SecCommerce
INFORMATIONSSYSTEME GMBH

SecCommerce

SecSigner®

für

Windows®

Anwenderhandbuch

Version 1.9
16.12.2008

Autor:
Ulrich Heller

www.seccommerce.de
info@seccommerce.de

Inhaltsverzeichnis

1 Einführung

n Deutschland werden die Rahmenbedingungen für rechtlich verbindliche digitale Signaturen durch das **Signaturgesetz** und die **Signaturverordnung** festgelegt.

Nur die darin definierte ***qualifizierte* elektronische Signatur** ist der persönlichen manuellen Unterschrift gesetzlich gleichgestellt und garantiert somit die Rechtsverbindlichkeit der unterzeichneten Willenserklärung; die Signatur ordnet eine solches Dokument eindeutig seinem Urheber zu. Mit der qualifizierten elektronischen Signatur von Ausgangsrechnungen haben Sie die Möglichkeit, Rechnungen vollelektronisch konform zu §14 UStG zu senden und zu empfangen und auf einen Papierversand zu verzichten.

Dazu benötigen Sie eine bei einer Zertifizierungsstelle erhältliche **Signaturkarte**, auf der ein **öffentlicher** und ein **privater Schlüssel** gespeichert sind. Den privaten Schlüssel benötigen Sie, um Dokumente mit einer digitalen Signatur zu versehen. Andere Nutzer können den öffentlichen Schlüssel bei der Zertifizierungsstelle abrufen, um Ihre Signaturen zu prüfen.
Die Signaturkarte wird mit einem **Kartenleser** an den PC/Server angeschlossen. Unsere Produkte unterstützen eine Vielzahl marktgängiger Kartenleser und Signaturkarten. Für Details verweisen wir Sie auf unsere Webseite.

SecSigner® signiert Dokumente oder andere Dateien (Text, HTML, PDF, Office-Dokumente, ...) mit qualifizierter elektronischer Signatur und bietet daneben weitere Funktionalität wie

- Hochsichere **Dokumentenanzeige** (Text, HTML-, XML-Dateien)
- **Mehrfachsignaturen** (mehrere Signaturen pro Dokument: '4-Augen-Prinzip')
- **Massensignaturen** (mehrere Signaturen mit einer PIN-Eingabe) mit geeigneten Signaturkarten.
- **Zeitstempel**-Einholung vom **Trustcenter** (soweit als Dienst vom Trustcenter angeboten)
- **Signatur-Verifikation** und **Online-Überprüfung** (OCSP) von Zertifikaten auf Gültigkeit
- **Verschlüsselung** beliebiger Dokumente

Besonders wichtig ist dabei die **Prüffunktion**, mit der Sie Urheberschaft und Integrität eines signierten Dokumentes verifizieren können.

Der **SecSigner®** ist ***frei verfügbar*** unter

www.seccommerce.de/de/produkte/webcontrust/secsigner/secsigner_eula.html

1.1 Anwendung

SecSigner® ermöglicht sowohl die Erstellung als auch die Überprüfung digitaler Signaturen.

Das **Unterzeichnen von Dokumenten** und beliebigen Dateien mit qualifizierter elektronischer Signatur nach dem Signaturgesetz erfolgt mit Hilfe der Signaturkarte, die über das Kartenlesegerät mit dem PC verbunden wird. Auf der Anzeige des Kartenlesers wird der Inhaber der Signaturkarte zur PIN-Eingabe (über die Tastatur des Kartenlesers) aufgefordert.

Auch ohne Signaturkarte und Kartenlesegerät ermöglicht SecSigner® die **Überprüfung** von elektronischen **Signaturen** und **Zeitstempeln**, inkl. Zertifikatstatusabfrage beim ausgebenden Trustcenter.

Signatur und Überprüfung werden dabei unterstützt durch eine **hochsicheren Anzeige** von Text-, HTML- und XML-Dokumenten.

SecSigner® ist eine nach Signaturgesetz (SigG, SigV) bestätigte und gemäß ITSEC E2/HOCH zertifizierte vollständige Signaturanwendungskomponente.

1.2 Eigenschaften

Merkmale des **SecSigner®**s in der Übersicht: Der **SecSigner®**

- ist eine in Version 2.0.0 nach **Signaturgesetz bestätigte** und gemäß ITSEC E2/HOCH zertifizierte vollständige **Signaturanwendungskomponente**, der die **Auslieferung über das Internet** gestattet ist,
- ist eine **Komponente mit HTML-Aufruf-Interface** zur einfachen Integration in Portalanwendungen,
- kann als **Komponente** in JAVA-Anwendungen oder andere Programme eingebunden werden,
- ist eine benutzerfreundliche **Anwendung direkt im Internet-Browser** mit sicherer Anzeige von Text-, HTML-, XML- und PDF/A-Dokumenten,
- signiert Dokumente oder andere Dateien (Text, HTML, PDF, Office-Dokumente, ...) mit PKCS#7-Signatur,
- kann **Mehrfachsignaturen** (mehrere Signaturen pro Dokument: '4-Augen-Prinzip') erzeugen,
- kann hochperformante **Massensignaturen** (mehrere Signaturen mit einer PIN-Eingabe) mit geeigneten Signaturkarten erzeugen,
- erfordert **keine** manuelle **Software-Installation**, da die Anwendung direkt über das Internet geladen und im Browser/Java-Plugin ausgeführt wird,
- unterstützt eine Vielzahl marktgängiger Kartenleser und Signaturkarten,
- bietet **Zeitstempel-Einholung vom Trustcenter** (soweit als Dienst vom Trustcenter angeboten) und
- **Signatur-** und **Zertfikat-Verifikation** inklusive
- **Online-Überprüfung** (OCSP) von Zertifikaten auf Gültigkeit.
- Unterstützt die **PDF-Signatur**

1.3 Benötigte Soft- und Hardware

1.3.1 Unterstützte Betriebssysteme

- Linux
- Microsoft Windows XP SP3, Vista
- Solaris (SunOS sparc, SunOS x86)
- Mac OS X 10.4.

Die in disem Handbuch beschriebene **installierbare** Version des **SecSigner®** ist nur für **Microsoft Windows 2000, XP, Vista** verfügbar.

1.3.2 Java® Laufzeitumgebung

SecSigner® ist eine **Java®**-Anwendung und setzt auf Ihrem PC die Laufzeitumgebung SUN Java® 1.4.2 (JRE) oder höher voraus. Diese kann von

java.sun.com/j2se/1.4.2/download.html

unter dem Menüpunkt „Download J2SE JRE“ geladen werden.

1.3.3 Signaturkarten und Kartenlesegeräte

Zur SignaturPRÜFUNG benötigen Sie keine zusätzliche Hardware.

Für die Signatur eigener Dokumente wird eine Signaturkarte benötigt, die über ein Kartenlesegerät an den PC angeschlossen wird. **SecSigner®** unterstützt eine Vielzahl marktgängiger Signaturkarten und Kartenlesegeräte**.**

1.4 Trustcenter-Anbindung

Für die Prüfung des Zertifikatstatus ist eine Online-Anbindung an das ausgebende Trustcenter notwendig. Es wird eine Kommunikation vom **SecSigner®** über das Internet zum Trustcenter aufgebaut. Bitte konfigurieren Sie je nach ausgewähltem Trustcenter Ihre Firewall für den Zugriff auf die entsprechenden Dienste der Anbieter.

1.5 Installation

Laden sie den frei verfügbaren **SecSigner®** als „**Setup_3_3_x.exe**“ von unserer Website

www.seccommerce.de/de/produkte/webcontrust/secsigner/secsigner_eula.html

Öffnen Sie die Datei **Setup_3_3_x.exe**“ durch Doppelklick. Akzeptieren Sie den Lizenzvertrag und bestätigen Sie die Installation im gewünschten Ordner.

Wenn Sie **SecSigner®** auch als Adobe Plug-In benutzen wollen, können Sie die Zuordnung während der Installation vornehmen:

Um SecSigner als Standardanwendung für die Signaturprüfung festzulegen, wählen Sie bitte im Acrobat Professional / Acrobat Reader:

Bearbeiten -> Grundeinstellungen -> Sicherheit -> Erweiterte Grundeinstellungen -> Verifikation -> „Immer Standard-Methode verwenden“

bzw.

Edit -> Preferences -> Security -> Advanced Preferences -> Verification -> -> "Always use the default method (overrides the document-specific method)" Wählen Sie dann in der Auswahlbox "SecCommerce.SecSignerPDF8".

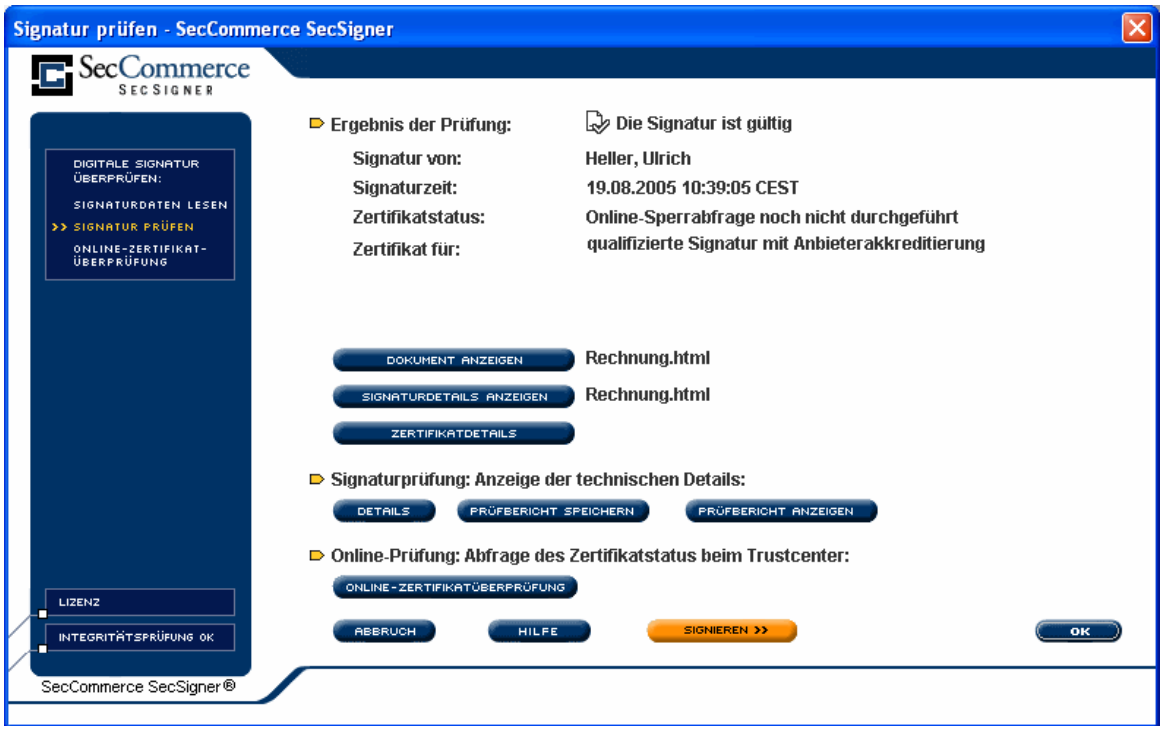
1.6 Initialisierung der Signaturkarte

Um eine Signaturkarte *erstmalig* zu nutzen, schalten Sie diese bitte zunächst mit unserem Administrationstool **SecCardAdmin®** frei:

www.seccommerce.de/de/produkte/seccardadmin/seccardadmin_demo.html

2 Signaturprüfung

Die Signatur eines Dokuments hat die Endung „**.pkcs7**“. Nach der Installation des **SecSigner**®s können Dokumente dieses Typs durch ***Doppelklick*** im Prüffenster geöffnet werden:

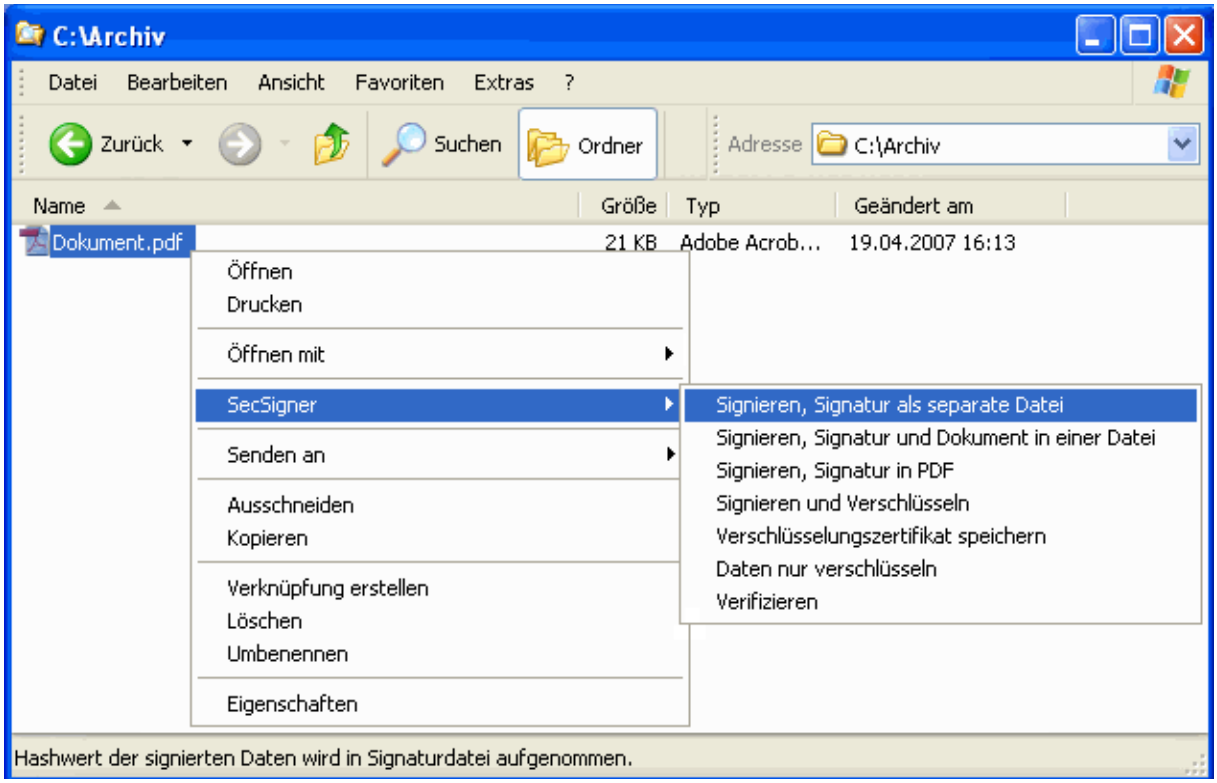


Sie können durch Wahl der entsprechenden Optionen nun auch eine **Online-Zertifikatprüfung** durchführen und/oder einen **Prüfbericht** erstellen lassen.

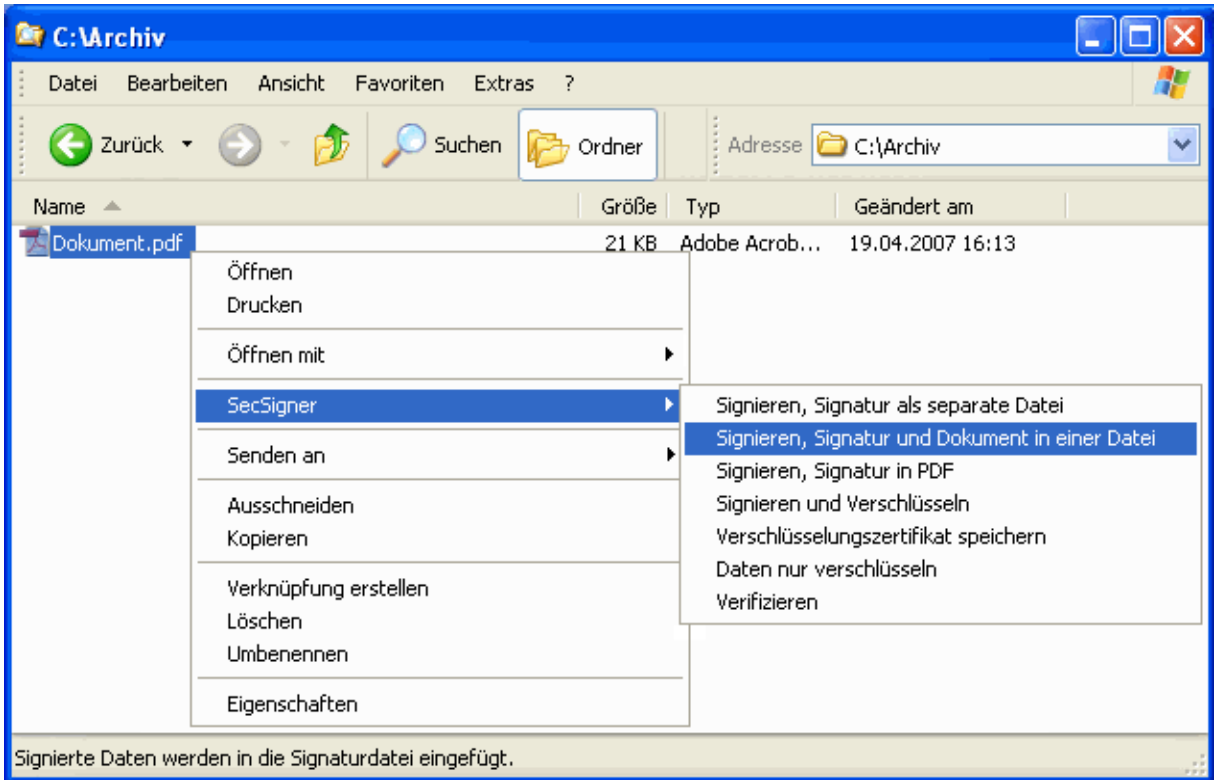
Handelt es sich beim signierten Dokument um eine Text-, HTML- oder XML-Datei, so kann diese mit der Option „Dokument anzeigen“ sicher angezeigt werden:

3 Erzeugen einer digitalen Signatur

Nach der Installation des **SecSigner**®s können Dokumente beliebigen Typs mit einer digitalen Signatur versehen werden. Der Klick auf ein Dokument mit der *rechten Maustaste* bietet die Optionen „SecSigner“, „Signieren, Signatur als separate Datei“.

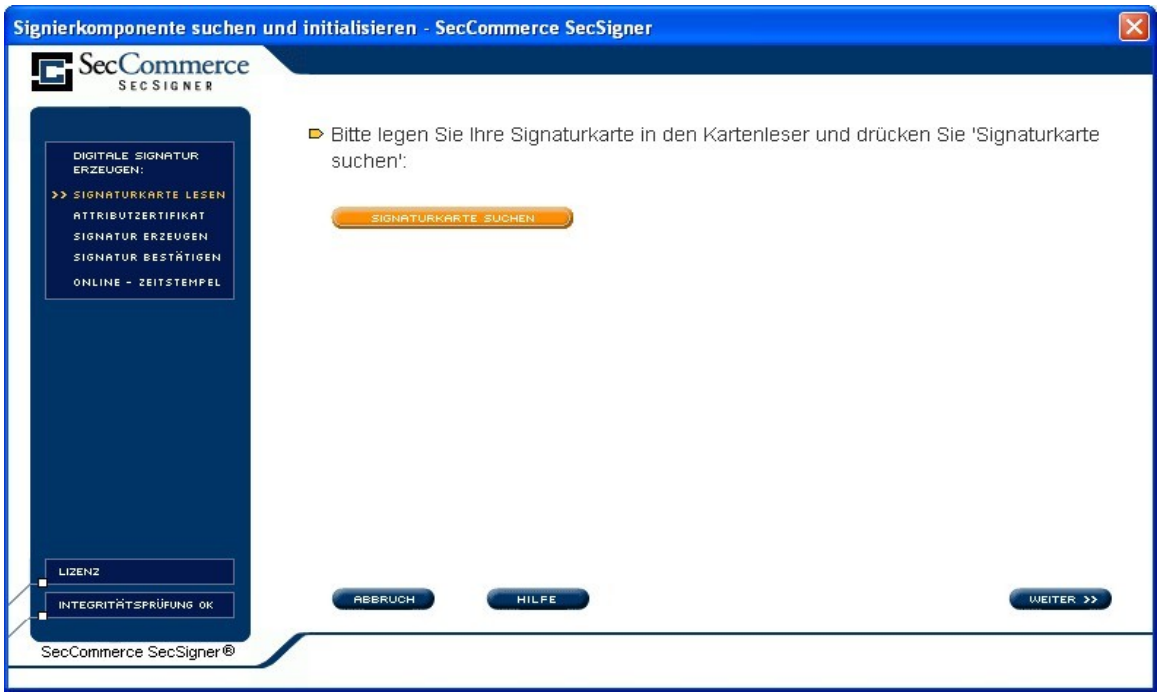


und „SecSigner“, „Signieren, Signatur und Dokument in einer Datei“.

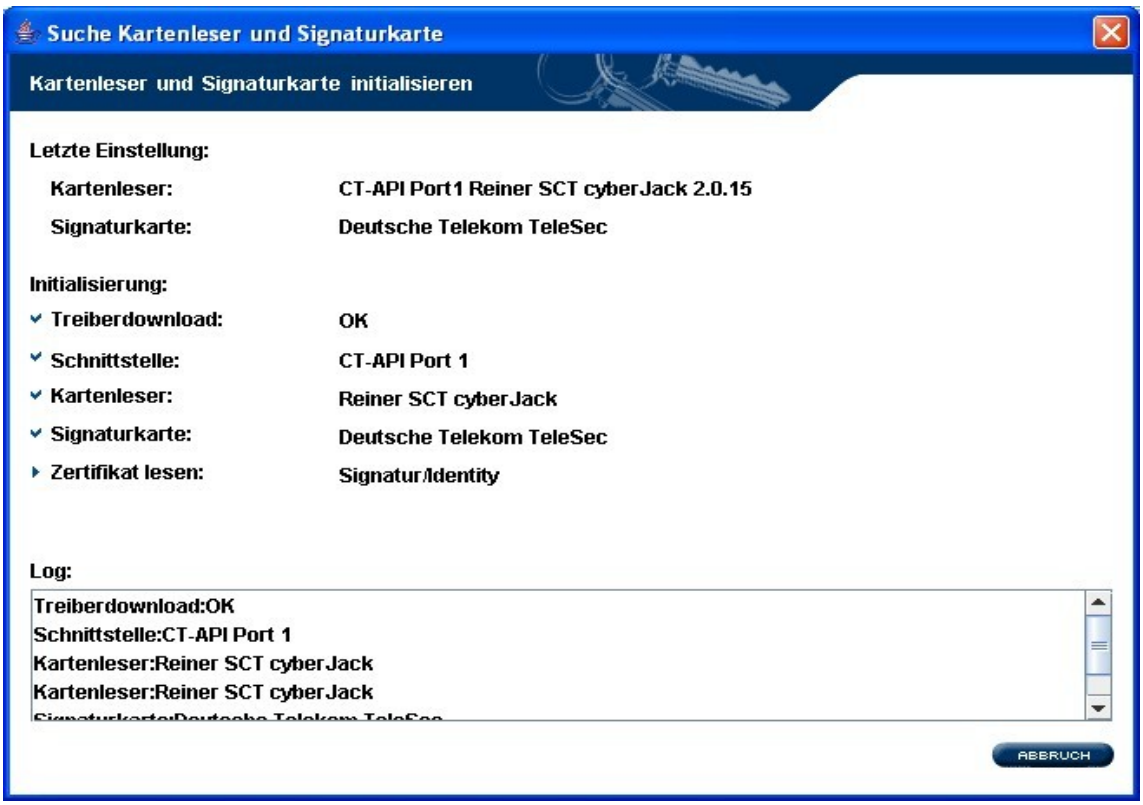


3.1 Initialisierung

Die Initialisierungs-Maske wird geöffnet:

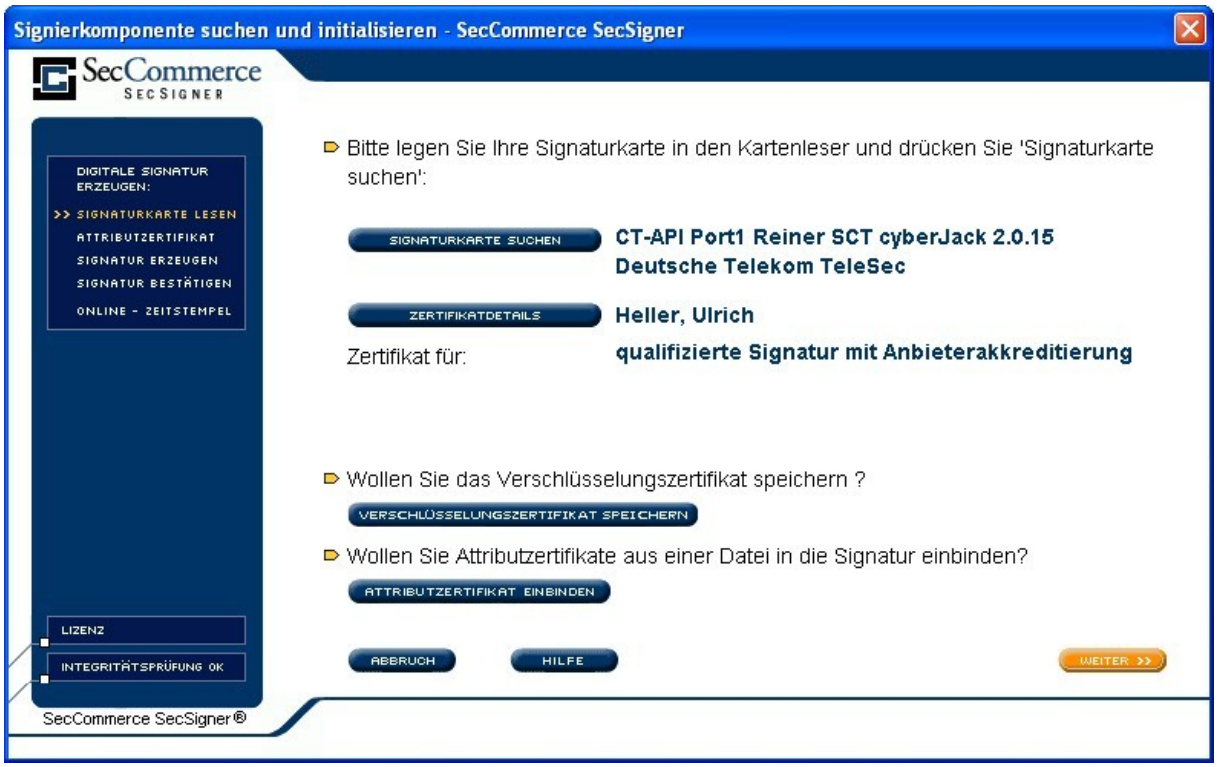


Nach de Wahl des Menüpunkts „Signaturkarte suchen“ werden Karte und Lesegerät initialisiert:



Der Signaturkartentyp (Trustcenter) wird bei der Initialisierung automatisch erkannt.

In der auf die Initialisierung folgenden Maske können Sie **Attributzertifikate** (Siehe **4.2**) in die Signatur einbinden.



3.2 Sichere Dokumentenanzeige

Mit der Option „weiter >>>“ gelangen Sie zur Anzeige-Maske:

Lesen Sie das Dokument vollständig durch und signieren Sie es anschließend.

3.3 Signatur

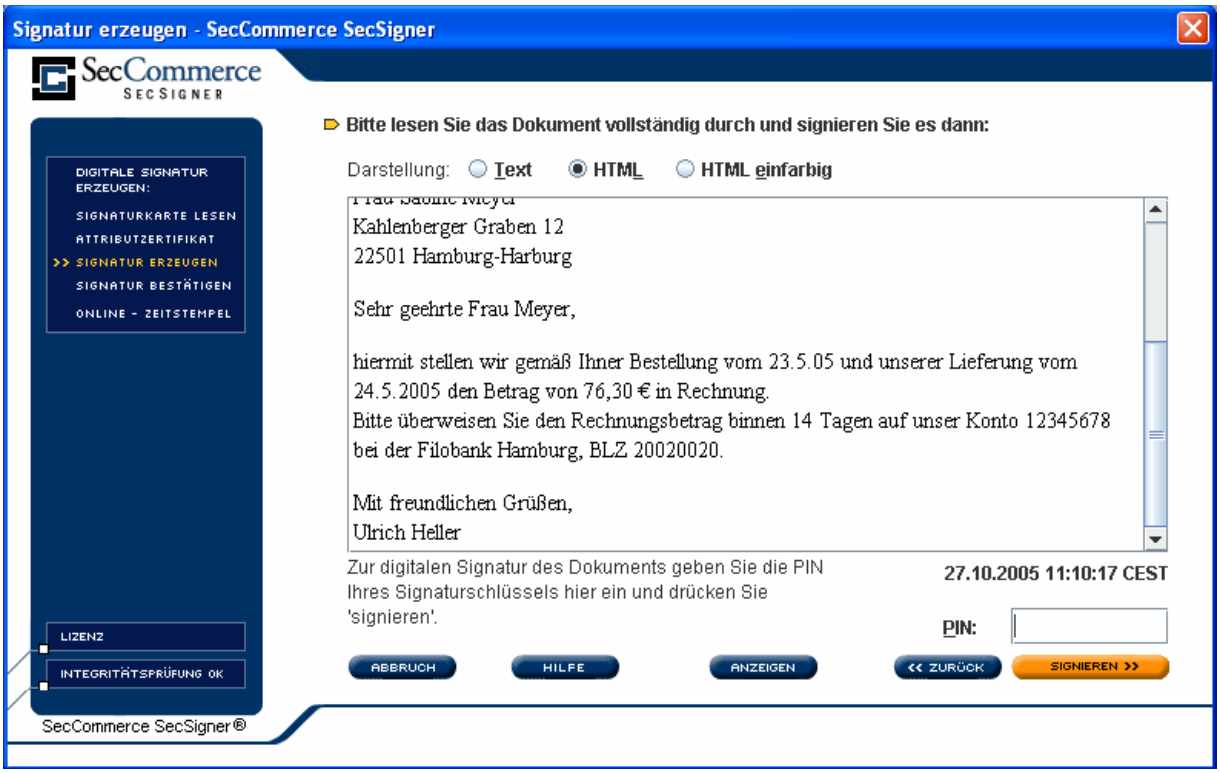
Sie werden nun aufgefordert, die PIN der Signaturkarte einzugeben.

3.3.1 Kartenlesegerät mit eigener PIN-Eingabe

Wenn Sie über ein Kartenlesegerät *mit* eigener PIN-Eingabe und geeigneten Treibern verfügen, geben Sie die PIN am Lesegerät ein:

3.3.2 Kartenlesegerät ohne eigene PIN-Eingabe

Wenn Sie über ein Kartenlesegerät *ohne* eigene PIN-Eingabe verfügen oder Ihr Lesegerät mit eigener PIN-Eingabe ohne geeigneten Treiber betreiben, so erfolgt die PIN-Eingabe über die Tastatur des PCs:



Bitte beachten Sie, dass das Signaturgesetz die PIN.-Eingabe am Kartenleser zur Erstellung qualifizierter Signaturen vorschreibt.

3.3.3 Zeitstempeldienst

Sie können anschließend Ihre Signatur mit einem Zeitstempel versehen, wenn Ihr Trustcenter diesen Dienst anbietet. Wählen Sie dazu die Option „Zeitstempel“. Sie werden dann aufgefordert, den PIN Ihrer Signaturkarte einzugeben und den Zeitstempeldienst der Signatur zu bestätigen.

3.3.4 Passwortbasierter Zeitstempeldienst

Daneben ist die Einholung von Zeitstempeln über passwortbasierte Authentifizierung möglich. Je nach Trustcenter bestehen verschiedene Möglichkeiten der Authentifizierung gegenüber dem Zeitstempelserver. Eine Authentifizierung wird von den Trustcentern für die Abrechnung der Zeitstempel verlangt. Dazu dienen folgende Einstellungen in der Konfigurationsdatei 'secsignersigg300.properties':

seccommerce.secsigner.timestampserver.url=<URL>

URL des Zeitstempelservers. Der Server muss Zeitstempel nach RFC 3161 erzeugen.

seccommerce.secsigner.timestampserver.httpusername=<NAME>

Benutzername zur Authentifizierung mittels HTTP-Basic-Authentication.

seccommerce.secsigner.timestampserver.httppassword=<PASSWORD>

Passwort zur Authentifizierung mittels HTTP-Basic-Authentication.

seccommerce.secsigner.timestampserver.keyfilename =<Dateiname>

PKCS#8 oder PKCS#12 privater Schlüssel zur Authentifizierung der TLS-Verbindung zum Zeitstempelserver oder zur Signatur der Anfragen.

seccommerce.secsigner.timestampserver.certfilename=<Dateiname>

Zertifikat zur Authentifizierung, wenn der Schlüssel als PKCS#8 vorliegt.

seccommerce.secsigner.timestampserver.keypassword=<PASSWORT>

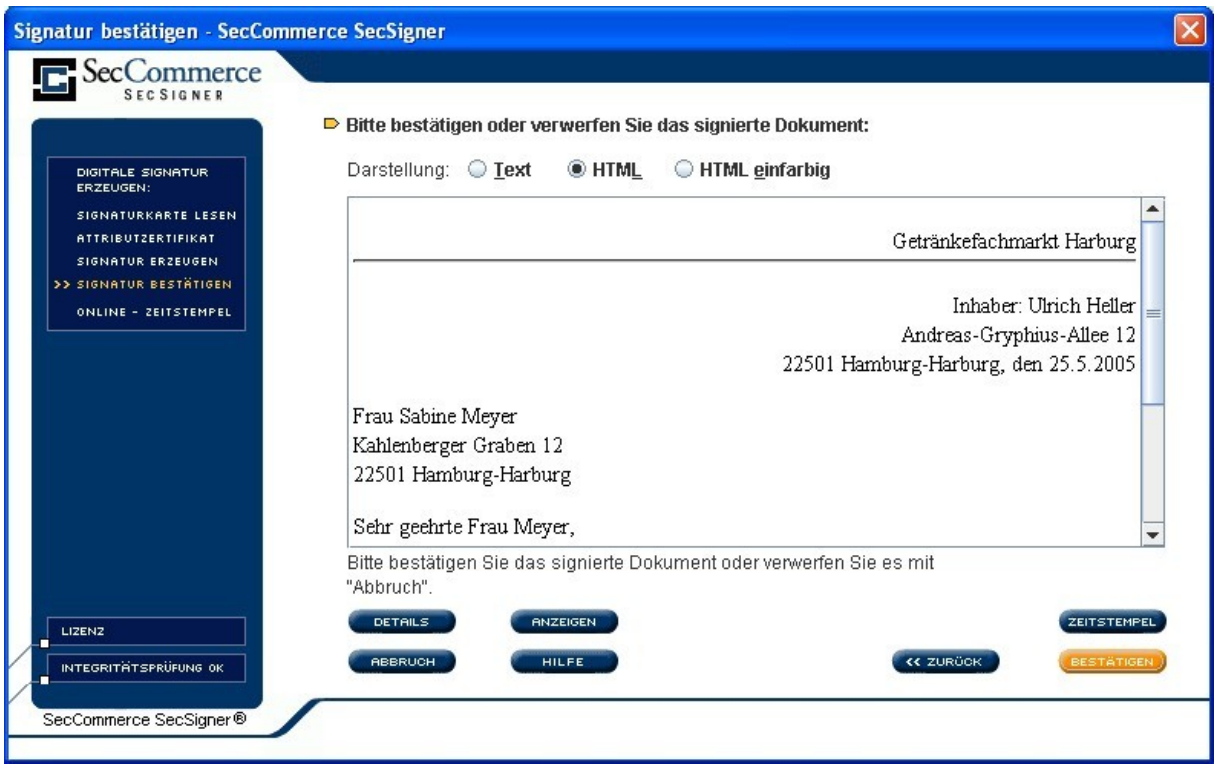
Passwort zur Entschlüsselung der PKCS#8- oder PKCS#12-Datei

seccommerce.secsigner.timestampserver.signreq=[on|off]

Entscheidet, ob die Zeitstempelanfragen signiert werden sollen.

3.4 Bestätigung der Signatur

Bestätigen Sie abschließend den Signaturvorgang mit der Option „bestätigen“:



Sie finden nach erfolgreicher Signaturerstellung im Verzeichnis des Dokuments zusätzlich die Signaturdatei gleichen Namens mit der Endung „**.pkcs7**“.

4 Weitere Funktionen des SecSigner®s

4.1 Online-Zertifikatprüfung

Während der Signaturprüfung können Sie die Zertifikatgültigkeit der verwendeten Signaturkarten testen. Es wird geprüft,

- ob die Zertifikate von den vorkonfigurierten Herausgeberzertifikaten abstammen
- ob das Gültig-Bis-Datum der Zertifikate bereits erreicht wurde
- ob der Zertifikatstatus (OSCP-Statusabfrage beim Trustcenter) OK ist.

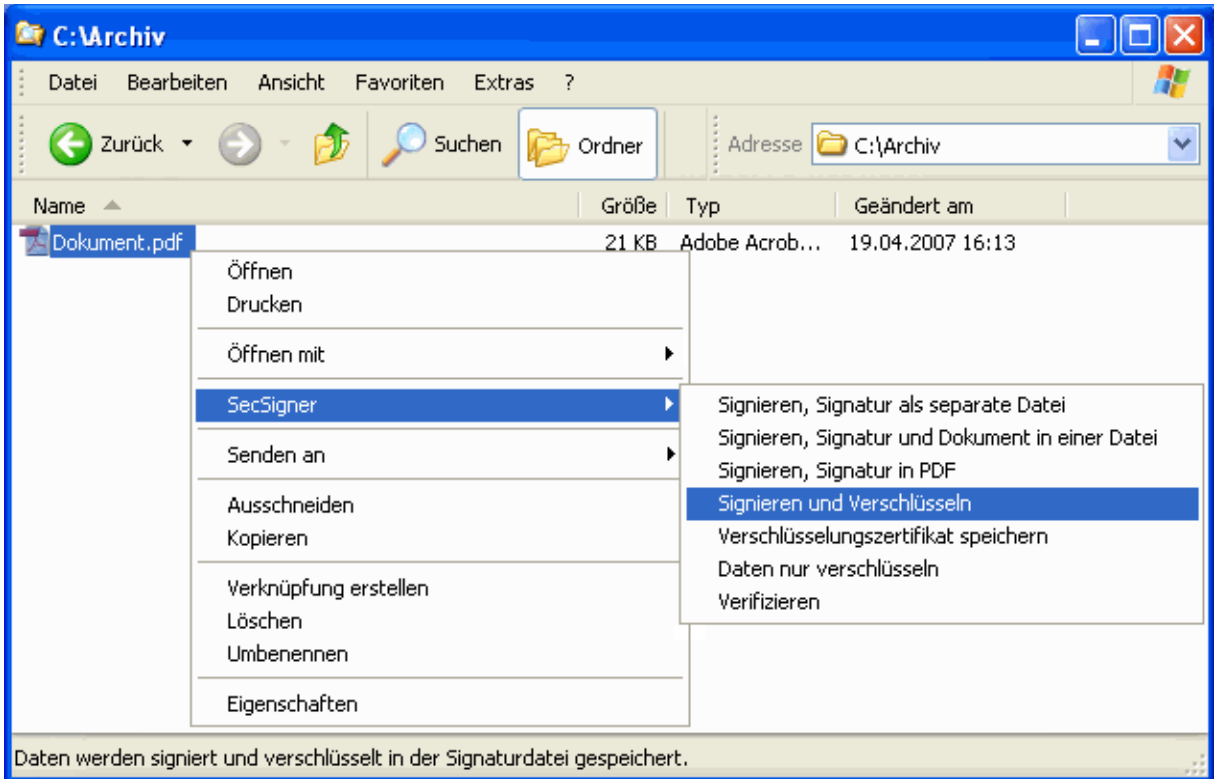
4.2 Attributzertifikat-Einbindung

Attributzertifikate sind zusätzliche Zertifikate in Dateiform, die zu einem Hauptzertifikat auf der Signaturkarte existieren können. Das Attributzertifikat kann bei der Erzeugung der Signatur in das erzeugte PKCS7-Signaturobjekt mit aufgenommen werden.

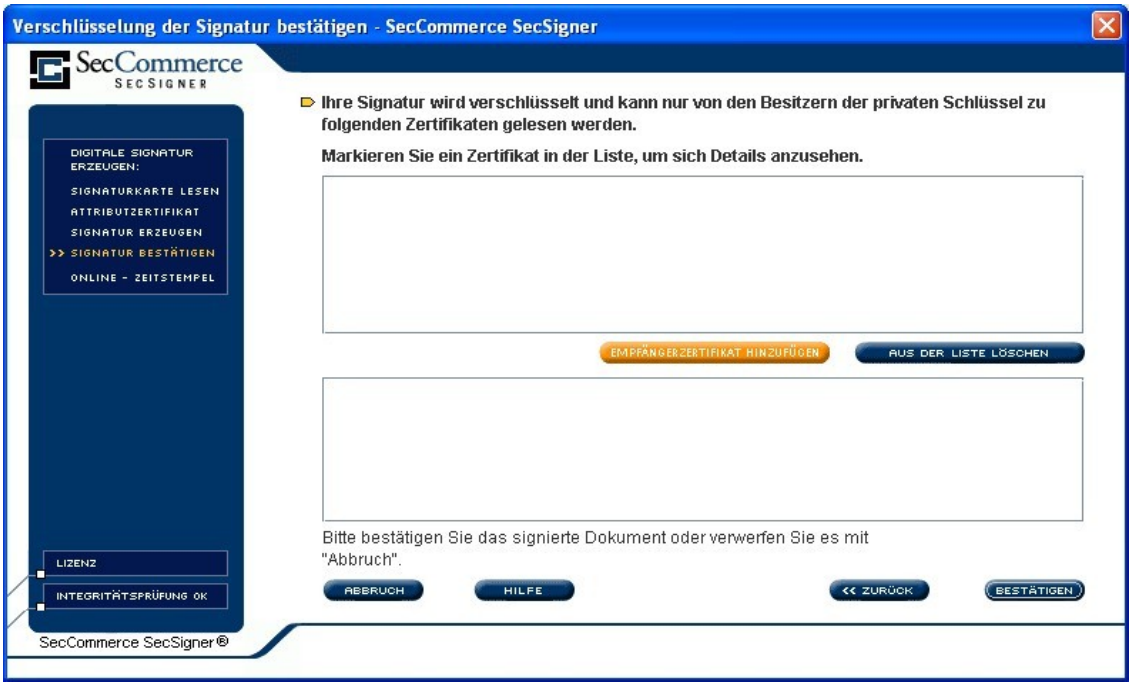
4.3 Signatur und Verschlüsselung

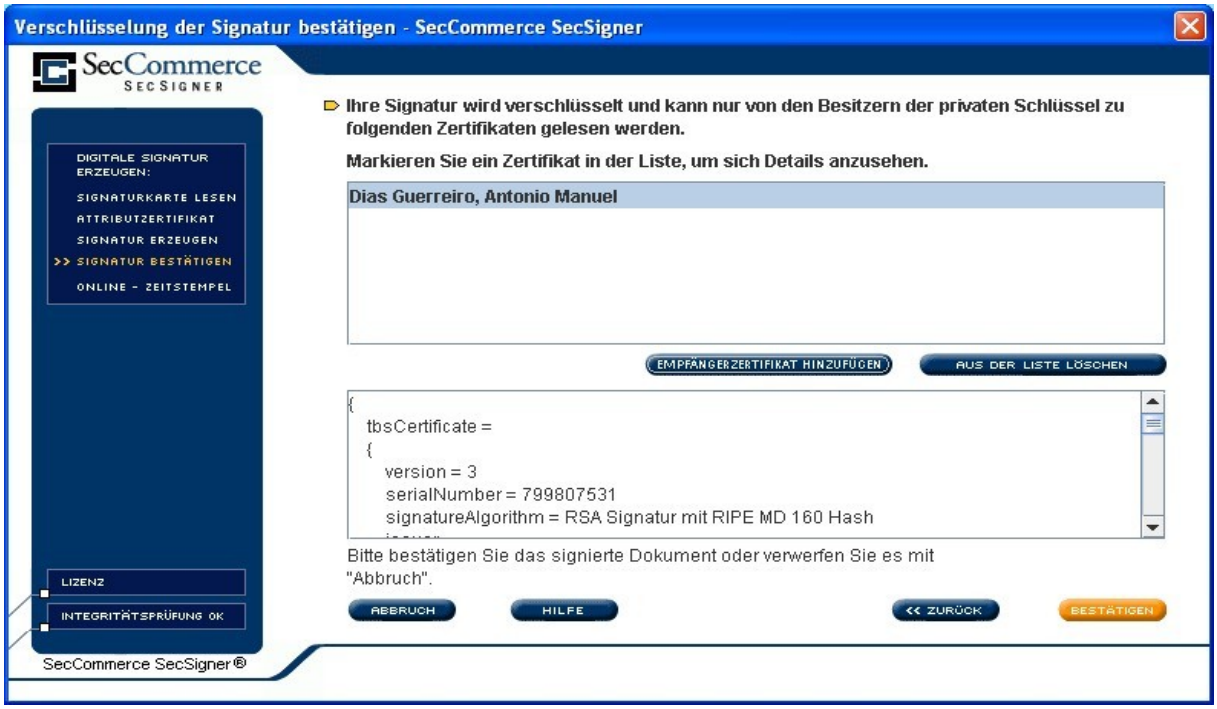
Wollen Sie eine Signatur zum Versand verschlüsseln, so benötigen Sie das ***Verschlüsselungszertifikat*** des Empfängers. (Siehe 4.5)

Der Ablauf der Signatur mit Verschlüsselung gleicht dem oben beschriebenen: Beim Klick mit der *rechten Maustaste* auf ein Dokument wählen Sie dazu die Option „SecSigner“, „Signieren und Verschlüsseln“:



Im Anschluss an Initialisierung, Anzeige und Signatur gelangen Sie zur Verschlüsselungs-Maske:



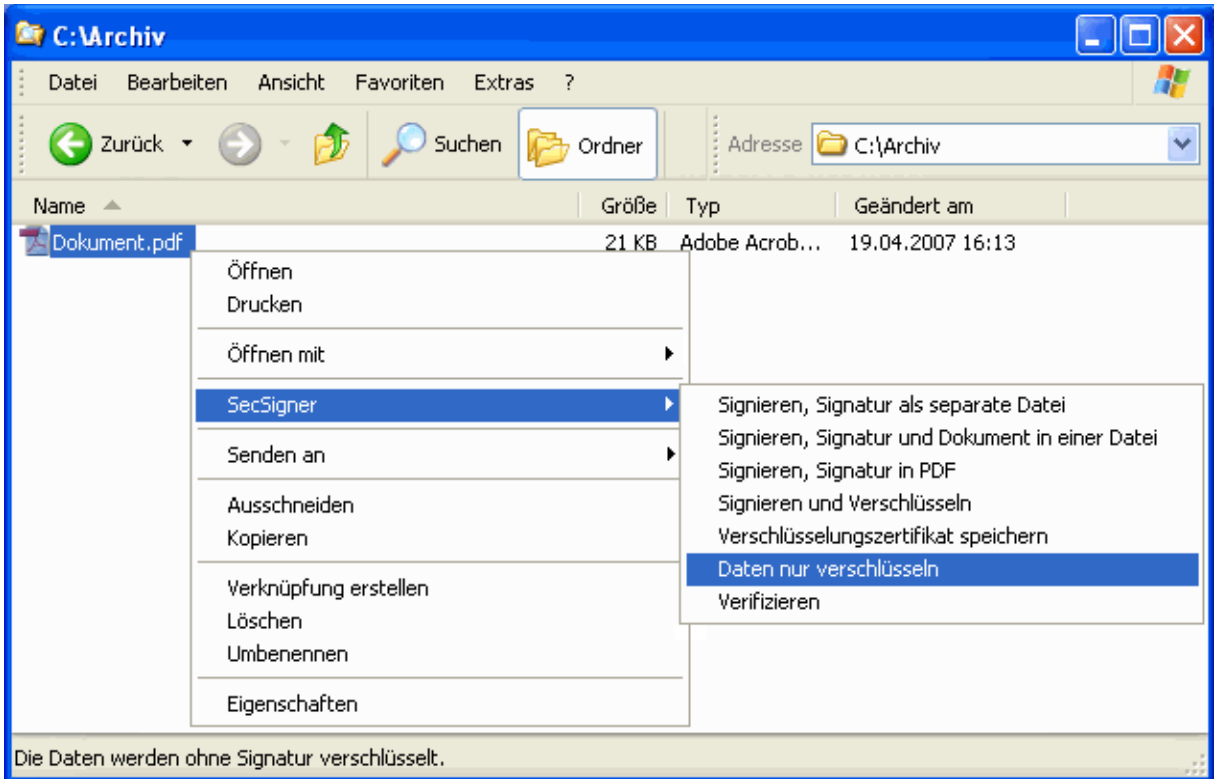


Wählen Sie den Menüpunkt „Empfängerzertifikat hinzufügen“ und laden Sie das Verschlüsselungszertifikat des Empfängers. Abschließend bestätigen Sie den Verschlüsselungsvorgang und erhalten zur Ausgangsdatei die verschlüsselte Signatur mit der Endung „.pkcs7“.

4.4 Daten nur Verschlüsseln

Wollen Sie ein Dokument verschlüsseln ohne es zu signieren, so benötigen Sie das ***Verschlüsselungszertifikat*** des Empfängers. (Siehe 4.5)

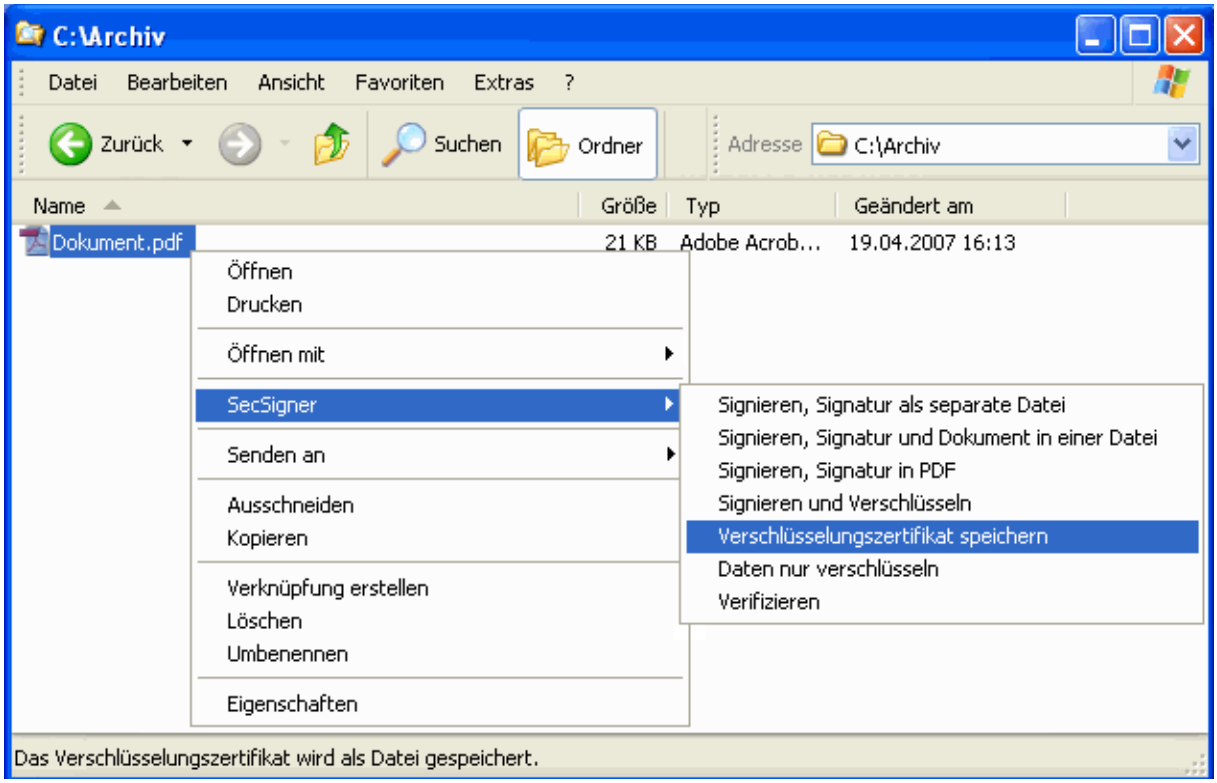
Der Ablauf der Signatur mit Verschlüsselung gleicht dem oben beschriebenen: Beim Klick mit der *rechten Maustaste* auf ein Dokument wählen Sie dazu die Option „SecSigner“, „Daten nur Verschlüsseln“:



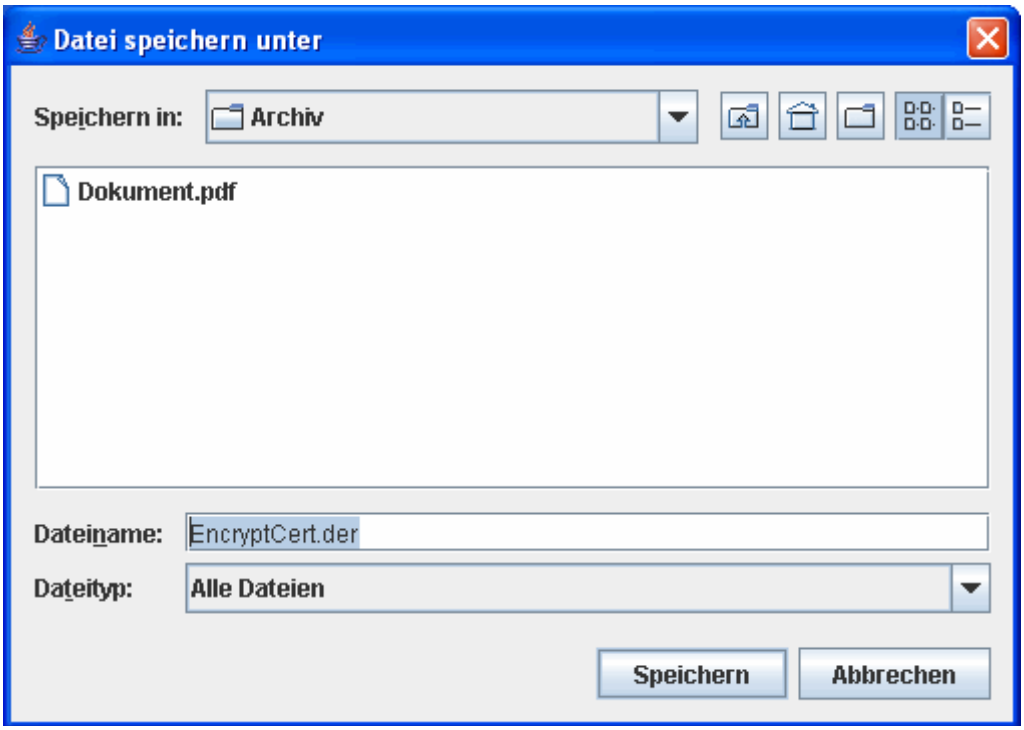
Der Verschlüsselungsvorgang ist analog zum Verschlüsselungsvorgang der Signatur. (Siehe 4.3).

4.5 Ablage des Verschlüsselungszertifikats als Datei

Wenn Sie Ihr Verschlüsselungszertifikat zur Weitergabe als Datei ablegen möchten, zeigen Sie auf ein beliebiges Dokument und wählen Sie mit der rechten Maustaste die Option „SecSigner“, „Verschlüsselungszertifikat speichern“:



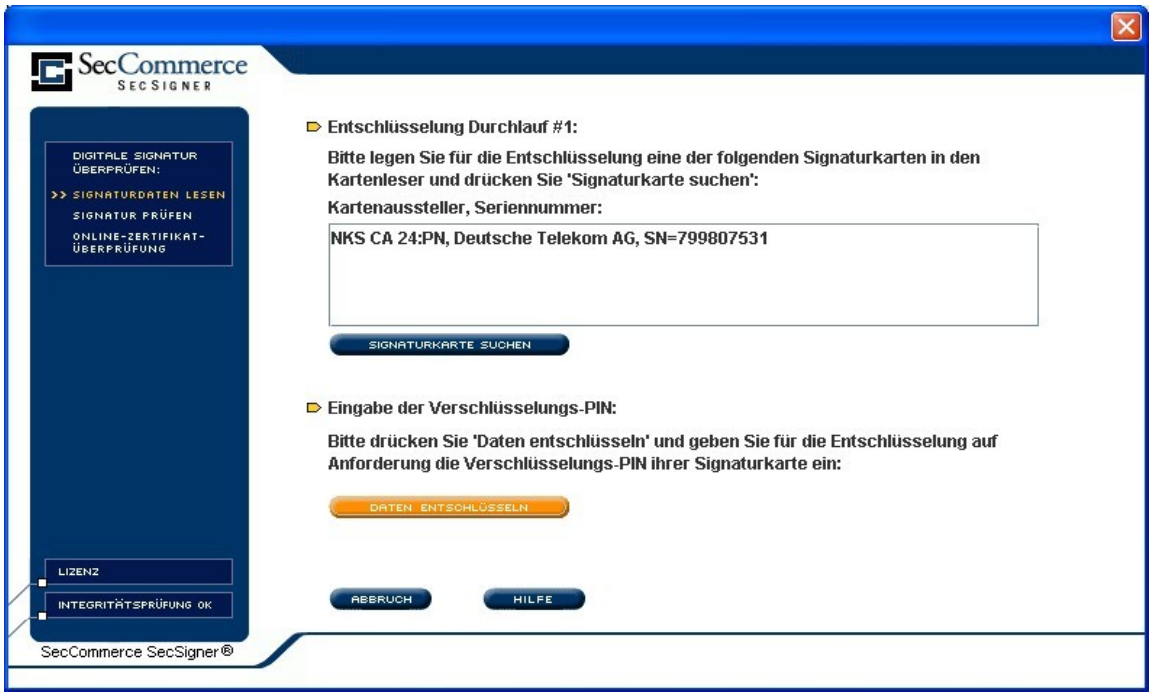
Nach der Suche Ihrer Signaturkarte haben Sie im Fileauswahldialog die Möglichkeit, Ihr Verschlüsselungszertifikat im Filesystem zu speichern:



4.6 Entschlüsselung

Erhalten Sie ein (Signatur-) Dokument, welches mit Ihrem Verschlüsselungszertifikat verschlüsselt worden ist, so wird dieses beim Öffnen im **SecSigner®** entschlüsselt.

Dazu wählen Sie nach der Initialisierung der Signaturkarte den Menüpunkt “Daten entschlüsseln”:

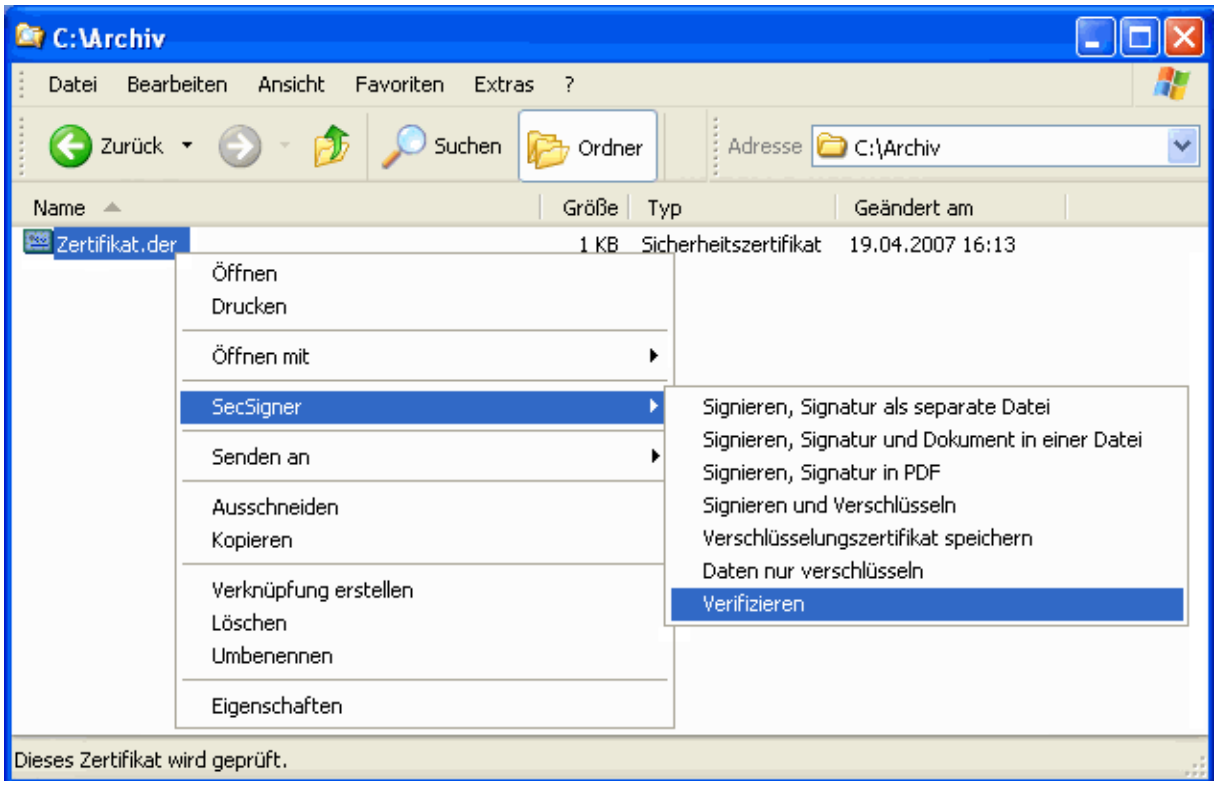


Sie werden nun aufgefordert, die PIN der Signaturkarte am Lesegerät einzugeben und verfahren anschließend entsprechend der Anleitung zur Signaturprüfung (Siehe Kapitel **2**).

Die entschlüsselten Daten werden abschließend in Ihrem Dateisystem abgelegt.

5 Zertifikatprüfung

Sie können mit dem SecSigner DER-codierte Zertifikate prüfen. Zeigen Sie dazu auf eine Zertifikat-Datei und wählen Sie mit der rechten Maustaste die Option „SecSigner“, „Verifizieren“:

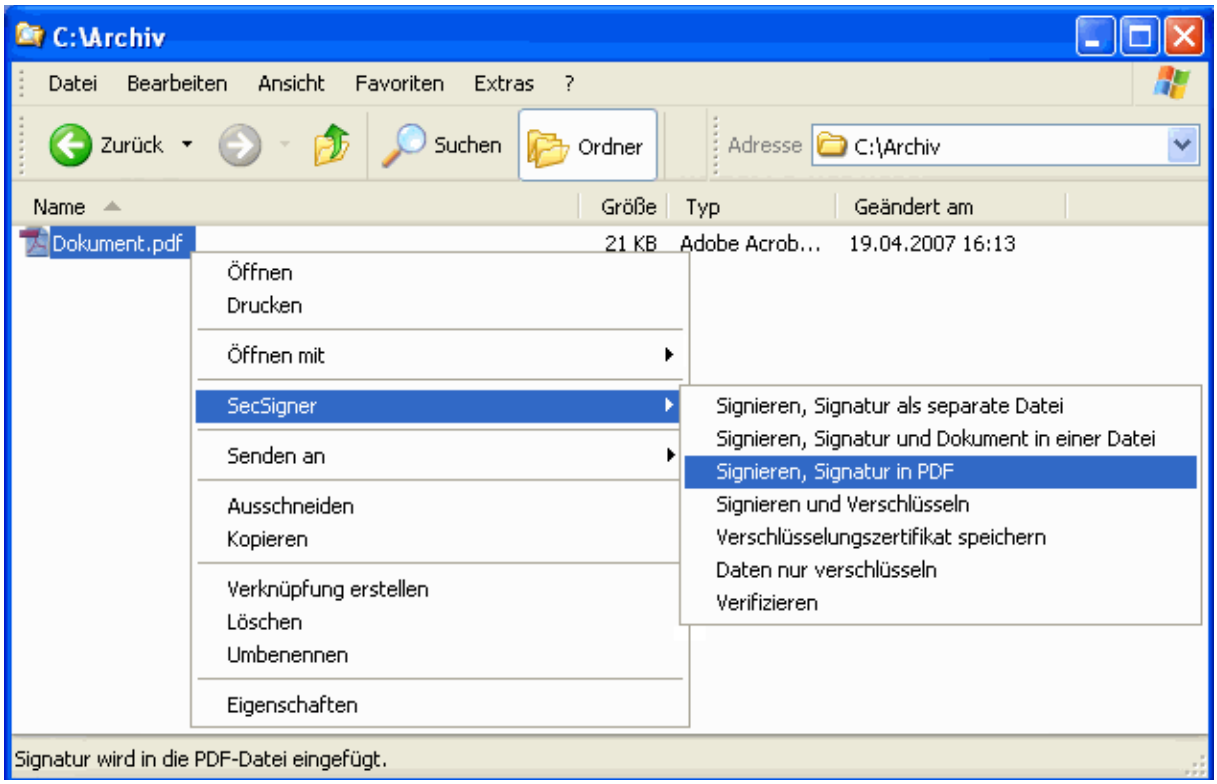


6 PDF-Signatur

SecSigner unterstützt neben dem PKCS#7-Standard auch die PDF-Signatur im Adobe Signaturformat:

6.1 PDF-Signaturen erzeugen

Um eine solche Signatur in ein PDF-Dokument aufzunehmen, zeigen Sie auf ein PDF-Dokument und wählen Sie mit der rechten Maustaste die Option „SecSigner“, „Signieren, Signatur in PDF“:



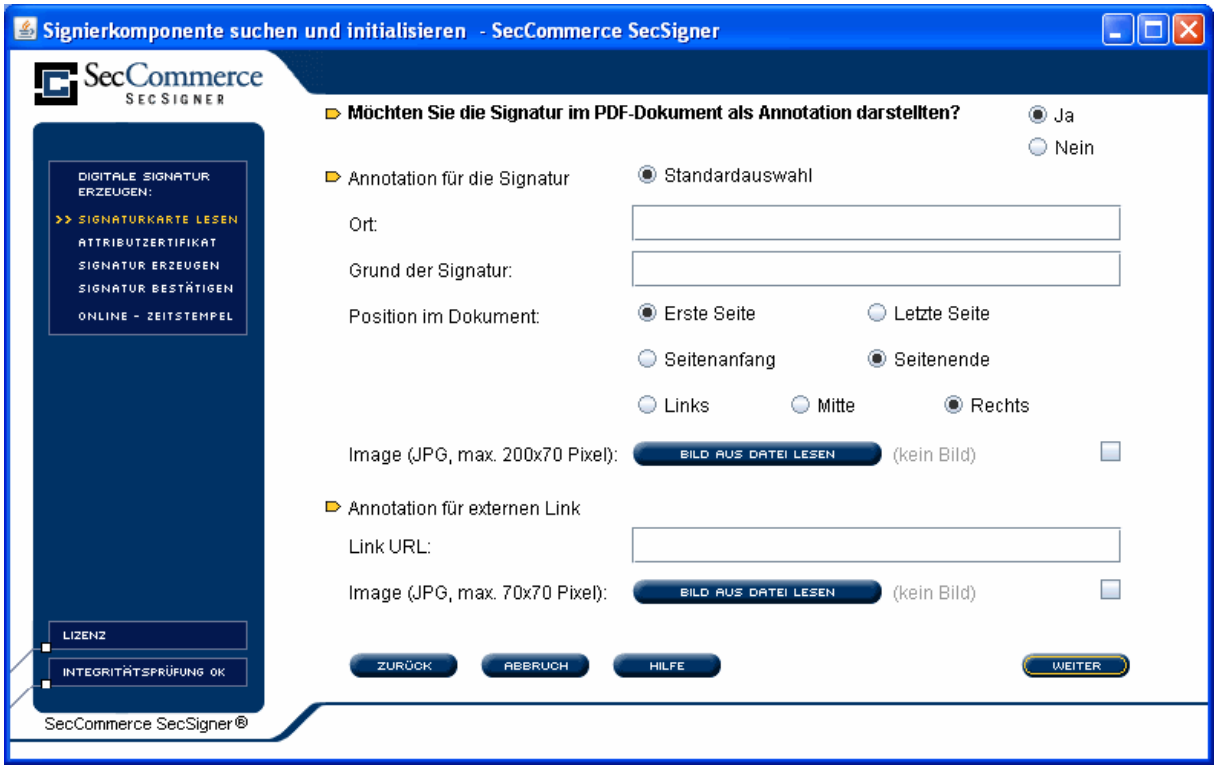
Die Signaturerzeugung wird analog zu 3.1 - 3.4 durchgeführt. Nach der Signatur des PDF-Dokumentes `'<Dateiname>.pdf'` wird die Signatur-Datei als `'<Dateiname>-signed.pdf'` in Dateisystem abgelegt.

6.1.1 Signatur-Annotation

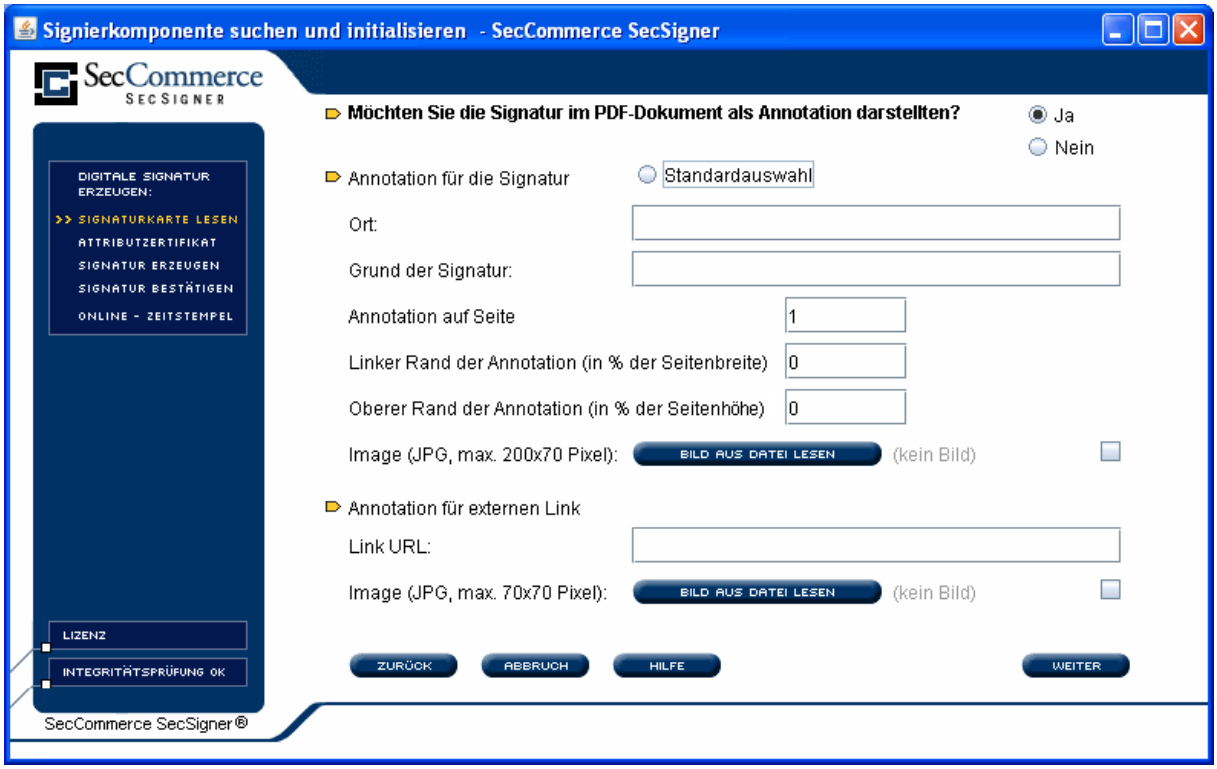
Die Signatur wird in Form einer Annotation ins PDF-Dokument eingebettet. Sie können **optional** Angaben für diese Annotation ergänzen, darunter

- Ort und Grund für die Signatur
- die Position der Annotation im Dokument
- ein **alternatives** Icon zur Annotationsdarstellung (JPG, max. 200 x 70 Pixel)
- ein Icon (JPG, max. 70 x 70 Pixel) zur Darstellung eines externen Links (z.B. auf eine Signaturanwendungskomponente zur Prüfung der Signatur) mit zugehöriger URL

Nach dem Initialisierungsdialog (vgl. Abschnitt 3.1) können Sie diese Angaben in einem eigenen Dialog hinzufügen:

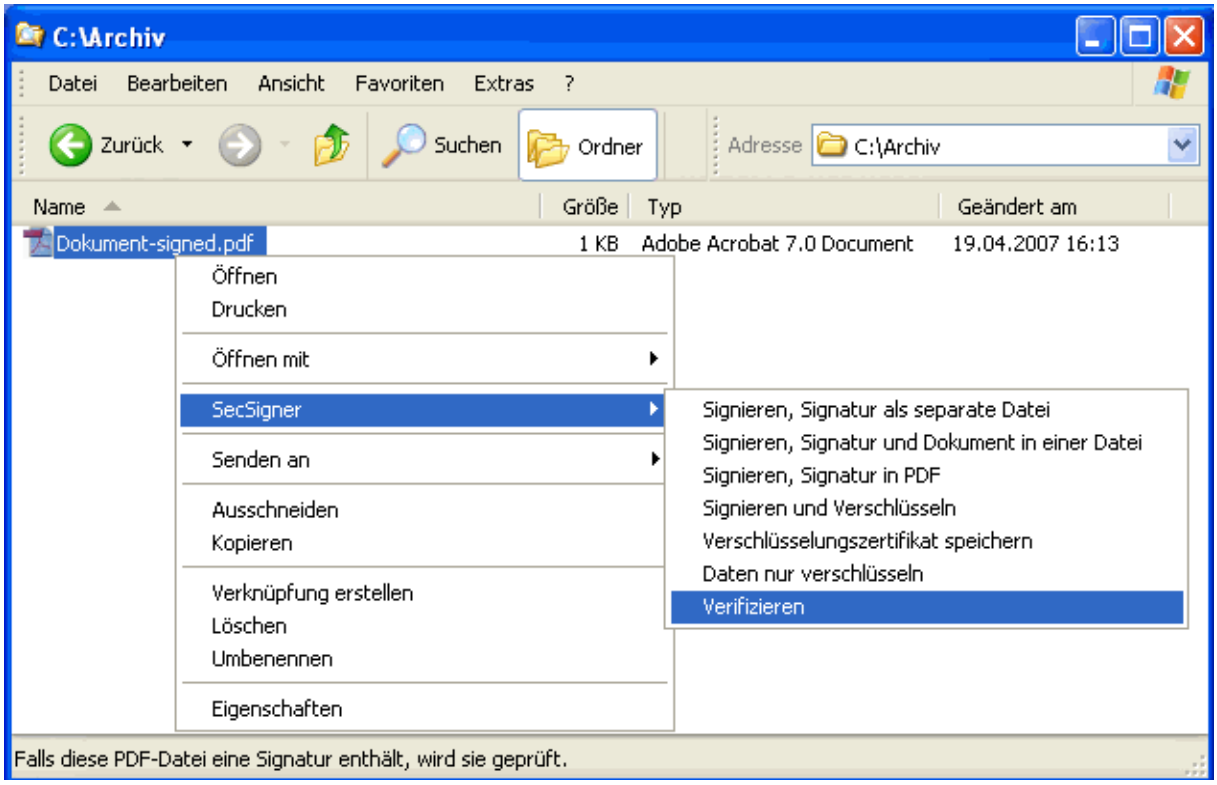


Die Positionierung kann über die 'Standardauswahl' oder nutzerspezifisch erfolgen. Schalten Sie die Option 'Standardauswahl' aus, wenn Sie die Positionierung genauer festlegen möchten:



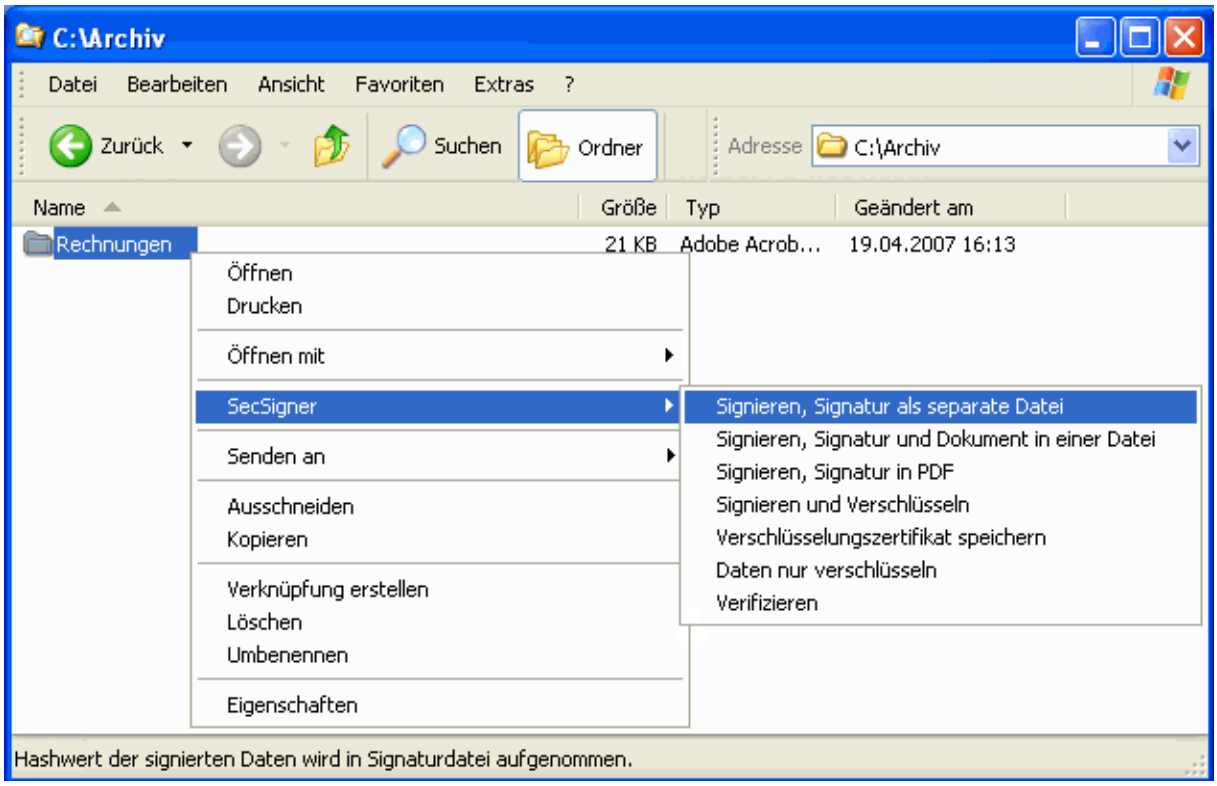
6.2 PDF-Signaturen prüfen

Um eine PDF-Signatur im Adobe Signaturformat zu prüfen, zeigen Sie auf ein PDF-Dokument und wählen Sie mit der rechten Maustaste die Option „SecSigner“, „Verifizieren“:



7 Signatur mehrerer Dateien mit einer PIN-Eingabe

Der Klick auf ein ***Verzeichnis*** mit der *rechten Maustaste* bietet wie bei einer Datei die Optionen „SecSigner“, „Signieren, Signatur als separate Datei“.



Entsprechend dem in Kapitel 3 geschilderten Vorgang können durch diesen Aufruf alle in diesem Verzeichnis befindlichen Dateien signiert werden. Im weiteren Verlauf des Signaturvorgangs können dabei alle Dateien angezeigt werden:

8 Firewalls und Online-Zertifikatprüfungen/Zeitstempelanfragen

8.1 Informationen für OCSP-Anfragen

SecSigner® bekommt die Informationen für eine Anfrage (Port, Adresse, Protokoll) aus seiner Properties-Datei. Die **Zuordnung** zwischen Benutzerzertifikat und OCSP-Adresse erfolgt **über das CA-Zertifikat**.

8.2 OCSP-Anfragen

Bei einer OCSP-Anfrage wird ein Socket zum Server geöffnet und dann **OCSP über HTTP** gesendet.

Anmerkung: Der OCSP-Dienst des Anbieters *D-Trust* sendet direkt an Server und Port.

8.3 Firewalls

Wenn eine Firewall die direkte Verbindung verhindert, muss im Internet-Explorer ein Proxy konfiguriert sein, der mittels CONNECT die Verbindung aufbaut. SecSigner® liest die **Proxy-Einstellungen**, welche der Internet-Explorer in der **Registry** gespeichert hat.

8.3.1 Manuelle Proxy-Konfiguration

Daneben gibt es die Möglichkeit, einen festen Proxy für SecSigner® einzustellen.
Dazu muss eine Datei

\Dokumente und Einstellungen\<username>\.seccommerce**scProxy.conf**

mit diesem Inhalt erstellt werden:

PROXY [IP-Adresse]:[Port]

Es können auch mehrere Proxies konfiguriert werden:

PROXY [IP-Adresse1]:[Port1]; [IP-Adresse2]:[Port2]; [IP-Adresse3]:[Port3]
usw.

Das **Online Certificate Status Protocol** (OCSP) ist ein Internet-Protokoll, dass es Clients ermöglicht, den Status von X.509-Zertifikaten abzufragen.

Es gibt Proxies, die nur TLS-Verbindungen über die CONNECT-Methode erlauben und die Verbindung wieder *schließen*, wenn sie feststellen, dass *kein TLS* benutzt wird.

8.4 Automatische OCSP-Abfrage

OCSP-Abfragen können automatisch gestartet werden. Dazu dient folgende Einstellungen in der Konfigurationsdatei 'secsignersigg300.properties':

seccommerce.secsigner.ocspmandatory=<on|off>

9 Impressum

Hersteller des **SecSigner**® und verantwortlich für diese Dokumentation:

SecCommerce Informationssysteme GmbH
Obenhauptstrasse 5
22335 Hamburg Deutschland
Tel. +49 40 53052-0
Fax. +49 40 53052-100
E-Mail: info@seccommerce.de
Web: www.seccommerce.de