




Installationen und Einstellungen für die Überprüfung von digital signierten PDF-Dokumenten / Strafregisterauszügen

I. Um signierte PDF-Dokumente validieren zu können benötigen Sie

- das installierte Root-Zertifikat der Zertifizierungsstelle, die das Zertifikat ausgegeben hat, mit dem das zu prüfende Dokument signiert wurde (zur Installation von Rootzertifikaten siehe unten unter II)
- **Adobe Acrobat Reader Version 8.x oder 9.x** (zu den notwendigen Einstellungen im Adobe Reader siehe unten unter III.a). Die Validierungsfunktionen von Adobe Acrobat Reader weisen ein sehr hohes Niveau auf und sind – hat man das Prinzip einmal begriffen – auch sehr benutzerfreundlich und aussagekräftig. Die Nutzer haben zusätzlich ein hohes Bewusstsein für das Original.
- eine **aktive Internetverbindung** (fakultativ, nur wenn sie die Revokationslisten online überprüfen wollen)
Falls Sie eine elektronische Signatur voll validieren möchten, müssen die aktuellen Revokationslisten bei der CA darauf geprüft werden, ob das zur Signatur verwendete Zertifikat revoziert wurde. Sie können die Prüfung der Revokationslisten im Adobe Reader aber auch deaktivieren (III.b). So wird ihnen die Unterschrift als gültig angezeigt, auch wenn Sie keine Internet-Verbindung haben.

Symbol und Bedeutung	Symbol und Bedeutung	Symbol und Bedeutung
		
Validierung nicht möglich aus einem oder mehreren der folgenden Gründe: 1. Root-Zertifikat nicht installiert 2. Adobe Acrobat Reader Einstellungen bezüglich Nutzung des Windows Zertifikatsspeichers nicht richtig. 3. keine Internetverbindung vorhanden bei aktiviertem Zugriff auf Revokationslisten..	Positiv validierte Unterschrift Positiv validierte Unterschrift mit Hinweis, z.B. wenn mehrere Personen ein Dokument signiert haben, wird bei den vorangehenden Unterschriften das Hinweissymbol sichtbar. Jede einem Dokument zugefügte Signatur erzeugt eine Revision/Version innerhalb des Dokuments. So kann reproduziert werden, welchen Inhalt das Dokument zum Zeitpunkt jeder Signatur hatte.	Positiv validierte Zertifizierung Wird ein Dokument zertifiziert, so können danach weder Änderungen vorgenommen, noch zusätzliche Unterschriften angefügt werden.

II. Download und Installation von Root Zertifikaten

Wenn Sie unter Windows den Windows Update automatisch oder benutzerdefiniert regelmässig durchführen, erhalten Sie auch ein Update für Root-/Stammzertifikate.. Alle in der Schweiz zur Ausgabe von qualifizierten Zertifikaten autorisierten CA haben ihre Root-Zertifikate durch Microsoft in den Windows Root Zertifikat Update integrieren lassen, ebenfalls die meisten ausländischen CA.







Praktisch führen aber die wenigsten Benutzer regelmässig den Root-Zertifikat Update via Windows Update durch. Im Büroumfeld wird der Windows Update und/oder der Windows Root Zertifikats Update normalerweise ebenfalls nicht ausgeführt. Es wird deshalb empfohlen, die Root-Zertifikate selbst zu installieren. Dies ist aber nur möglich, wenn der Benutzer über entsprechende Rechte verfügt (privat meist vorhanden, im Büro oft nicht vorhanden).

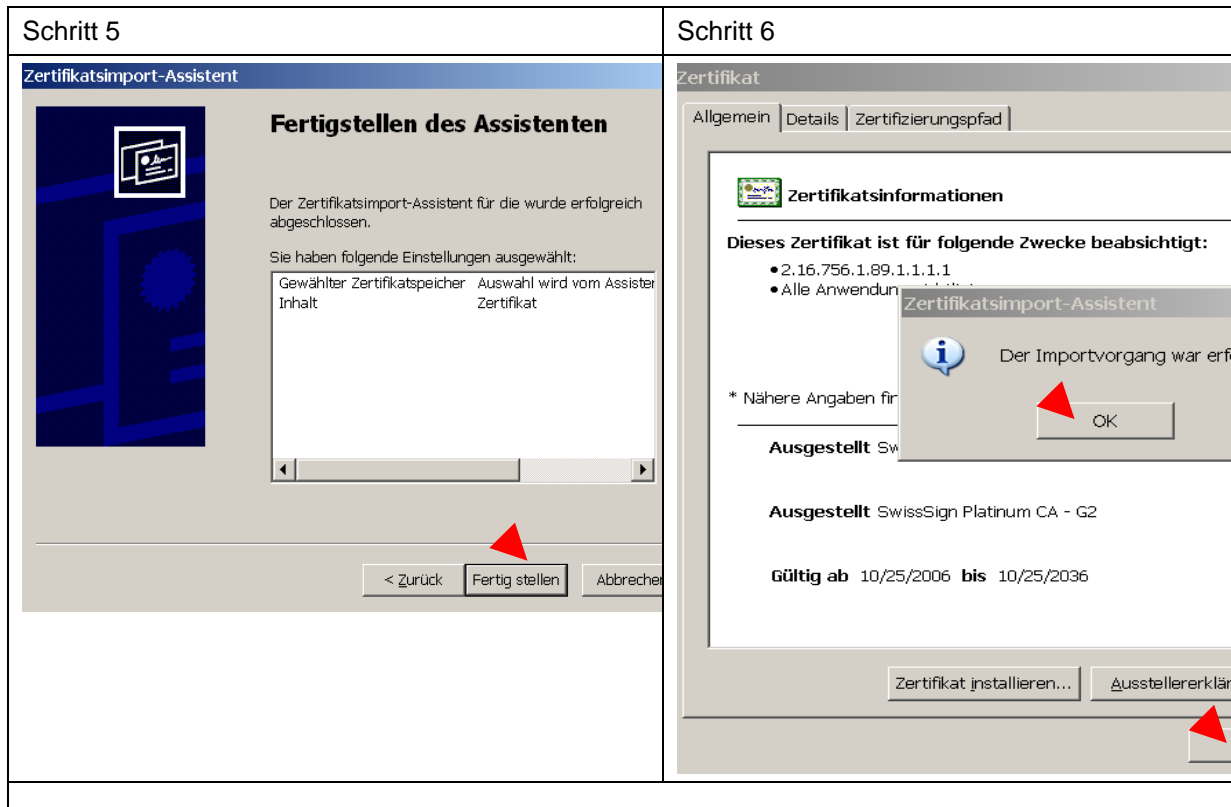
Installieren Sie nun die notwendigen CA Root- und Zwischenzertifikate auf dem Computer, auf dem die Signaturprüfung durchgeführt werden soll.

Die für die Überprüfung eines elektronischen, digital signierten Strafregisterauszuges notwendigen Zertifikate finden Sie bei swissdigicert.ch (Root CA und Diamond CA) und bei bit.admin.ch (Root CA und CA-A-T01)

Unter Windows befinden sich die CA Zertifikate, die für die Validierung benötigt werden, danach im Zertifikatsspeicher. Auf anderen Rechnern müssen sie meist direkt in den Zertifikatsspeicher von Adobe Acrobat (Reader) Versionen 8x und 9x installiert werden.

Wenn Sie das **Zertifikat herunterladen, speichern Sie es zuerst ab**. Wird die Zertifikatsdatei unter der Extension .PEM abgespeichert, wechseln sie die Extension auf .CRT oder .CER. Danach **Doppelklick auf die Zertifikats-Datei** um die Installation zu starten.

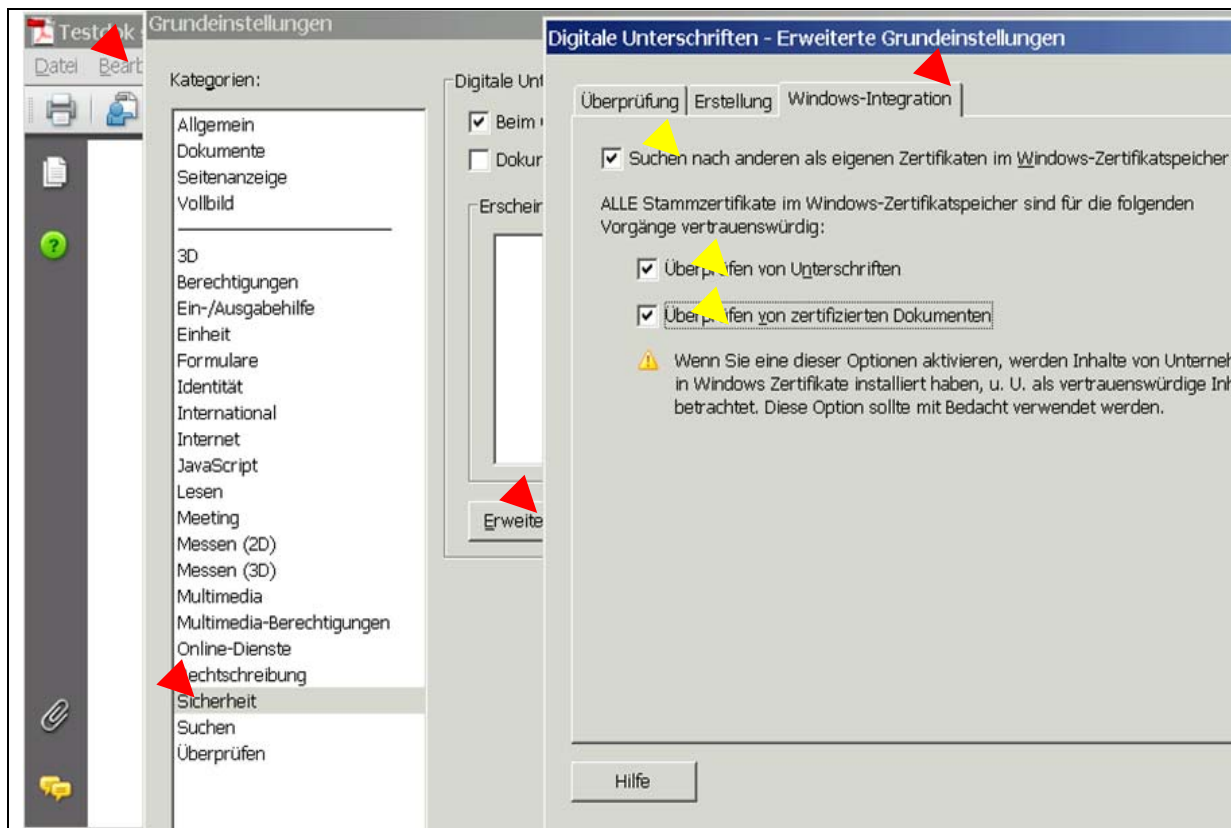
<p>Schritt 1</p> <p>Datei öffnen - Sicherheitswarnung</p> <p>Möchten Sie diese Datei öffnen?</p> <p>Name: Platinum_G2.crt Herausgeber: Unbekannter Herausgeber Typ: Sicherheitszertifikat Von: C:\Documents and Settings\UserD\Eigene Dateien</p> <p> <input type="button" value="Öffnen"/> <input type="button" value="Abbrechen"/></p> <p><input checked="" type="checkbox"/> Vor dem Öffnen dieser Datei immer bestätigen</p> <p>! Dateien aus dem Internet können nützlich sein, aber dieser Dateityp kann eventuell auf dem Computer Schaden anrichten. Öffnen Sie diese Software nicht, falls Sie der Quelle nicht vertrauen. Welches Risiko besteht?</p>	<p>Schritt 2</p> <p>Zertifikat</p> <p>Allgemein Details Zertifizierungspfad</p> <p> Zertifikatsinformationen</p> <p>Dieses Zertifikat ist für folgende Zwecke beabsichtigt:</p> <ul style="list-style-type: none"> • 2.16.756.1.89.1.1.1.1 • Alle Anwendungsrichtlinien <p>* Nähere Angaben finden Sie in den Angaben der Zertifizierungsstelle</p> <p>Ausgestellt SwissSign Platinum CA - G2</p> <p>Ausgestellt SwissSign Platinum CA - G2</p> <p>Gültig ab 10/25/2006 bis 10/25/2036</p> <p> <input type="button" value="Zertifikat installieren..."/> <input type="button" value="Ausstellererklärung"/></p> <p><input type="button" value="OK"/></p>
<p>Schritt 3</p> <p>Zertifikatsimport-Assistent</p> <p>Willkommen</p> <p>Dieser Assistent hilft Ihnen beim Kopieren von Zertifikaten, Zertifikatsvertrauenslisten und -sperrlisten vom Datenträger in den Zertifikatsspeicher.</p> <p>Ein Zertifikat wird von einer Zertifizierungsstelle ausgestellt und dient der Bestätigung Ihrer Identität. Zertifikate enthalten Informationen für den Datenschutz oder für den Aufbau sicherer Netzwerkverbindungen. Ein Zertifikatsspeicher ist der Systembereich in dem Zertifikate gespeichert werden.</p> <p>Klicken Sie auf "Weiter", um den Vorgang</p> <p> <input type="button" value=" < Zurück"/> <input type="button" value=" Weiter >"/> <input type="button" value=" Abbrechen"/></p>	<p>Schritt 4</p> <p>Zertifikatsimport-Assistent</p> <p>Zertifikatsspeicher</p> <p>Zertifikatsspeicher sind Systembereiche, in denen Zertifikate gespeichert</p> <p> Windows kann automatisch einen Zertifikatsspeicher auswählen oder Sie können einen Pfad für die Zertifikate angeben.</p> <p><input checked="" type="radio"/> Zertifikatsspeicher automatisch auswählen (auf dem Zertifikattyp basierend)</p> <p><input type="radio"/> Alle Zertifikate in folgendem Speicher speichern</p> <p>Zertifikatsspeicher:</p> <p><input type="text"/> <input type="button" value="Durchsuchen..."/></p> <p> <input type="button" value=" < Zurück"/> <input type="button" value=" Weiter >"/> <input type="button" value=" Abbrechen"/></p>



III. Einstellungen Adobe Reader 8.x oder 9.x für die Vaidierung von Unterschriften.

- a) Auf der Windows Plattform sollten Sie Adobe Acrobat Reader so konfigurieren, das er den Root-Zertifikaten im Windows Zertifikatspeicher vertraut:

Wählen Sie im Menu *Bearbeiten* die *Grundeinstellungen*. Wählen Sie danach in Kategorien *Sicherheit* und klicken Sie auf *Erweiterte Grundeinstellungen*. Im nun erscheinenden Fenster den Reiter *Windows Integration* anwählen und die 3 Check Boxes aktivieren.



b) Wenn Sie eine **Internet Verbindung haben**, achten Sie darauf, dass die Option *Beim Prüfen von Unterschriften immer feststellen, ob das zugehörige Zertifikat gesperrt wurde*, aktiviert ist.

Wenn Sie **keine Internet Verbindung haben**, deaktivieren sie die Check Box (gelber Pfeil), sonst werden gültige Unterschriften nicht positiv validiert, weil Adobe Acrobat Reader versucht eine Verbindung zu den Revokationslisten herzustellen.

