

Sign Live! CC

Qualifiziertes Signieren und Validieren

(Kurzanleitung)

Inhaltsverzeichnis

1	Einführung	2
2	Begriffe und Abkürzungen.....	2
3	Bevor es losgeht:.....	3
3.1	Was tun, wenn keine Lizenz vorliegt:	3
4	Datei signieren	4
4.1	So signieren Sie ein PDF-Dokument qualifiziert mit Sign Live! CC.....	4
4.2	So signieren Sie eine TXT-Datei qualifiziert mit Sign Live! CC.....	9
4.3	TXT-Dokument in Signatur einbetten.....	10
5	Signaturprüfung (Validierung).....	11
5.1	Darstellung einer Signaturprüfung.....	11
5.2	Dokument Validieren und Validierungsergebnis anzeigen.....	11
5.3	Validierungsprotokoll erzeugen.....	12
6	Sie benötigen Unterstützung?.....	12

1 Einführung

Die elektronische Signatur erfüllt auf digitalen Dokumenten dieselbe Funktion wie eine von Hand geleistete Unterschrift auf einem Papierdokument. Durch die elektronische Signatur ist es möglich, den Ersteller einer Signatur eindeutig zu identifizieren. Die elektronische Signatur gibt es in verschiedenen Sicherheitsstufen. Die *qualifizierte* elektronische Signatur erfüllt die höchsten Sicherheitsansprüche. Daher ist die *qualifizierte* elektronische Signatur (bis auf wenigen Ausnahmen) gem. § 126a BGB der eigenhändigen Unterschrift rechtlich gleich gestellt. Ausführliche Informationen zum Thema elektronische Signatur finden Sie im *Whitepaper „Elektronische Signaturen“* auf unserer Homepage <https://www.intarsys.de/infomaterial>.

Es können verschiedene Dateien signiert werden. Zum Beispiel PDF-Dateien, TXT-Dateien etc. Für jeden Dateityp gibt es bestimmte Signaturverfahren.

Die Echtheit der Signatur und die Dokumentintegrität können durch die Signaturvalidierung geprüft werden.

Zur Erstellung einer elektronischen Signatur benötigen Sie eine Signaturkarte, ein Kartenlesegerät sowie Signaturanwendungssoftware.

Dieses Dokument ist eine **Kurzanleitung** zur qualifizierten Signatur von PDF- und TXT-Dateien mit Sign Live! CC sowie der Signaturvalidierung und erhebt keinen Anspruch auf Vollständigkeit. Ausführliche Informationen finden Sie innerhalb der Anwendung im Menüpunkt „Hilfe“ oder mit der Tastenkombination F1.

2 Begriffe und Abkürzungen

SigG SigG ist die Abkürzung für „SignaturGesetz“. Das Signaturgesetz ist die rechtliche Grundlage der elektronischen Signatur.

Zertifikat Ein digitales Zertifikat ist ein digitaler Datensatz, der bestimmte Eigenschaften von Personen oder Objekten bestätigt und dessen Authentizität und Integrität durch kryptografische Verfahren geprüft werden kann. Das digitale Zertifikat enthält insbesondere die zu seiner Prüfung erforderlichen Daten.

Das **qualifizierte Zertifikat** – auch SigG Zertifikat - wird genutzt, um qualifizierte elektronische Signaturen nach dem SigG zu erstellen. Eine qualifizierte Signatur entspricht den höchsten Sicherheitsanforderungen. So fordert der Gesetzgeber zum Beispiel beim elektronischen Rechnungsversand eine qualifizierte Signatur, damit der Rechnungsempfänger zum Vorsteuerabzug gem. § 14 UStG berechtigt ist. Für verschiedene andere Anwendungen reichen fortgeschrittene Signaturen.

Das **fortgeschrittene Zertifikat** wird zum Beispiel für die Anmeldung in WEB-Portalen, sowie für die Ver- und Entschlüsselung von Dateien genutzt.

- SAK Als SAK (Signaturanwendungskomponente) bezeichnet man die Software, mit der Sie Signaturen auf Dokumenten erstellen. *Sign Live! CC* ist eine SAK.
- Signaturkarte Auf einer Signaturkarte befindet sich ein Chip mit fortgeschrittenen und qualifizierten digitalen Zertifikaten.
- Kartenlesegerät Um Signaturkarten nutzen zu können benötigen Sie ein geeignetes Lesegeräte. Eine Liste der von uns getesteten Kartenlesegeräte finden Sie im Sign Live! CC – Datenblatt, das zusammen mit der Software ausgeliefert wird.
- Signaturvalidierung Die Signaturvalidierung ist die Prüfung der Signatur auf dem Dokument. Dabei wird eine Echtheitsprüfung des Zertifikats und eine Prüfung der Dokumentintegrität vorgenommen. Die Echtheitsprüfung bestätigt, dass das Zertifikat des Unterzeichners oder das entsprechend übergebene Zertifikat in der Liste vertrauenswürdiger Zertifikate vorhanden ist. Ferner wird das Unterschriftszertifikat auf Gültigkeit geprüft.

3 Bevor es losgeht:

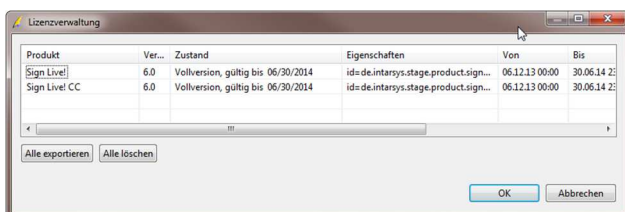
Um dieser Anleitung zu folgen sollten Sie folgendes vorab prüfen:

- *Sign Live! CC* ist auf Ihrem Rechner installiert, eine gültige Lizenz liegt vor
- Ein Kartenleser liegt bereit und die entsprechende Treibersoftware ist installiert
- Eine gültige Signaturkarte ist vorhanden, die Signatur-Pin für diese Karte ist bekannt
- Ein zu signierendes PDF-Dokument für ist vorhanden

TIPP: Mit der Tastenkombination **STRG+N** können Sie in *Sign Live! CC* ein leeres PDF-Dokument erzeugen. Dieses Dokument muss vor der Signatur gespeichert werden.

So überprüfen Sie, ob eine gültige Lizenz für Sign Live! CC vorliegt:

- Starten Sie Sign Live! CC
- Wählen Sie Menüpunkt EXTRAS ->Lizenzverwaltung
- So sollte der Bildschirm aussehen:



Achten Sie in der Lizenzverwaltung auf das Gültigkeitsdatum.

Schließen Sie das Fenster mit [OK]

3.1 Was tun, wenn keine Lizenz vorliegt:

Beantragen Sie eine zeitlich beschränkte Testlizenz unter der Mailadresse license@intarsys.de

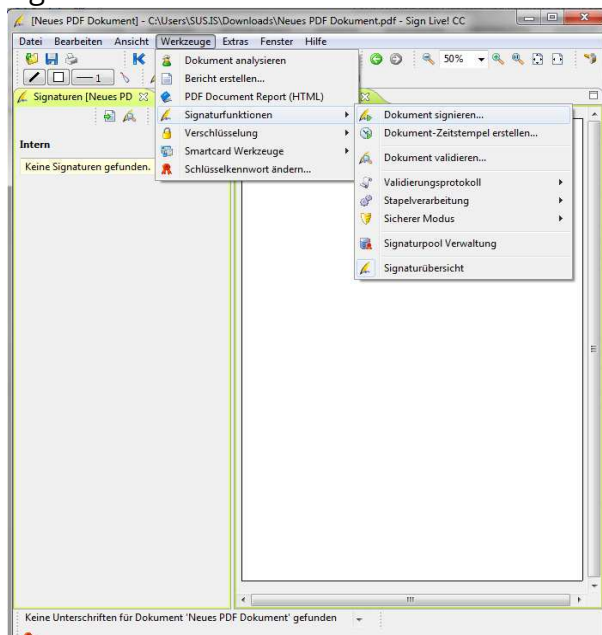
4 Datei signieren

Um ein Dokument zu signieren schließen Sie bitte Ihr Kartenlesegerät an.

TIPP: Die Signaturkarte sollte erst bei Aufforderung eingesteckt werden. Bei verschiedenen Kartenlesern treten Fehler auf, wenn die Signaturkarte bereits beim Start der Anwendung steckt.

4.1 So signieren Sie ein PDF-Dokument qualifiziert mit Sign Live! CC.

1. Starten Sie Sign Live! CC
2. Öffnen Sie die zu signierende **PDF-Datei** mit Menüpunkt DATEI - Öffnen.
3. Zur Signatur nutzen Sie den Menüpunkt WERKZEUGE > Signaturfunktionen > Dokument signieren.



TIPP:

Erzeugen Sie zum Test ein leeres PDF-Dokument mit der Tastenkombination STRG+N

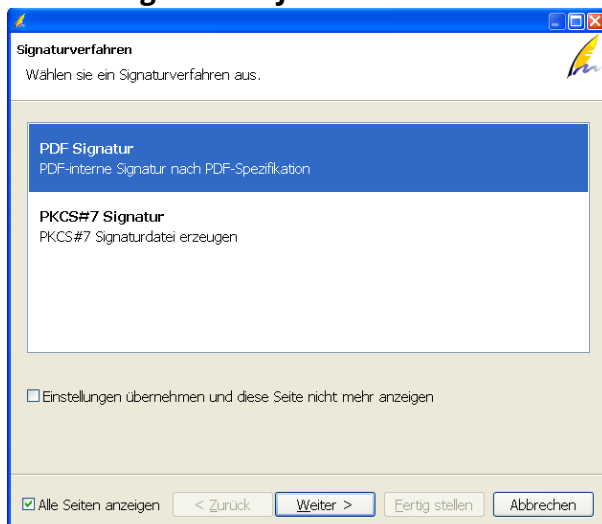
Jede zu signierende Datei muss vor der Signatur gespeichert sein.

Hinweis:

Beim Öffnen eines Dokuments prüft Sign Live! CC ob sich darauf bereits eine Signatur befindet. Aus diesem Grund kann die Darstellung des Dokuments einen Moment dauern.

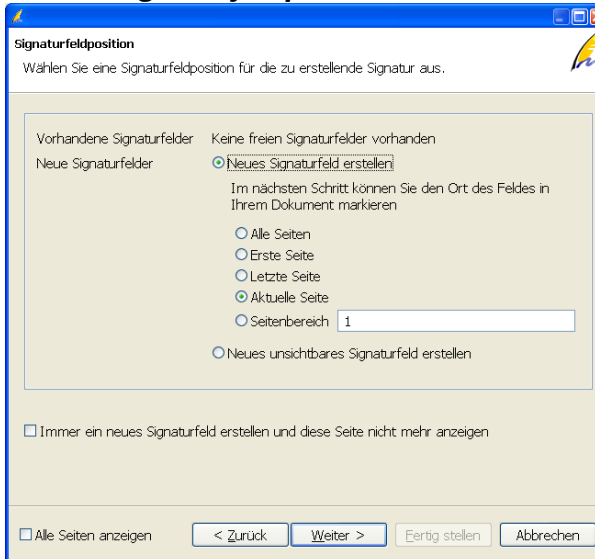
Es öffnet sich automatisch das Fenster „Signaturverfahren“.

4. Fenster **Signaturverfahren:**



Markieren **PDF-Signatur** und drücken Sie [Weiter >].

5. Fenster **Signaturfeldposition:**

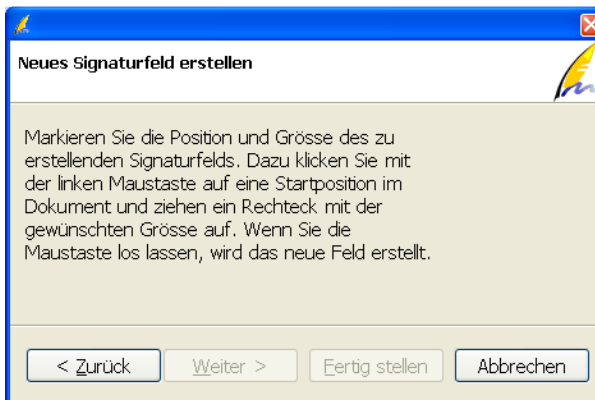


Sie können nun eine sichtbare, oder eine unsichtbare Signatur erstellen.

Bei der unsichtbaren Signatur werden die Signaturdaten in das PDF unsichtbar eingebettet. Die Signatur wird dennoch von einer Signaturvalidierungs-Software erkannt und kann geprüft (validiert) werden.

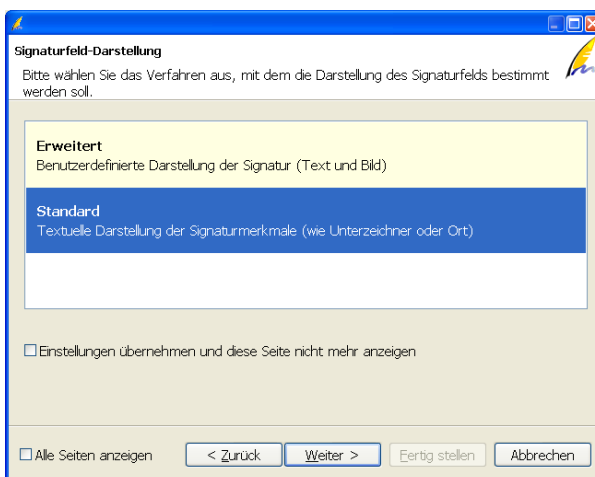
Bei einer sichtbaren Signatur wählen Sie die Seite/n aus, auf denen die Signatur sichtbar dargestellt werden soll. Nutzen Sie dazu die Option „Neues Signaturfeld erstellen“, wählen Sie die Seite/n und drücken Sie dann [Weiter >].

6. Es öffnet sich das Fenster **Neues Signaturfeld erstellen.**



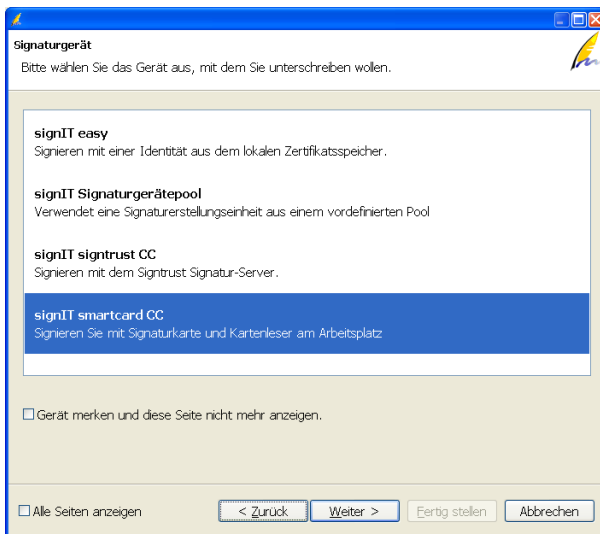
Wenn Sie nun mit der Maus auf das Dokument zeigen **ändert sich die Darstellung der Maus zum Fadenkreuz**. Ziehen Sie mit gedrückter linker Maustaste ein Feld in der Größe und an der Position, an der die Signatur dargestellt werden soll.

7. Sobald Sie die Maus loslassen öffnet sich das Fenster **Signaturfeld-Darstellung**



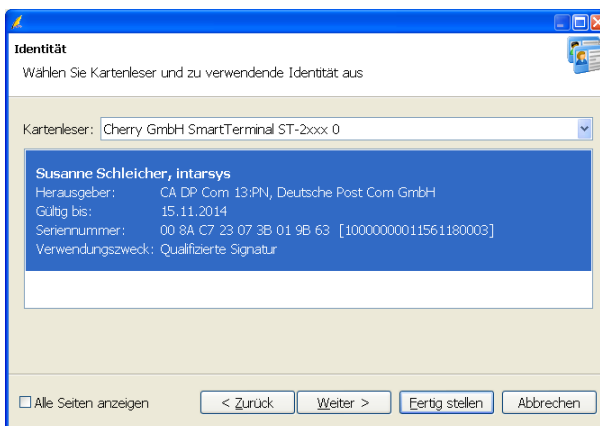
Wählen Sie hier „Standard“ und drücken Sie dann [Weiter >].

8. Fenster **Signaturgerät**



Hier markieren Sie „signIT smartcard CC“, da Sie mit einer Signaturkarte und Kartenlesegerät am Arbeitsplatz signieren möchten [Weiter >].

9. Im Fenster **Identität**



Hier wird der angeschlossene Kartenleser angezeigt und Sie werden zum Einstecken der Signaturkarte aufgefordert. Steckt diese, wird die Identität geprüft und das Zertifikat auf der Karte wird angezeigt. Hier können Sie bereits [Fertig stellen] drücken.

Wenn Sie mit Ihrer Signaturkarte eine Attributzertifikat beantragt haben, kann dies im nächsten Fenster durch [Weiter >] angezeigt und genutzt werden.

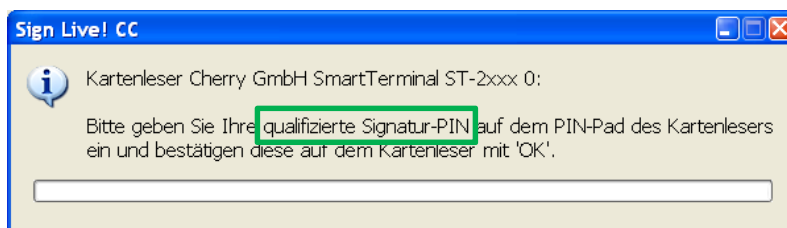
10. Sie werden nun zur Eingabe der PIN (für qualifizierte Signatur) aufgefordert.

Hinweis:

Auf den Signaturkarten befinden sich üblicherweise verschiedene Zertifikate. Z. B. für die „qualifizierte Signatur“ und für die „fortgeschrittenen Signatur“ (Authentisierung).

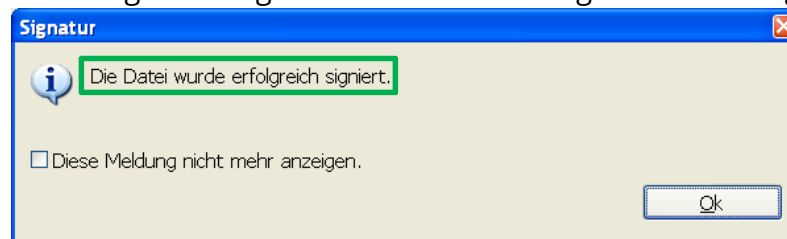
Unter Umständen haben Sie für diese Zertifikate verschiedene PINs vergeben.

Lesen Sie daher bitte genau, welche PIN Ihre Software verlangt. Geben Sie die angeforderte PIN auf dem Kartenlesegerät ein und bestätigen Sie die Eingabe ebenfalls auf dem Kartenlesegerät.

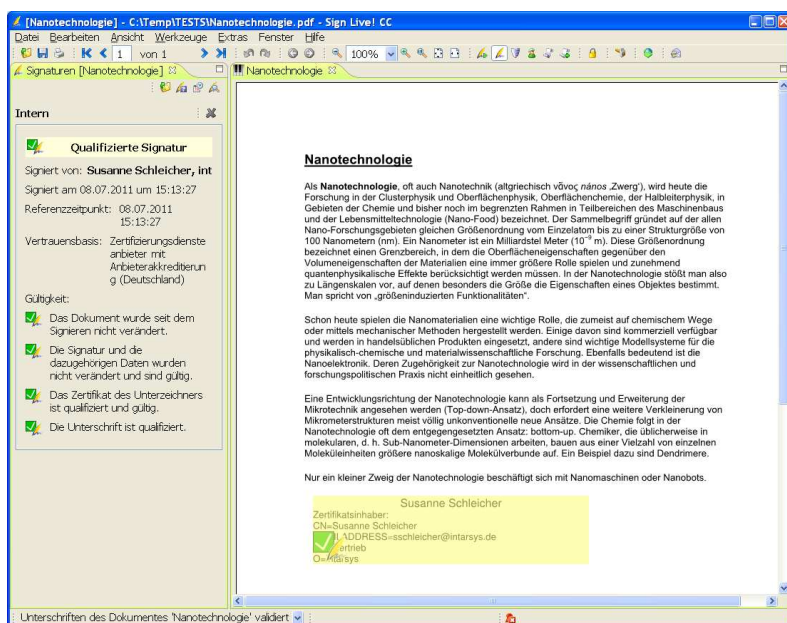


Bitte beachten Sie, dass die PIN-Eingabe aus Sicherheitsgründen innerhalb von 30 Sekunden erfolgen muss. Ansonsten wird der Vorgang abgebrochen.

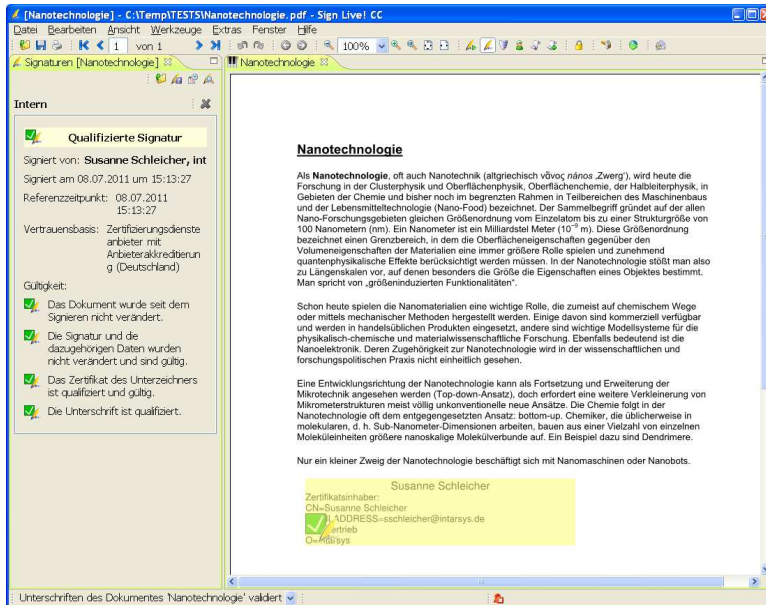
11. Die erfolgreiche Signatur wird mit nachfolgender Meldung bestätigt.



Das Dokument ist nun mit einer sichtbaren Signatur versehen.

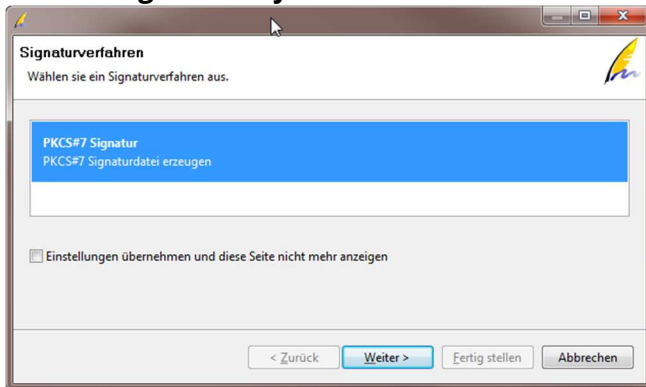


Es sollte die Seitenleiste „Signaturübersicht“ im linken Fenster angezeigt werden. Wenn nicht, kann die Anzeige im Menüpunkt **Ansicht-Seitenleiste-Signaturübersicht** eingeschaltet werden.



4.2 So signieren Sie eine TXT-Datei qualifiziert mit Sign Live! CC.

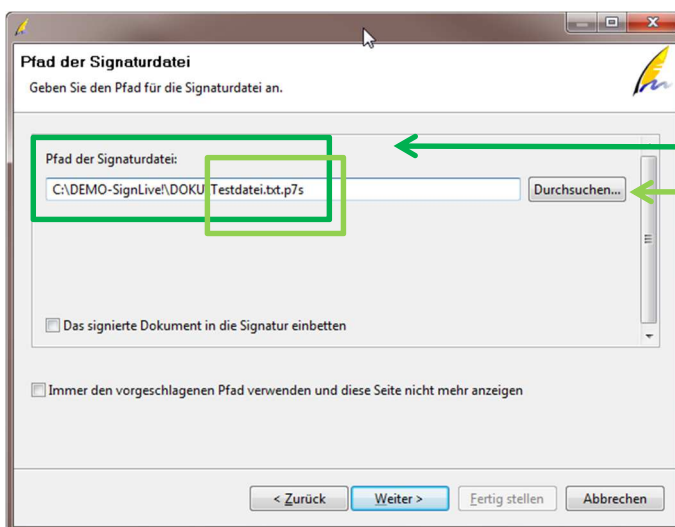
1. Starten Sie Sign Live! CC
2. Öffnen Sie die zu signierende **TXT-Datei** mit Menüpunkt DATEI - Öffnen.
3. Zur Signatur nutzen Sie den Menüpunkt WERKZEUGE – Signaturfunktionen - Dokument signieren.
4. Fenster **Signaturverfahren:**



Abhängig vom Dokumenttyp gibt es verschiedenen Signaturverfahren. (Ausführliche Informationen finden Sie in der Hilfe).

TXT-Dateien werden signiert, indem eine PKCS#7-Datei erzeugt wird. Deshalb steht kein anderes Verfahren zur Verfügung. Drücken Sie [Weiter >].

5. Fenster **Pfad der Signaturdatei:**
Bei der Signatur der TXT-Datei mit PKCS#7 wird immer eine separate Signatur-Datei erzeugt. Sie haben somit zwei Dateien: Die Originaldatei im TXT-Format und eine Signaturdatei.
- 5.1 Die Signaturdatei wird normalerweise im selben Verzeichnis abgelegt, in dem auch die TXT-Datei abgelegt ist. Dieses Verzeichnis wird im *Feld „Pfad der Signaturdatei“* angezeigt. Mit dem Schalter „Durchsuchen..“ können Sie das Verzeichnis ändern. Der Dateiname der PKCS#7-Datei (Signaturdatei) inklusive Dateieindung wird ebenfalls in dieses Feld eingetragen. Die Dateieindung *p7s zeigt eine externe Signatur an.



4.3 TXT-Dokument in Signatur einbetten

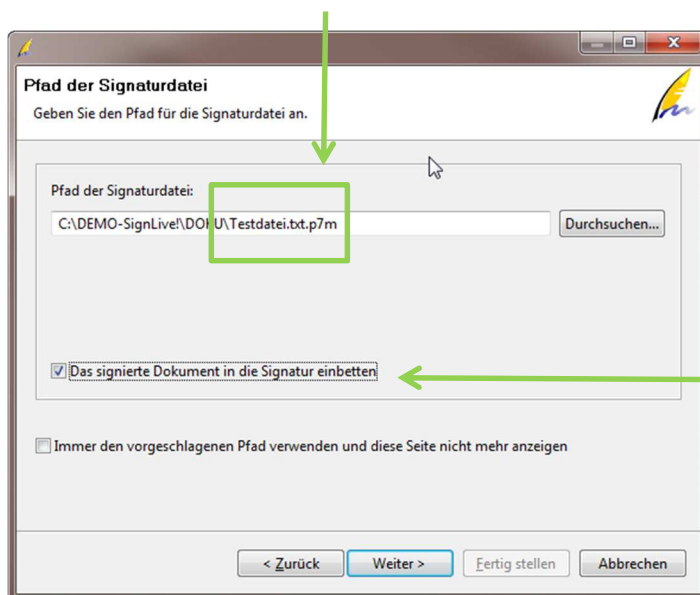
Bleiben **Originaldokument** und **Signaturdatei** im selben Verzeichnis, wird bei der Signaturvalidierung beim Öffnen der Signaturdatei automatisch auch das **TXT-Dokument geöffnet** und der **signierte Text** wird angezeigt.

In vielen Fällen ist es allerdings nötig, die Signaturdatei zu versenden.

Damit der Empfänger die Signatur prüfen kann und den Text sieht auf den sich die Signatur bezieht, müssen dem Empfänger beide Dateien zur Verfügung stehen.

Daher kann es sinnvoll sein, die TXT-Datei in die Signaturdatei einzubetten. Dann muss dem Empfänger nur die Signaturdatei (im P7M-Format) zugeschickt werden.

- 5.2. Zum Einbetten des Dokuments in die Signaturdatei aktivieren Sie das Kontrollkästchen. Die Dateiendung ***p7m** zeigt eine eingebettet Signatur an.



Durch Drücken auf [Weiter >] öffnet sich das Fenster **Signaturgerät**.

Die Erstellung der Signatur erfolgt analog der Signatur eines PDF-Dokuments. Bitte lesen Sie dazu im Kapitel 4.1 ab Punkt 8.

5 Signaturprüfung (Validierung)

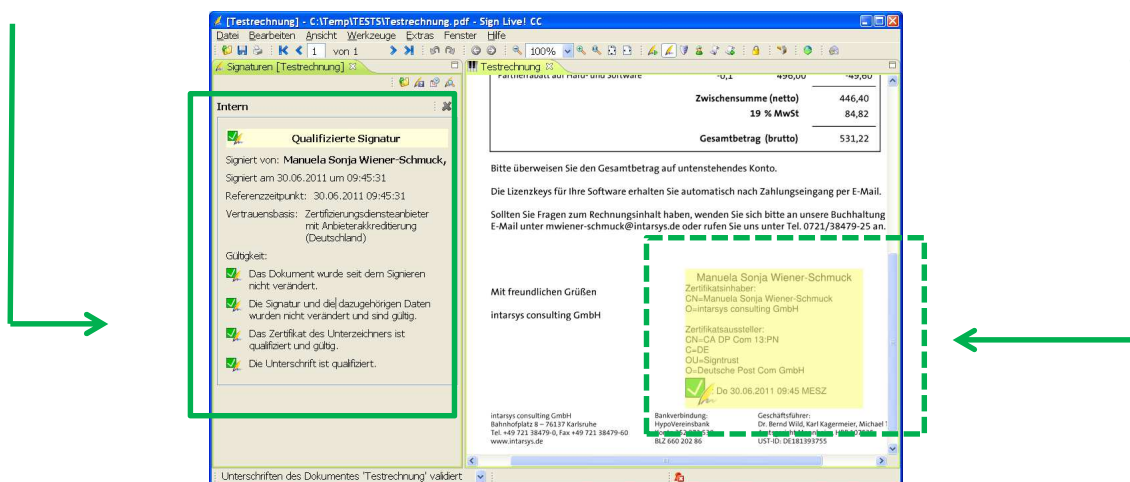
Bereits beim Öffnen der Datei überprüft *Sign Live! CC* standardmäßig jedes Dokument auf vorhandene Signaturen. Auch unsichtbare oder nicht-qualifizierte Signaturen werden erkannt.

Folgende Prüfungen werden vorgenommen:

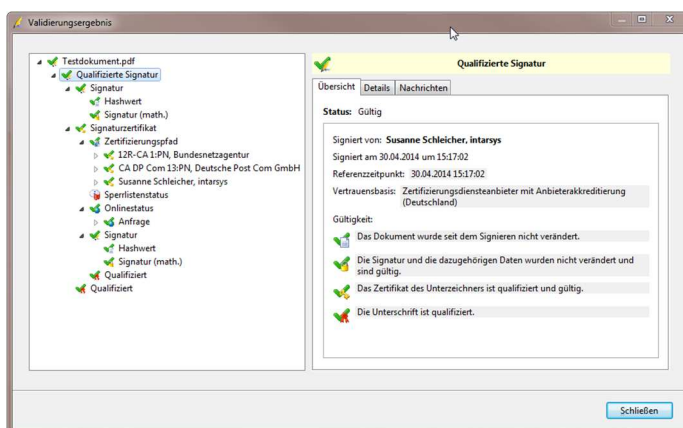
- Wurde das Dokument seit dem Signieren verändert?
- Ist die Signatur gültig und wurde diese nicht verändert?
- Ist das zur Signatur benutzte Zertifikat gültig?
- Handelt es sich um eine qualifizierte Signatur nach SigG?

5.1 Darstellung einer Signaturprüfung

Beim Öffnen eines PDF-Dokuments wird standardmäßig sofort geprüft, ob das Dokument signiert ist. Wenn ja, wird im linken Fenster das Validierungsergebnis, (Menü: Ansicht Seitenleiste Signaturübersicht) im rechten Fenster das Dokument dargestellt. Die Signatur muss nicht zwingend sichtbar sein.



5.2 Dokument Validieren und Validierungsergebnis anzeigen

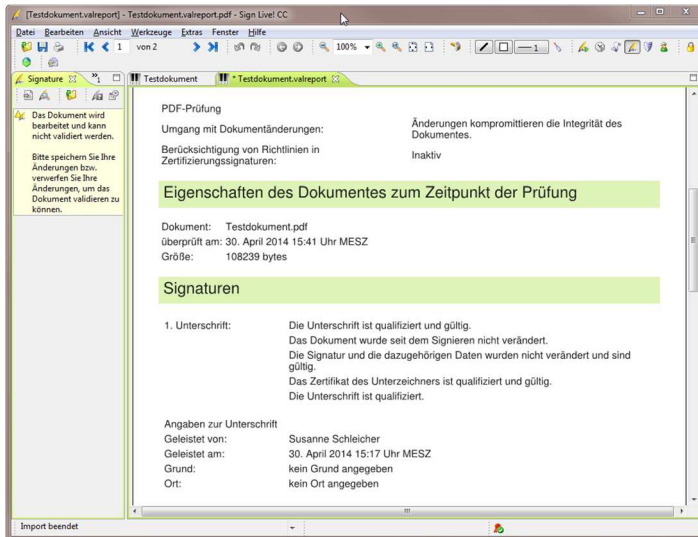


Dass die Prüfung des Dokuments bereits beim Öffnen erfolgt, kann im Menüpunkt *Extras > Einstellungen* im Bereich *Signaturvalidierung* ausgeschaltet werden. In diesem Fall kann die Validierung manuell angestoßen werden. Wählen Sie Menüpunkt *Werkzeuge*, dort *Signaturfunktionen* und dann *Signatur validieren* zur Anzeige des Validierungsergebnisses.

Weitere Informationen finden Sie in der Hilfe im Kapitel „Signaturen anzeigen und validieren“.

5.3 Validierungsprotokoll erzeugen

Sie erzeugen ein Validierungsprotokoll im PDF-Format über Menüpunkt *Werkzeuge > Signaturfunktionen > Validierungsprotokoll - erzeugen*.



Sign Live! CC ist werkseitig so eingestellt, dass beim Öffnen eines Dokuments dies automatisch auf das Vorhandensein einer Signatur untersucht wird. Durch diese Prüfung dauert das Öffnen eines Dokuments etwas länger.

Ist dies nicht gewünscht, kann die automatische Prüfung im Menüpunkt *Extras > Einstellungen* im Bereich *Signaturvalidierung* ausgeschaltet werden.

In diesem Fall muss die Validierung manuell angestoßen werden.

Sie erhalten den Validierungsreport als separate Datei. Beim Speichern wird automatisch der <Name des Dokuments>.valreport vorgeschlagen.

Weitere Möglichkeiten des Validierungsprotokolls.

Über Menüpunkt *Werkzeuge > Signaturfunktionen > Validierungsprotokoll mit erweiterten Optionen erzeugen* können Sie weitere Einstellungen für Ihr Validierungsprotokoll vornehmen.

- Ausgabeformat in HTML, PDF oder XML
- PDF/A-Konformität sicherstellen
- Protokoll (Bericht) an Originaldokument anhängen. Hier ist Vorsicht geboten, da durch das Anhängen des Validierungsprotokolls die Originaldatei verändert wird. Dies wird bei der Signaturprüfung erkannt, die Datei ist nicht mehr im Originalzustand.

6 Sie benötigen Unterstützung?

Bei Fragen hilft Ihnen unser Support-Team gerne schriftlich weiter. Bitte schreiben Sie Ihr Anliegen unter Verwendung einer aussagekräftigen Betreff-Zeile an support@intarsys.de.