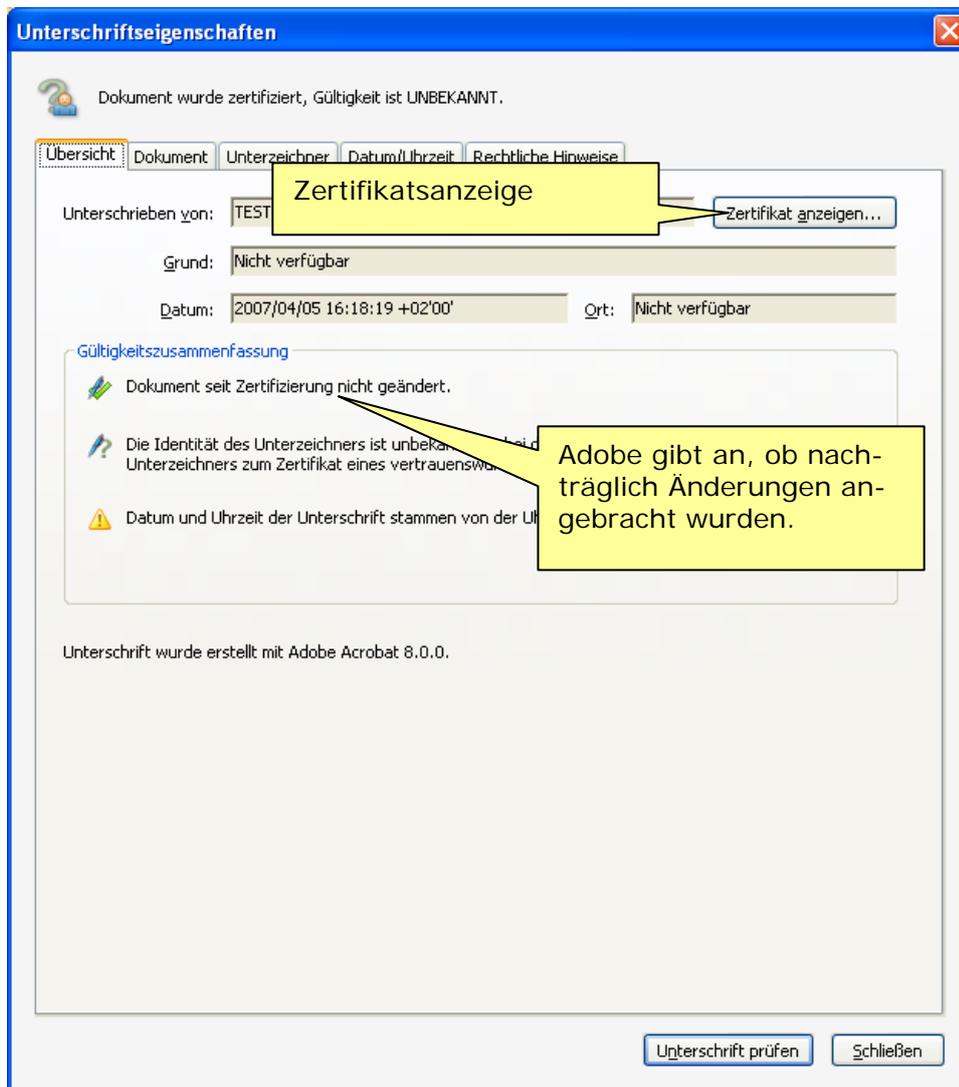
Prüfung einer qualifizierten Signatur

Eine qualifizierte Signatur kann in Adobe Acrobat ohne Zusatzsoftware nicht korrekt verifiziert werden, da die Zertifikate so genannte QC Statements (Qualified Certificate) beinhalten, die (in der Fachsprache) „kritisch“ markiert wurden und Adobe Acrobat wenig anfangen kann.

Nichtsdestotrotz können diese Signaturen einfach auf ihre Gültigkeit hin überprüft werden:

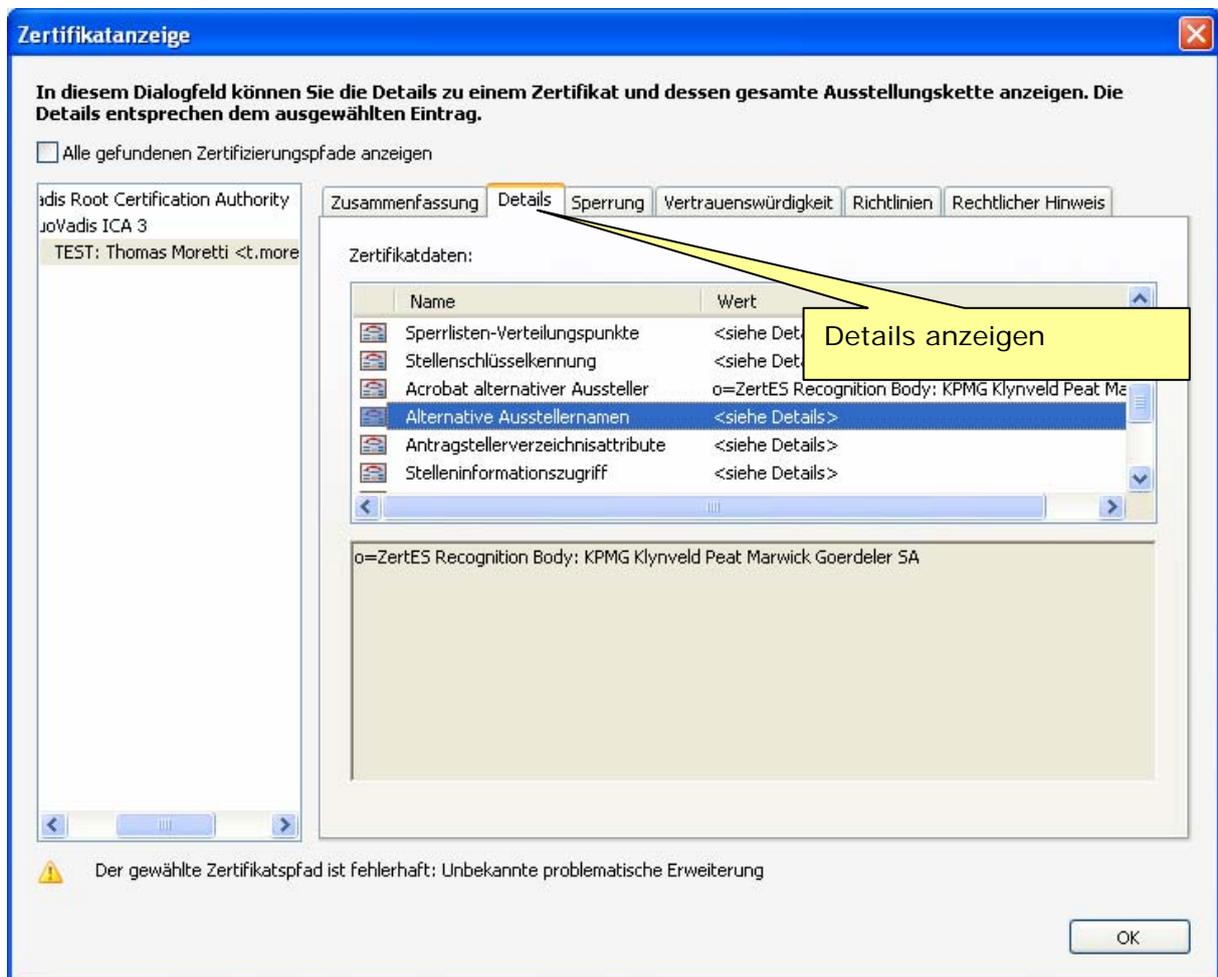


Über die Unterschriftseigenschaften wird der Detaildialog angezeigt:



Überprüfen Sie, ob das Dokument seit der Zertifizierung/Unterschrift nicht geändert wurde.

Lassen Sie sich anschliessend das Zertifikat anzeigen und prüfen Sie folgende Zertifikatsdaten:



Das Datum der Signatur muss zwischen den Daten in den Feldern **Gültigkeit beginnt am** und **Gültigkeit endet am** liegen.

Bei einem Schweizer qualifizierten Zertifikat muss im Feld **Alternative Ausstellernamen** der folgende Eintrag stehen:

o=ZertES Recognition Body: KPMG Klynveld Peat Marwick Goerdeler SA

Im Feld **Antragstellerverzeichnisattribute** sind weitere Informationen zum Unterzeichner ersichtlich, wie zum Beispiel:

- Geburtsdatum
- evtl. Geschlecht
- Geburtsort respektive Bürgerort
- Staatsangehörigkeit (Nationalität)
- Wohnsitzland

Die **Zertifikatsrichtlinien** müssen die folgenden Einträge aufweisen:

Richtlinien-OID: 0.4.0.1456.1.1

Richtlinien-OID: 0.4.0.1456.1.2

bedeutet: Zertifikatsrichtlinien für qualifizierte Zertifikate für die Öffentlichkeit und Pflicht zur Verwendung einer sicheren Signaturerstellungseinheit)

Der Eintrag **QC-Statements** muss folgende Merkmale aufweisen:

- 1.3.6.1.5.5.7.11.1 (*PKIX Compliance (kritisch gemäss RFC 3039)*)
- QC-Kompatibilität
- QC-EU-Grenzwert: n.nn CHF (Menge: n, Exponent: n, Währung: XXX)
- QC-SSCD

Im **Aussteller-Zertifikat** (QuoVadis ICA 3) müssen ebenfalls unter **QC-Statements** die folgende Einträge ersichtlich sein:

- 1.3.6.1.5.5.7.11.1 (*PKIX Compliance (kritisch gemäss RFC 3039)*)
- QC-Kompatibilität



Hinweis

Da Adobe Acrobat bei einem qualifizierten Zertifikat keine OCSP Prüfung durchführt, kann im Zweifelsfall auch die Sperrliste heruntergeladen werden. Doppelklickt man danach auf die Datei kann die Seriennummer des Zertifikats in der Liste gesucht werden. Ist diese darin nicht vorhanden ist das Zertifikat nicht revoziert.

Die Download Informationen sind im Eintrag Sperrlisten-Verteilungspunkte ersichtlich. Zur Überprüfung von qualifizierten QuoVadis Zertifikaten verwenden Sie folgenden Link: <http://www.quovadisoffshore.com/crl/qvica3.crl>

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.