

Produktdokumentation



Urheberrechtshinweise

Die in dieser Dokumentation beschriebene Software wird auf Grund eines Lizenzvertrages bereitgestellt und darf nur dieser Vereinbarung entsprechend verwendet werden.

Ohne vorherige schriftliche Genehmigung der IT Solution GmbH, darf diese Dokumentation weder ganz noch teilweise kopiert, reproduziert, übersetzt oder in einem elektronischen Medium veröffentlicht werden.

Gültigkeitsdauer

Der Inhalt dieses Handbuches gilt von Version 3.0 für Windows XP/Vista/7 bis zur Veröffentlichung einer neuen Version der Software und somit dieses Handbuches im Internet.



Inhaltsverzeichnis

1	<i>IT Solution GmbH</i>	3
2	<i>Sicherheitshinweise</i>	4
3	<i>Systemvoraussetzungen</i>	5
3.1	Hardware	5
3.2	Betriebssystem	5
3.3	Unterstützte Smartcards	5
3.4	Kartenlesegeräte	5
4	<i>Installation</i>	6
4.1	Download aus dem Internet	6
4.2	CD	6
4.3	Installationsschritte	6
5	<i>Deinstallation</i>	15
6	<i>Signieren</i>	15
7	<i>Verifizieren</i>	17
8	<i>Verschlüsseln</i>	18
9	<i>Entschlüsseln</i>	20
10	<i>Acrobat</i>	21
11	<i>Optionen</i>	23
12	<i>Setup Kommandozeilenparameter</i>	24
13	<i>Uninstaller Kommandozeilenparameter</i>	28
14	<i>Beispiele silent setup</i>	29
15	<i>Wörterbuch</i>	30

1 IT Solution GmbH

IT Solution ist Anbieter von Standardsoftware für die elektronische Signatur mit dem speziellen Fokus auf die sichere elektronische Signatur nach dem österreichischen und dem deutschen Signaturgesetz.

Gegründet im Jahre 1998, hat sich das Unternehmen sowohl auf Desktop-Anwendungen für den einzelnen Arbeitsplatz als auch auf die Entwicklung von Server-Komponenten für den unternehmensweiten Einsatz von Public Key Infrastructure (PKI) Technologien spezialisiert.

Für die effiziente Umsetzung von PKI Integrationsaufgaben stellt IT Solution Basistechnologien für die elektronische Unterschrift sowie Entwicklungs-SDKs zur Verfügung.

Seit der Ausrollung von Signaturkarten durch Banken, Kreditkartenunternehmen und Sozialversicherer trägt IT Solution durch gezielte Softwareschulungen und Seminare zur Umsetzung der elektronischen Signatur in Österreich bei.

Die elektronische Signatur ermöglicht den Einsatz elektronischer Dokumente überall dort, wo heute eine Unterschrift auf Papier notwendig ist.

IT Solution stellt ihren Kunden die dafür notwendige Basistechnologie, stets auf dem neuesten Stand der Technik, zur Verfügung.

Der Einsatz von Standardapplikationen ermöglicht die rasche Realisierung der elektronischen Signatur in Ihrem Unternehmen, der Kostenvorteil ist kurzfristig spürbar.

Durch individuell adaptierbare Standardkomponenten mit offenen Schnittstellen ist die Integration der elektronischen Signatur in die bestehende Systemumgebung unter Einbeziehung von vorhandenen Applikationen möglich. So hilft IT Solution Ihnen und Ihren Kunden, Effizienzsteigerungspotenziale aus dem Einsatz der elektronischen Signatur rasch und effizient zu nutzen.

2 Sicherheitshinweise

Neben den hard- und softwaretechnischen Sicherheitsmaßnahmen sind bei der Verwendung digitaler Signaturen auch organisatorische Vorkehrungen zu treffen:

- Ihr Arbeitsbereich bzw. der Standort Ihres Personal Computers ist so aufzubauen und einzurichten, dass ein aktives oder passives Ausspähen Ihres Nutzersystems nicht möglich ist.
- Sowohl der PC und damit die Signaturerstellungsoftware trustView als auch die verwendeten sicheren Signaturerstellungseinheiten müssen vor einer unbefugten Nutzung durch Dritte geschützt sein:
- Passwort für PC
- Chipkarten nicht offen herumliegen lassen, sondern einsperren, einstecken, etc.
- Chipkarte mit der gleichen Sorgfalt behandeln wie Kredit- oder Bankomatkarten
- PIN weder notieren noch in der Nähe von Signaturerstellungseinheit bzw. Kartenleser deponieren
- Sowohl Passwort als auch PIN sind nur so lange sicher, als sie nicht ausgespäht oder verraten werden. Die PIN wird ausschließlich von Ihnen zur Signatur benötigt und dient keinesfalls zu Servicezwecken:

! *Sie dürfen die PIN auch **n i e m a l s** Mitarbeitern Ihres Trustcenters, des Soft- oder Hardwareherstellers bekannt geben.*

- Ein aktiver Schutz vor Viren oder anderen bösartigen Programmen muss gegeben sein:
Eine Überprüfung der Software mittels Virenschanner (z.B. McAfee Antivirus, Dr.Solomon Antivirus, Kaspersky Antivirus, Norton Antivirus – URLs oder nützliche Links dazu finden Sie im Literaturverzeichnis) vor der Installation und danach in regelmäßigen Abständen wird dringend empfohlen. Jedenfalls sollte eine Prüfung durchgeführt werden,
- wenn abnormes Verhalten bei der Ausführung von Programmen auftritt;
- nach Installation von Software;
- nach jeder Internetanwendung, also wenn Sie am PC z. B. E-Mails, Internet-Browser, Downloads u. dgl. verwendet haben;
- jedenfalls aber vor der Verwendung von trustView
- Vorbeugend ist außerdem die Installation einer Firewall zu empfehlen.
- Die lokale Uhrzeit Ihres PCs muss der tatsächlichen lokalen Uhrzeit entsprechen. Konsultieren Sie dazu bitte die Dokumentation Ihres PC-Betriebssystems.
- Ihre Grafikkarte muss auf eine Farbtiefe von mindestens 15 Bit (32768 Farben) eingestellt sein. Konsultieren Sie dazu bitte das Handbuch zu Ihrer Grafikkarte.

! *Ist trustDesk professional nicht gestartet und greifen Sie auf Software zu, die die Bürgerkartensoftware voraussetzt, kann der Browser die Internet Seite nicht anzeigen. Kontrollieren Sie in diesem Fall, ob die Software gestartet ist: Die Goldene Chipkarte muss rechts unten in der Taskleiste angezeigt sein.*

3 Systemvoraussetzungen

3.1 Hardware

	Empfohlen	Minimum
Mainboard	Pentium III Klasse	Pentium Klasse
Ram	128 MB oder größer	Minimum 16 MB
CPU	Prozessor ab 500 MHz	Ab Pentium 60
Grafikkarte	1024x768 16Bit Farbtiefe	640x480 15 Bit Farbtiefe
Harddisk	5 GB Festplatte oder größer	Minimum 200 MB Festplatte
CD-Laufwerk	Standard	Standard

3.2 Betriebssystem

Windows XP, Windows Vista, Windows 7

3.3 Unterstützte Smartcards

Karte	System
A-Trust A-Sign Premium SmartCard	ACOS / ACOS4
A-Trust Trust sign SmartCard	StarCOS 2.3
A-Trust Trust mark Token SmartCard	StarCOS 2.3
Österreichische e-Card	StarCOS 3.x (bis e-cards der dritten Generation)
Österreichische o-Card	StarCOS 3.x
D-Trust	Siemens CardOS 4.3b
D-Trust MS	Siemens CardOS 4.3b
Estnische EstEID Karte	Micardo 2.1
Italienische Karte	
Belgische Karte	
Finnische Karte	

3.4 Kartenlesegeräte

Empfohlen	Minimum
Reiner SCT Cyberjack® e-com USB	Alle Lesegeräte welche Karten im üblichen Smartcard Format ISO 7816 ID-1 (Scheckkarten Format) einlesen können, und per PC/SC und/oder CT-API Protokoll angesteuert werden können.
Reiner SCT Cyberjack® e-com plus USB	
Reiner SCT Cyberjack® secoder USB	
Reiner SCT Cyberjack® biometric USB	
Cherry ST-1210 SmartTerminal	
Cherry Smartboard G83-6744LUZxx und G83-6744LBZxx	

4 Installation

Um die Software trustDesk professional fehlerfrei installieren zu können, müssen Sie auf dem System, auf dem installiert werden soll, über Administratorenrechte verfügen. Sollte dies nicht der Fall sein, loggen Sie sich bitte mit einem Administratorenaccount ein oder wenden SIE sich an ihren Systemadministrator um Hilfe.

! *Dies gilt auch für die Installation der Online-Updates*

4.1 Download aus dem Internet

trustDesk professional kann von der Webseite www.itsolution.at kostenfrei für 60 Tage bezogen werden.

Die Dauer des Downloads ist in erster Linie von der Internetverbindung, über die die Software geladen wird, abhängig und kann einige Minuten in Anspruch nehmen. Die zu installierenden Dateien werden in das Verzeichnis für temporäre Daten des angemeldeten Benutzers kopiert. Der Aufruf des Installationsprogramms startet nach dem Download selbstständig und kann nicht abgebrochen werden. Die Installation selbst kann nach jedem Schritt entweder unterbrochen oder abgebrochen werden.

4.2 CD

trustDesk professional wird in Ausnahmefällen auch auf CD ausgeliefert. Diese muss in ein angeschlossenes CD-Laufwerk eingelegt werden.

 Startet die CD nicht automatisch, muss die Datei trustDesk professional.exe per Maus mit einem Doppelklick aufgerufen werden.

4.3 Installationsschritte

4.3.1 Download

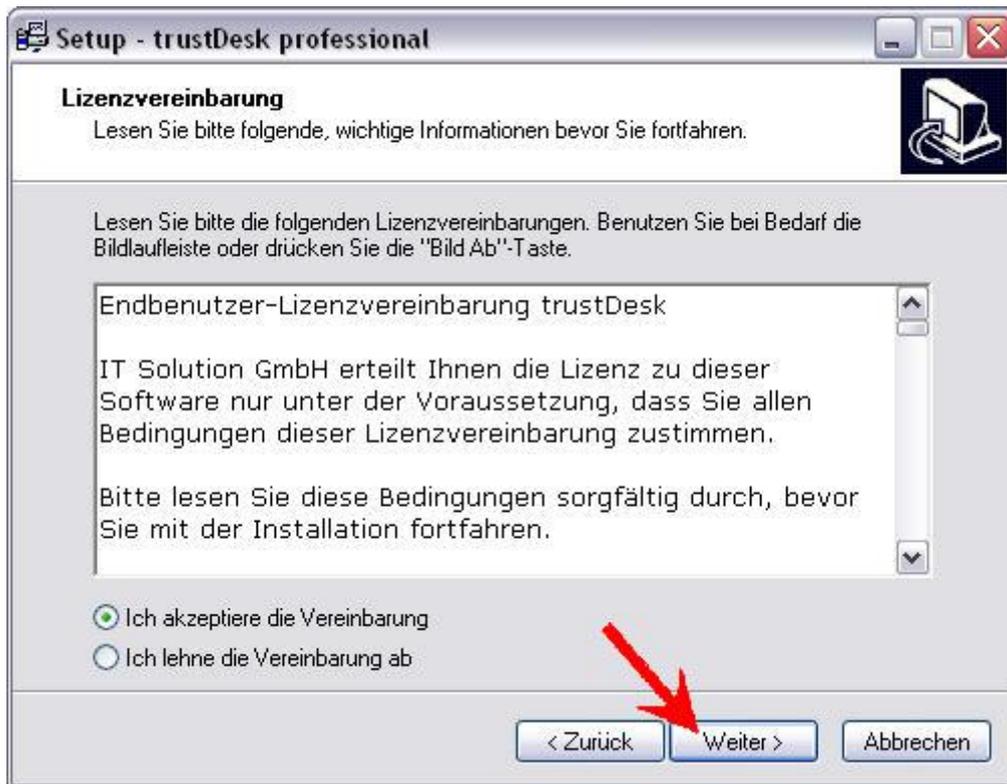


! *Sprache und Buttonbeschriftung sind abhängig von der Betriebssystemsprache*

Soll der Installationsvorgang sofort gestartet werden, klicken Sie auf RUN (Ausführen)

4.3.2 Lizenzvereinbarung

Die Lizenzvereinbarung ist die Basis für die Nutzung von trustDesk professional. Lesen Sie die Lizenzvereinbarungen bitte aufmerksam durch.



Auswahlfelder

Name	Gültige Werte	Bedeutung
Ich akzeptiere die Vereinbarung	<input checked="" type="radio"/>	Sie erklären sich mit den Bedingungen der Lizenzvereinbarung einverstanden..
Ich lehne die Vereinbarung ab	<input type="radio"/>	Sie sind nicht mit den Bedingungen der Vereinbarung einverstanden. Die Software kann nicht installiert werden.

Buttons

Name	Bedeutung
<input type="button" value=" < Zurück"/>	Anzeige der vorherigen Maske. Haben Sie auf dieser Maske bereits Eingaben gemacht, werden diese gespeichert.
<input type="button" value=" Weiter >"/>	Dieser Button wird nur aktiv, wenn Sie Ich akzeptiere die Vereinbarung gewählt haben. Die Installation wird fortgesetzt.
<input type="button" value=" Abbrechen"/>	Abbruch des Installationsvorganges → Warnmeldung <p><i>Das Setup ist noch nicht abgeschlossen. Wenn Sie jetzt beenden, wird das Programm nicht installiert.</i></p> <p><i>Sie können das Setup zu einem späteren Zeitpunkt nochmals ausführen, um die Installation zu vervollständigen. Setup verlassen?</i></p> <p><i>Mit der Auswahl Ja wird die Installation abgebrochen, mit der Auswahl Nein wird die Warnmeldung ausgeblendet und Sie können die Installation fortsetzen.</i></p> <p>Mit der Auswahl Ja auf der Folgemaske wird die Installation abgebrochen, mit der Auswahl Nein</p>

wird die Warnmeldung ausgeblendet und Sie können die Installation fortsetzen.

4.3.3 Willkommen

Nach der Entscheidung den Lizenzvertrag zu akzeptieren beginnen Sie den Installationsvorgang mit dem Installationsassistenten. Der Installationsassistent gibt Ihnen wichtige Hinweise zur Installation.

Entscheiden Sie, ob Sie die Installation automatisch oder benutzerdefiniert durchführen wollen.

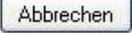


Eingabefelder

Name	Gültige Werte	Bedeutung
automatisch		Der Installationsvorgang startet unmittelbar nachdem Sie diese Maske mit Weiter verlassen. Sie installieren mit den vorgegebenen Installationsparametern. der Fortschritt wird in einem Balken angezeigt.
benutzerdefiniert		Sie legen die Installationsparameter auf den folgenden Masken fest. Es sind jene Standardwerte vorgegeben

Buttons

Name	Bedeutung
	Anzeige der vorherigen Maske. Haben Sie auf dieser Maske bereits Eingaben gemacht, werden diese gespeichert.
	Anzeige der nächsten Maske. Bei der automatischen Installation wird sofort mit dem Kopieren der notwendigen Daten begonnen. Bei der benutzerdefinierten Installation gelangen Sie auf Folgemasken, wie unten abgebildet.

	<p>Abbruch des Installationsvorganges → Warnmeldung</p> <p><i>Das Setup ist noch nicht abgeschlossen. Wenn Sie jetzt beenden, wird das Programm nicht installiert.</i></p> <p><i>Sie können das Setup zu einem späteren Zeitpunkt nochmals ausführen, um die Installation zu vervollständigen. Setup verlassen?</i></p> <p><i>Mit der Auswahl Ja wird die Installation abgebrochen, mit der Auswahl Nein wird die Warnmeldung ausgeblendet und Sie können die Installation fortsetzen.</i></p> <p>Mit der Auswahl Ja auf der Folgemaske wird die Installation abgebrochen, mit der Auswahl Nein wird die Warnmeldung ausgeblendet und Sie können die Installation fortsetzen.</p>
---	---

Die automatische Installation erfolgt ohne Parameterangabe nach vorgegebenen Einstellungen.

In der benutzerdefinierten Installation kann der Benutzer die Installationsparameter selbst definieren.



4.3.4 Zielordner

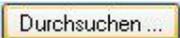
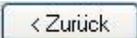
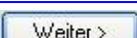
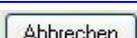
Der Zielordner gibt jenen Ort auf Ihrem Computer an, an dem die Daten für trustDesk professional gespeichert werden. Das Standardverzeichnis sehen Sie in der Maske abgebildet.



Eingabefelder

Name	Gültige Werte	Bedeutung
Programmdateien	Vorhandenes Verzeichnis	In dieses Verzeichnis werden die Programmdateien von trustDesk professional installiert. Ist das angegebene Verzeichnis nicht vorhanden, wird es angelegt.

Buttons

Name	Bedeutung
	Auswahl des Pfades für die Installationsdateien mithilfe des Windows Browsers
	Anzeige der vorherigen Maske. Haben Sie auf dieser Maske bereits Eingaben gemacht, werden diese gespeichert.
	Anzeige der nächsten Maske
	<p>Abbruch des Installationsvorganges → Warnmeldung</p> <p><i>Das Setup ist noch nicht abgeschlossen. Wenn Sie jetzt beenden, wird das Programm nicht installiert.</i></p> <p><i>Sie können das Setup zu einem späteren Zeitpunkt nochmals ausführen, um die Installation zu vervollständigen. Setup verlassen?</i></p> <p><i>Mit der Auswahl Ja wird die Installation abgebrochen, mit der Auswahl Nein wird die Warnmeldung ausgeblendet und Sie können die Installation fortsetzen.</i></p> <p>Mit der Auswahl Ja auf der Folgemaske wird die Installation abgebrochen, mit der Auswahl Nein wird die Warnmeldung ausgeblendet und Sie können die Installation fortsetzen.</p>

4.3.5 Startmenü Ordner auswählen

trustDesk professional kann über **Start – Alle Programme** aufgerufen werden. Hier legen Sie fest, wie der Ordner in Ihrem Programmeverzeichnis heißen soll.



Eingabefelder

Name	Gültige Werte	Bedeutung
Startmenü Ordner	alphanumerisch	Unter dieser Programmgruppe können Sie trustDesk professional starten.
	Leer	Ist dieses Feld leer, muss die Checkbox Keinen Ordner im Startmenü erstellen aktiviert sein. Ist dieses Feld leer und die Checkbox nicht aktiviert, erhalten Sie die Warnmeldung <i>Sie haben keinen Ordernamen eingegeben, wollen Sie keinen Eintrag im Startmenü.</i> Mit Auswahl Ja wird die Checkbox automatisch aktiviert, mit Auswahl Nein wird die Meldung ausgeblendet und Sie können den Namen des Startmenüordners angeben.
Keinen Ordner im Startmenü erstellen	<input type="checkbox"/>	Es soll ein Startmenü Eintrag erfolgen. Das Feld Startmenü Ordner muss ausgefüllt sein
	<input checked="" type="checkbox"/>	Unabhängig davon, ob im Feld Startmenü Ordner ein Eintrag steht wird kein Startmenü Eintrag gemacht.

Buttons

Name	Bedeutung
<input type="button" value="Durchsuchen ..."/>	Auswahl eines bestehenden Startmenü Ordners
<input type="button" value=" < Zurück"/>	Anzeige der vorherigen Maske. Haben Sie auf dieser Maske bereits Eingaben gemacht,

	werden diese gespeichert.
<input type="button" value="Weiter >"/>	Anzeige der nächsten Maske
<input type="button" value="Abbrechen"/>	<p>Abbruch des Installationsvorganges → Warnmeldung</p> <p><i>Das Setup ist noch nicht abgeschlossen. Wenn Sie jetzt beenden, wird das Programm nicht installiert.</i></p> <p><i>Sie können das Setup zu einem späteren Zeitpunkt nochmals ausführen, um die Installation zu vervollständigen. Setup verlassen?</i></p> <p><i>Mit der Auswahl Ja wird die Installation abgebrochen, mit der Auswahl Nein wird die Warnmeldung ausgeblendet und Sie können die Installation fortsetzen.</i></p> <p>Mit der Auswahl Ja auf der Folgemaske wird die Installation abgebrochen, mit der Auswahl Nein wird die Warnmeldung ausgeblendet und Sie können die Installation fortsetzen.</p>

4.3.6 Symbole

Der Start von trustDesk professional kann auch über Symbole auf dem Desktop oder in der Schnellstartleiste erfolgen. Hier legen Sie fest, ob diese Symbole automatisch erstellt werden.



Eingabefelder

Name	Gültige Werte	Bedeutung
Desktop Symbol anlegen	<input type="checkbox"/>	Es wird kein Symbol am Desktop angelegt.
	<input checked="" type="checkbox"/>	Es wird ein Symbol am Desktop angelegt

Symbol in der Schnellstartleiste anlegen	<input type="checkbox"/>	Es wird kein Symbol in der Schnellstartleiste angelegt
	<input checked="" type="checkbox"/>	Es wird kein Symbol in der Schnellstartleiste angelegt

Buttons

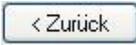
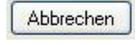
Name	Bedeutung
<input type="button" value=" < Zurück"/>	Anzeige der vorherigen Maske. Haben Sie auf dieser Maske bereits Eingaben gemacht, werden diese gespeichert.
<input type="button" value=" Weiter >"/>	Anzeige der nächsten Maske
<input type="button" value=" Abbrechen"/>	<p>Abbruch des Installationsvorganges → Warnmeldung</p> <p><i>Das Setup ist noch nicht abgeschlossen. Wenn Sie jetzt beenden, wird das Programm nicht installiert.</i></p> <p><i>Sie können das Setup zu einem späteren Zeitpunkt nochmals ausführen, um die Installation zu vervollständigen. Setup verlassen?</i></p> <p><i>Mit der Auswahl Ja wird die Installation abgebrochen, mit der Auswahl Nein wird die Warnmeldung ausgeblendet und Sie können die Installation fortsetzen.</i></p> <p>Mit der Auswahl Ja auf der Folgemaske wird die Installation abgebrochen, mit der Auswahl Nein wird die Warnmeldung ausgeblendet und Sie können die Installation fortsetzen.</p>

4.3.7 Zusammenfassung

Alle Angaben, die Sie auf den vergangenen Masken angegeben haben, werden nochmals auf einen Blick zusammengefasst. Sind Sie mit einer Auswahl nicht zufrieden, können Sie durch Klicken auf **Zurück** Ihre Angaben jederzeit verändern.



Buttons

Name	Bedeutung
	Anzeige der vorherigen Maske. Haben Sie auf dieser Maske bereits Eingaben gemacht, werden diese gespeichert.
	Das Kopieren der notwendigen Daten wird begonnen, der Fortschritt wird in einem Balken angezeigt.
	<p>Abbruch des Installationsvorganges → Warnmeldung</p> <p><i>Das Setup ist noch nicht abgeschlossen. Wenn Sie jetzt beenden, wird das Programm nicht installiert.</i></p> <p><i>Sie können das Setup zu einem späteren Zeitpunkt nochmals ausführen, um die Installation zu vervollständigen. Setup verlassen?</i></p> <p><i>Mit der Auswahl Ja wird die Installation abgebrochen, mit der Auswahl Nein wird die Warnmeldung ausgeblendet und Sie können die Installation fortsetzen.</i></p> <p>Mit der Auswahl Ja auf der Folgemaske wird die Installation abgebrochen, mit der Auswahl Nein wird die Warnmeldung ausgeblendet und Sie können die Installation fortsetzen.</p>

4.3.8 Software starten



Auswahlfelder

Name	Gültige Werte	Bedeutung
trustDesk professional starten	<input type="checkbox"/>	Nach Fertigstellung der Installation wird das Programm nicht automatisch gestartet
	<input checked="" type="checkbox"/>	Nach Fertigstellung der Installation wird das Programm automatisch gestartet

Buttons

Name	Bedeutung
	Installation wird abgeschlossen. Haben Sie trustDesk professional starten aktiviert, wird die Signaturmaske angezeigt. Haben Sie trustDesk professional starten nicht aktiviert, wird der Installationsassistent geschlossen.
	Anzeige der vorherigen Maske. Haben Sie auf dieser Maske bereits Eingaben gemacht, werden diese gespeichert.

5 Deinstallation

Sie können trustDesk professional über das Startmenü mittels Auswahl des Menüpunktes „trustDesk professional entfernen“ deinstallieren.

6 Signieren

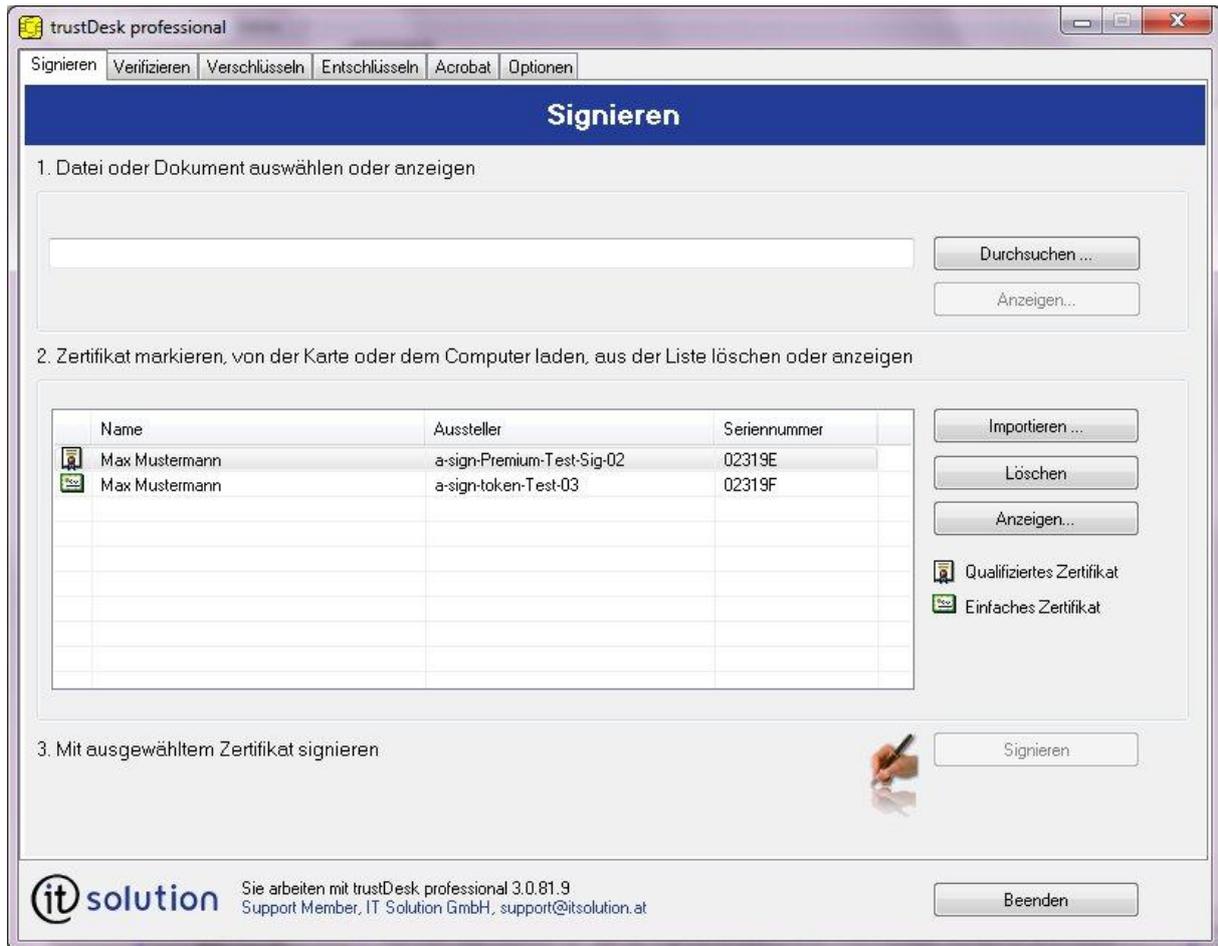
Das Signieren von Dateien und Dokumenten erfolgt in drei einfachen Schritten:

1. Datei oder Dokument auswählen. Das Dokument kann vor der Unterschrift im Originalformat angezeigt werden.
2. Zertifikat markieren.



Zertifikate werden ein Mal von Ihrer Karte oder von Ihrem Computer (Softwarezertifikat) für trustDesk professional geladen. Anschließend stehen Sie für die Signatur zur Verfügung.

3. Mit ausgewähltem Zertifikat signieren.



Eingabefeld

Name	Gültige Werte	Bedeutung
Datei oder Dokument	alphanumerisch	Name und Pfad der Datei oder des Dokumentes, das signiert werden soll.

Buttons

Bereich Zertifikat

Name	Bedeutung
	Auswahl des Pfades für der zu signierenden Datei mithilfe des Windows Browsers
	Anzeige der zu signierenden Datei im Originalformat.

Bereich Datei oder Dokument

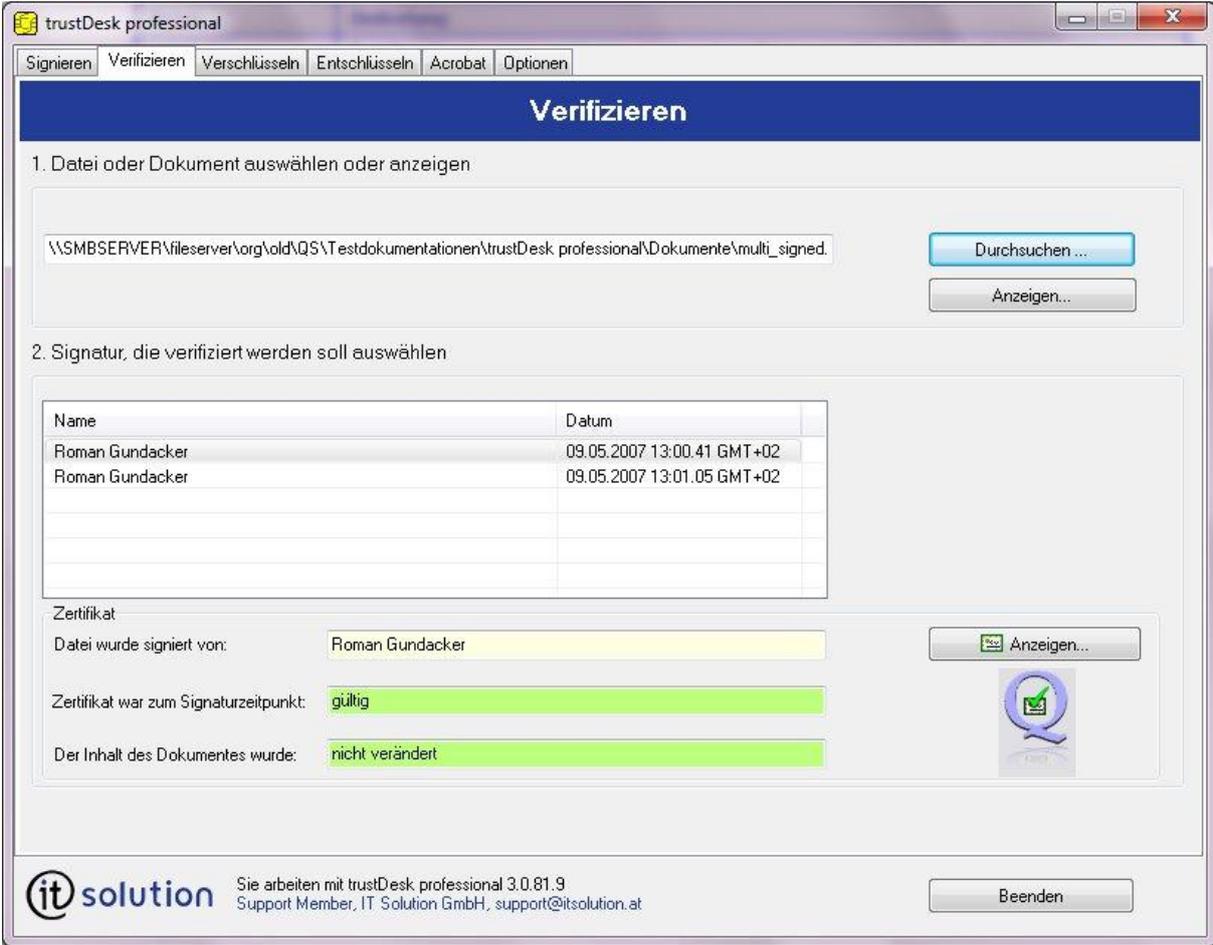
Name	Bedeutung
	Auswahl des Zertifikates für die Signatur mithilfe des Windows Browsers. Zertifikate können entweder von einer Smartcard, die im Kartenlesegerät steckt oder als Datei von Ihrem Computer geladen werden. Wurde das Zertifikat ein Mal in trustDesk professional importiert, steht es für weitere Signaturvorgänge zur Verfügung. Achten Sie bitte darauf, dass zum Signieren mit Smartcardzertifikaten immer die Karte im Kartenlesegerät sein muss.

<input type="button" value="Löschen"/>	Löschen des markierten Zertifikates aus der Liste.
<input type="button" value="Anzeigen..."/>	Anzeige der Detaildaten des Zertifikates.

Bereich mit ausgewähltem Zertifikat signieren

Name	Bedeutung
<input type="button" value="Signieren"/>	Der Signaturvorgang wird ausgelöst. Haben Sie ein qualifiziertes Zertifikat gewählt, wird das Dokument im Secure Viewer angezeigt.

7 Verifizieren



trustDesk professional

Signieren Verifizieren Verschlüsseln Entschlüsseln Acrobat Optionen

Verifizieren

1. Datei oder Dokument auswählen oder anzeigen

\\SMBSERVER\files\server\vorg\vold\QS\Testdokumentationen\trustDesk professional\Dokumente\multi_signed

Durchsuchen ...

Anzeigen...

2. Signatur, die verifiziert werden soll auswählen

Name	Datum
Roman Gundacker	09.05.2007 13:00.41 GMT+02
Roman Gundacker	09.05.2007 13:01.05 GMT+02

Zertifikat

Datei wurde signiert von: Roman Gundacker

Anzeigen...

Zertifikat war zum Signaturzeitpunkt: gültig

Der Inhalt des Dokumentes wurde: nicht verändert

Beenden

it solution Sie arbeiten mit trustDesk professional 3.0.81.9
Support Member, IT Solution GmbH, support@itsolution.at

Eingabefeld

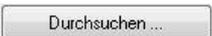
Name	Gültige Werte	Bedeutung
Datei oder Dokument	alphanumerisch	Name und Pfad der Datei oder des Dokumentes, dessen Signatur verifiziert werden soll.

Ausgabefelder

Name	Bedeutung
Zertifikat	Name des Zertifikatsinhabers. Wurde das Dokument von mehreren Personen

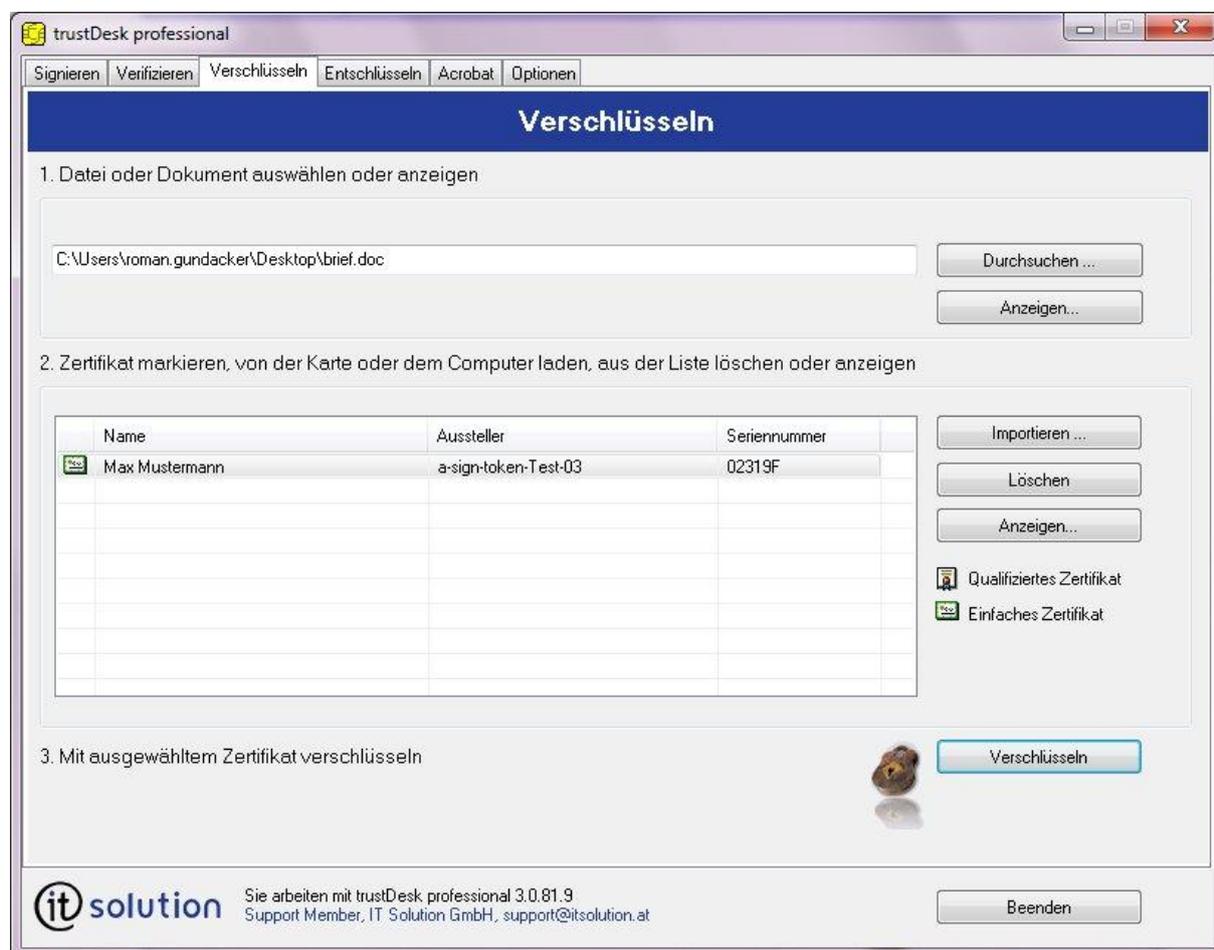
	unterschrieben, werden alle Zertifikatsinhaber aufgelistet.
Datei wurde signiert von	Name des Signators
Zertifikat war zu Signaturzeitpunkt	Gültigkeit des Zertifikates.
Der Inhalt des Dokumentes wurde	Verändert oder nicht verändert, nachdem die Signatur aufgebracht wurde.

Buttons

Name	Bedeutung
	Auswahl des Pfades für der zu verifizierenden Datei mithilfe des Windows Browsers

8 Verschlüsseln

Verschlüsselte Dokumente können nur von der Person, für die das Dokument verschlüsselt wurde, geöffnet und gelesen werden.



Eingabefeld

Name	Gültige Werte	Bedeutung
Datei oder Dokument	alphanumerisch	Name und Pfad der Datei oder des Dokumentes, das verschlüsselt werden soll.

Buttons

Bereich Datei oder Dokument

Name	Bedeutung
<input type="button" value="Durchsuchen ..."/>	Auswahl des Pfades für der zu signierenden Datei mithilfe des Windows Browsers
<input type="button" value="Anzeigen..."/>	Anzeige der zu verschlüsselnden Datei im Originalformat.

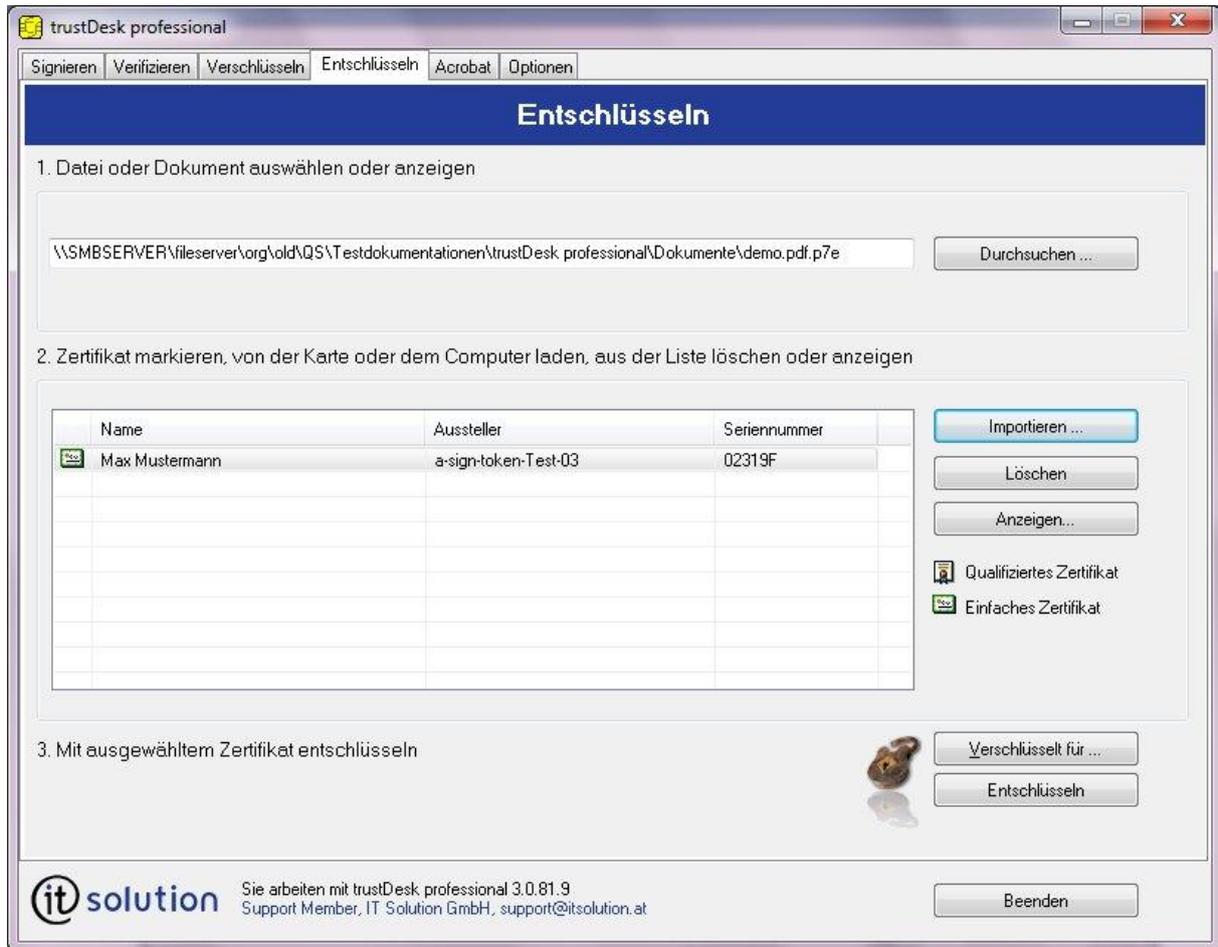
Bereich Zertifikat

Name	Bedeutung
<input type="button" value="Durchsuchen ..."/>	Auswahl des Zertifikates der Person, für die das Dokument verschlüsselt werde soll. Zertifikate können entweder von einer Smartcard, die im Kartenlesegerät steckt, als Datei von Ihrem Computer oder aus der Liste der Zertifizierungsdiensteanbieter im Internet geladen werden. Wurde das Zetifikat ein Mal in trustDesk professional importiert, steht es für weitere Verschlüsselungsvorgänge zur Verfügung. Achten Sie bitte darauf, dass zum Signieren mit Smartcardzertifikaten immer die Karte im Kartenlesegerät sein muss.
<input type="button" value="Löschen"/>	Löschen des markierten Zertifikates aus der Liste.
<input type="button" value="Anzeigen..."/>	Anzeige der Detaildaten des Zertifikates.

Bereich Verschlüsseln

Name	Bedeutung
<input type="button" value="Verschlüsseln"/>	Der Verschlüsselungsvorgang wird ausgelöst. Die verschlüsselte Datei wird gespeichert.

9 Entschlüsseln



Eingabefeld

Name	Gültige Werte	Bedeutung
Datei oder Dokument	alphanumerisch	Name und Pfad der Datei oder des Dokumentes, das entschlüsselt werden soll.

Bereich Zertifikat

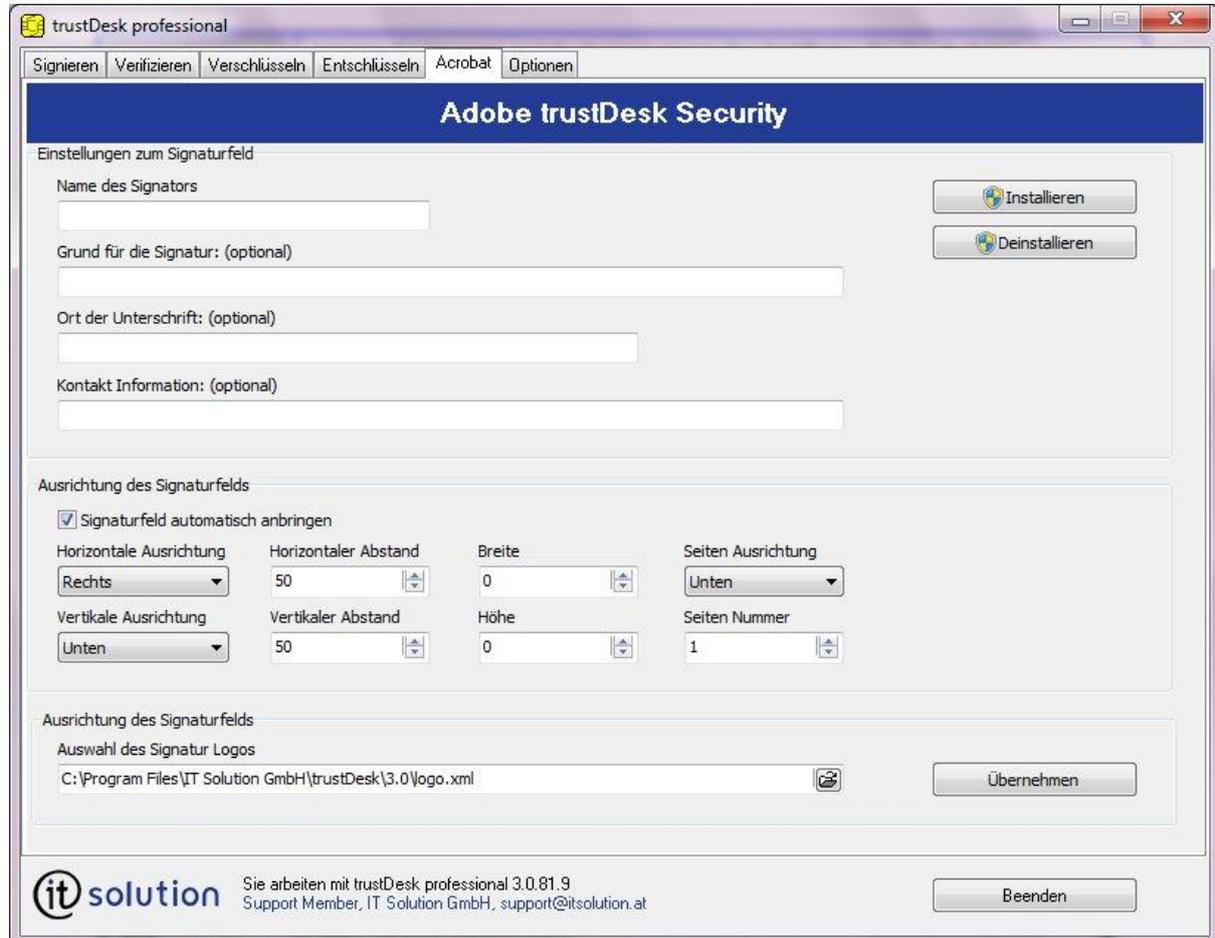
Name	Bedeutung
<input type="button" value="Durchsuchen ..."/>	Auswahl des Zertifikates der Person, für die das Dokument verschlüsselt wurde. Zertifikate können entweder von einer Smartcard, die im Kartenlesegerät steckt, als Datei von Ihrem Computer oder aus der Liste der Zertifizierungsdiensteanbieter im Internet geladen werden. Wurde das Zertifikat ein Mal in trustDesk professional importiert, steht es für weitere Verschlüsselungsvorgänge zur Verfügung. Achten Sie bitte darauf, dass zum Signieren mit Smartcardzertifikaten immer die Karte im Kartenlesegerät sein muss.
<input type="button" value="Löschen"/>	Löschen des markierten Zertifikates aus der Liste.
<input type="button" value="Anzeigen..."/>	Anzeige der Detaildaten des Zertifikates.

Bereich Entschlüsseln

Name	Bedeutung
------	-----------

<input type="button" value="Verschlüsselt für ..."/>	Anzeige des Namens und der Seriennummer des Zertifikates für das die Datei verschlüsselt wurde.
<input type="button" value="Entschlüsseln"/>	De Entschlüsselungsvorgang wird ausgelöst, die Datei wird im Originalformat angezeigt.

10 Acrobat



Eingabefelder

Bereich Einstellungen zum Signaturfeld

Name	Gültige Werte	Bedeutung
Name des Signators	alphanumerisch	Name der im Adobe Acrobat als Signator angezeigt werden soll.
Grund für die Signatur	alphanumerisch	Signaturgrund der im Adobe Acrobat angezeigt werden soll.
Ort der Unterschrift	alphanumerisch	Unterschriftsort der im Adobe Acrobat angezeigt werden soll.
Kontakt Information	alphanumerisch	Kontakt Information die im Adobe Acrobat angezeigt werden soll.

Bereich Ausrichtung des Signaturfelds

Name	Gültige Werte	Bedeutung
Horizontaler Abstand	numerisch	Horizontaler Abstand des Signaturfeldes vom Seitenrand in Pixel.

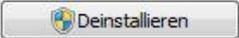
Vertikaler Abstand	numerisch	Vertikaler Abstand des Signaturfeldes vom Seitenrand in Pixel.
Breite	numerisch	Breite des Signaturfeldes in Pixel. (0=Standardgröße)
Höhe	numerisch	Höhe des Signaturfeldes in Pixel. (0=Standardgröße)
Seiten Nummer	numerisch	Nummer der Seite auf welcher das Signaturlogo plaziert werden soll. Bei „Seiten Ausrichtung: Oben“ wird von der ersten Seite des Dokuments nach hinten gezählt. Bei „Seiten Ausrichtung: Unten“ wird von der letzten Seite des Dokuments nach vorne gezählt.

Bereich Auswahl des Signatur Logos

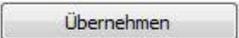
Name	Gültige Werte	Bedeutung
Auswahl des Signaturlogos	alphanumerisch / .xml .jpg	Name und Pfad der Datei, welche das zu verwendende Signaturlogo enthält.

Buttons

Bereich Einstellungen zum Signaturfeld

Name	Bedeutung
	Dieser Button installiert das trustDesk Acrobat PlugIn für die Verifikation und Erstellung von digitalen Signaturen im Adobe Acrobat. (der Acrobat muss vorher beendet werden)
	Dieser Button entfernt das trustDesk Acrobat PlugIn für die Verifikation und Erstellung von digitalen Signaturen aus dem Adobe Acrobat. (der Acrobat muss vorher beendet werden)

Bereich Auswahl des Signatur Logos

Name	Bedeutung
	Dieser Button speichert die Einstellungen im Eingabefeld „Auswahl des Signaturlogos“.

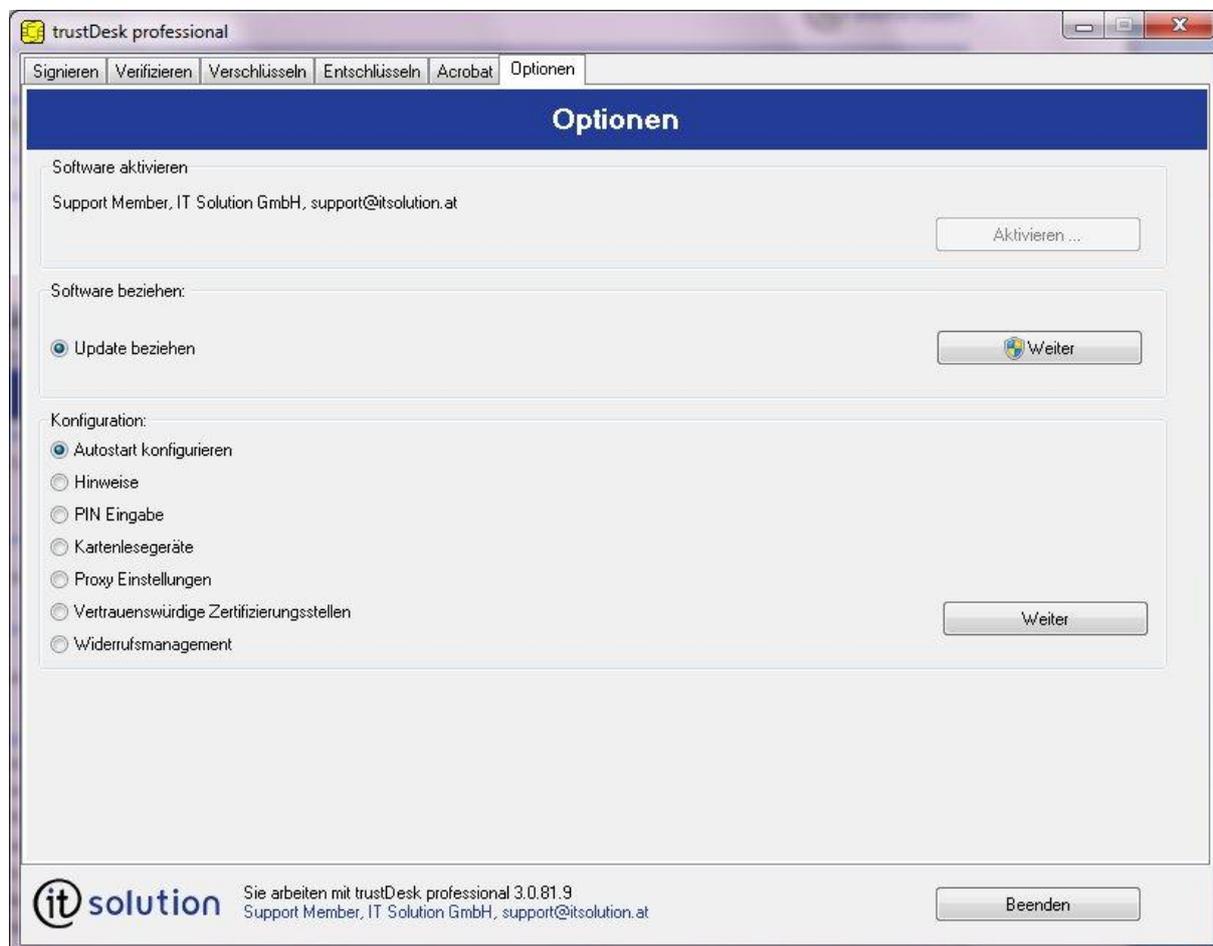
Auswahlfelder

Bereich Ausrichtung des Signaturfelds

Name	Gültige Werte	Bedeutung
Signaturfeld automatisch anbringen		Es wird kein sichtbares Signaturfeld erstellt.
		Es wird automatisch ein Signaturfeld mit den vorgegebenen Werten erstellt.
Horizontale Ausrichtung	Links 	Das Signaturfeld wird am linken Seitenrand ausgerichtet.
	Zentriert 	Das Signaturfeld wird in der Seitenmitte zentriert.
	Rechts 	Das signaturfeld wird am rechten Seitenrand ausgerichtet.
Vertikale Ausrichtung	Oben 	Das Signaturfeld wird am oberen Seitenrand ausgerichtet.
	Mitte 	Das Signaturfeld wird in der Seitenmitte zentriert.
	Unten 	Das Signaturfeld wird am unteren Seitenrand ausgerichtet.
Seiten Ausrichtung	Oben 	Die Platzierung des Signaturfeldes wird in Relation zur ersten Seite des Dokuments vorgenommen.

	<input type="button" value="Unten"/>	Die Platzierung des Signaturfeldes wird in Relation zur letzten Seite des Dokuments vorgenommen.
--	--------------------------------------	--

11 Optionen



Bereich Software aktivieren

Name	Bedeutung
<input type="button" value="Aktivieren ..."/>	Sollte Ihre Software noch nicht aktiviert sein, so gelangen Sie über diesen Button zur Aktivierung. (eine gültige Seriennummer wird benötigt)

Bereich Software beziehen

Name	Bedeutung
<input type="button" value="Weiter"/>	Überprüft ob neue Versionen der Software zur Verfügung stehen, und leitet gegebenenfalls ein online update ein.

Bereich Konfiguration

Name	Bedeutung
<input type="button" value="Weiter"/>	Öffnet das jeweilige Konfigurationsfenster, abhängig davon welcher Punkt der Konfiguration zuvor per Linksklick markiert wurde.

Autostart konfigurieren	Hier können Sie einstellen ob die Software automatisch beim Systemstart gestartet werden soll.
Hinweise	Hier können Sie einstellen ob beim Löschen von Zertifikaten aus der Zertifikatsliste ein Warnhinweis erscheinen soll.
PIN Eingabe	Hier können Sie verschiedene Optionen für die Softwarepin-eingabe einstellen.
Kartenlesegeräte	Hier können Sie ihre Kartenlesegeräte automatisch erkennen lassen, und Änderungen an der Konfiguration vornehmen.
Proxy Einstellungen	Hier können Sie die Daten Ihres Proxy Servers eingeben, falls Ihre Verbindung ins Internet über einen Proxy hergestellt wird.
Vertrauenswürdige Zertifizierungsstellen	Hier können Sie die Liste der vertrauenswürdigen Zertifizierungsstellen verwalten. Vertrauenswürdige Stammzertifikate dienen zur Verifikation anderer Zertifikate.
Widerrufsmanagement	Hier können Sie die Einstellungen für den Bezug von Zertifikats-Widerrufslisten konfigurieren.

12 Setup Kommandozeilenparameter

Das Setup Programm kann mit optionalen Kommandozeilenparametern aufgerufen werden. Diese erlauben Administratoren eine flexible Vorkonfiguration der Software sowie einen erweiterten Einfluss auf den Installationsvorgang. (z.B. silent/unattended installation)

Bitte stellen Sie sicher dass Sie beim Aufruf des Setups mit Kommandozeilenparametern über lokale Administratorrechte verfügen.

/USERNAME="username", /ORGANIZATION="org", /EMAIL="email"

Diese Parameter dienen der Produktaktivierung. Mindestens einer dieser Parameter muss für eine erfolgreiche Aktivierung angegeben werden.

`username` = Voller Name des Benutzers (z.B. Max Mustermann)

`org` = Volle Bezeichnung der Organisation

`email` = eMail-Adresse des Benutzers

/REGCODE="000000000000000000"

Diese Parameter dienen der Produktaktivierung, und muss für eine erfolgreiche Aktivierung angegeben werden. Er übergibt den Registrierungscode der Lizenz.

/SILENT, /VERYSILENT

Diese Parameter dienen dazu die Installation mit minimaler oder gänzlich ohne Feedback/Benutzerinteraktion durchzuführen. /SILENT unterdrückt die Anzeige des Wizards und des Hintergrundfensters, die Installationsfortschrittsanzeige wird jedoch angezeigt. /VERYSILENT Unterdrückt sowohl den Wizard, als auch das Hintergrundfenster und die Fortschrittsanzeige der Installation. Andere Anzeigen sind davon nicht betroffen. Fehlermeldungen z.B. warden angezeigt. Auch der startup prompt wird angezeigt. (sofern er nicht mittels des Parameters DisableStartupPrompt oder der '/SP-' Kommandozeilenoption unterdrückt wird)

Sollte ein Neustart nötig sein und das '/NORESTART' Kommando nicht gesetzt worden sein wird bei /SILENT ein Dialogfenster eingeblendet. Bei Verwendung von /VERYSILENT wird der Neustart ohne Hinweis oder Benutzerinteraktion durchgeführt.

/NOSTART

Dieser Parameter verhindert das automatische starten des securitylayers direkt nach der Installation.

Diese Funktion ist wichtig wenn die Installation von einem Administrator für andere Benutzer durchgeführt wird. Ohne /NOSTART würde in diesem Fall der securitylayer vom Benutzerkonto des Administrators gestartet werden. Vorgenommene Konfigurationsänderungen z.B. würden sich demnach auf das Konto des Administrators beziehen, und nicht auf das Konto des Benutzers.

/SUPPRESSMSGBOXES

Dieser Parameter unterdrückt die Anzeige von Message Boxes. Kann nur in Verbindung mit '/SILENT' oder '/VERYSILENT' verwendet werden.

Die default Antwort in Situationen mit Benutzerinteraktion ist wie folgt:

- ✓ Ja bei 'Neuere Datei behalten?' Situationen.
- ✓ Nein bei 'Datei existiert bereits, soll diese überschrieben werden?' Situationen.
- ✓ Abbrechen in Abbrechen/Wiederholen Situationen.
- ✓ Ja (=fortfahren) bei
 - Festplattenspeicherplatz Warnungen
 - Verzeichnis existiert bereits Warnungen
 - Verzeichnis existiert noch nicht Warnungen
 - NoUninstall Warnung
 - Setup Beenden Nachricht
 - Deinstallation Bestätigen

Situationen.

- ✓ Ja (=Neustart) bei
 - Neustart Abgeschlossen Meldungen
 - Erfolgreich deinstalliert, Neustart erforderlich

Situationen.

Folgende 5 Message Boxes können nicht unterdrückt werden:

- ✓ Die "about Setup" Meldung.
- ✓ Die "Setup verlassen?" Meldung.
- ✓ Die "Datei nicht in Verzeichnis" Meldung, welche angezeigt wird wenn das Setup das einlegen eines neuen Datenträgers verlangt und dieser nicht gefunden werden konnte.
- ✓ Jede Fehlermeldung die angezeigt wird bevor das Setup die Kommandozeilenparameter lesen kann.
- ✓ Jede Meldung die von der [Code] support Funktion `MsgBox` erzeugt wird.

/LOG

Dieser Parameter veranlasst die Erstellung einer Logdatei im TEMP Verzeichnis des Benutzers. Protokolliert werden Dateioperationen und [Run] Operationen die während des Installationsvorganges durchgeführt werden. Dies ist z.B. sehr hilfreich wenn man feststellen möchte, ob bei der Installation bestimmte Dateien erfolgreich ersetzt/überschrieben wurden oder nicht.

Jeder Logdatei erhält einen einzigartigen Namen basierend auf dem derzeitigen Datum. (bestehende Datei werden also nicht überschrieben, und es wird auch nichts an diese angefügt)

Die in der Logdatei enthaltenen Informationen sind technischer Natur und nicht für die Auswertung durch einen normalen Endbenutzer gedacht. Die Form wurde nicht speziell für Maschinenlesbarkeit ausgelegt. (parsing) Änderungen am derzeitigen Format sind dem Hersteller vorbehalten.

/LOG="filename"

Dieser Parameter hat die gleiche Funktion wie /LOG, mit der Ausnahme dass ein bestimmter Pfad/Dateiname vorgegeben werden kann. Existiert bereits eine Datei mit diesem Namen, so wird diese Datei überschrieben. Kann die Datei nicht erzeugt werden, bricht das Setup mit einer Fehlermeldung ab.

/NOCANCEL

Verhindert den Abbruch des Installationsvorgangs durch den Benutzer. Der Abbruch Button wird dadurch deaktiviert, und Klicks auf den „Schliessen“ Button werden ignoriert. Kann mit '/SILENT' und '/VERYSILENT' kombiniert werden.

/NORESTART

Dieser Parameter unterdrückt einen Neustart durch das Setup, selbst wenn der Neustart nötig wäre.

/RESTARTEXITCODE=exit code

Legt den exit code fest der vom Setup zurückgegeben wird wenn ein Neustart notwendig ist. Kann mit '/NORESTART' kombiniert werden.

/LOADINF="filename"

Veranlasst das Setup Einstellungen aus der angegebenen Datei zu laden nach der Überprüfung der Kommandozeile. Diese Datei kann mittels '/SAVEINF=' vorbereitet werden wie unten beschrieben.

Sollte der Dateiname Leerzeichen enthalten sind Hochkommata "" zwingend notwendig.

/SAVEINF="filename"

Dieser Parameter veranlasst das Setup Installationseinstellungen in die angegebene Datei zu schreiben. Sollte der Dateiname Leerzeichen enthalten sind Hochkommata "" zwingend notwendig.

/LANG=Sprache

Dieser Parameter legt die zu verwendende Sprache fest. *Sprache* gibt hierbei den internen Name der Sprache an wie in einem [Languages] Abschnitt Eintrag definiert.

Wird ein gültiger /LANG Parameter übergeben, wird der *Sprache auswählen* Dialog unterdrückt.

/DIR="x:\dirname"

Dieser Parameter ersetzt den default Verzeichnisnamen welcher im Dialogfenster *Ziel-Ordner wählen* im Setup Wizard angezeigt wird. Es muss ein vollständiger gültiger Pfadname eingegeben werden.

/GROUP="folder name"

Dieser Parameter ersetzt den default Ordernamen welcher im Dialogfenster *Startmenü-Ordner auswählen* im Setup Wizard angezeigt wird. Wenn die [Setup] Abschnitt Direktive `DisableProgramGroupPage` auf `yes`, gesetzt wurde wird dieser Parameter ignoriert.

/NOICONS

Dieser Parameter veranlasst das Setup die Checkbox *Keinen Ordner im Startmenü erstellen* im Dialogfenster "Startmenü-Ordner auswählen" des Setup Wizards per default zu aktivieren.

/COMPONENTS="Komma separierte Liste der Komponenten Namen"

Dieser Parameter ersetzt die default Komponenten Einstellungen. Es werden automatisch die angegebenen Komponenten voreingestellt.

/TASKS="Komma separierte Liste der task Namen"

Spezifiziert eine Liste von tasks welche anfangs ausgewählt bzw. Nicht ausgewählt werden sollen. Um einen task zu deselektieren muss dem Namen ein "!" vorangestellt werden.

Nur die angegebenen tasks (und zu diesen zugehörige) werden selektiert, der Rest wird deselektiert. Verwenden Sie statt dessen den /MERGETASKS Parameter wenn Sie möchten dass die default task Liste beibehalten wird, und nur einige ausgewählte tasks selektiert/deselektiert werden sollen.

Beispiele:

- Alle tasks deselektieren, und dann die tasks "desktopicon" und "fileassoc" selektieren:
/TASKS="desktopicon,fileassoc"
- Alle tasks deselektieren, dann einen task selektieren, mit Ausnahme eines zu diesem task zugehörigen child tasks:
/TASKS="parent,!parent\child"

/MERGETASKS="Komma separierte Liste der task Namen"

Funktioniert wie der /TASKS Parameter, mit dem Unterschied dass die angegebenen tasks mit der default task Liste vermischt werden, anstatt diese gänzlich zu ersetzen.

Wenn `UsePreviousTasks` auf `yes` gesetzt wurde, werden die angegebenen tasks selektiert/deselektiert nachdem alle vorherigen tasks wiederhergestellt wurden.

Beispiele:

- Selektion der "desktopicon" und "fileassoc" tasks unter Beibehaltung der default task Liste:
/MERGETASKS="desktopicon,fileassoc"

- Deselektion des "desktopicon" tasks unter Beibehaltung der default task Liste:

```
/MERGETASKS="!desktopicon"
```

/PASSWORD=Passwort

Gibt das Passwort an welches verwendet werden soll. Wenn die [Setup] Abschnittsdirektive `Password` nicht gesetzt wurde, wird dieser Kommandozeilenparameter ignoriert.

Sollte ein ungültiges Passwort angegeben werden, so wird dieser Parameter ebenfalls ignoriert.

/SIGforceOCSP="yes/no"

Gibt an ob OCSP für den Bezug von Widerrufslisten, für die Prüfung von Signaturzertifikaten verwendet werden soll oder nicht. Wird der Parameter auf „yes“ gesetzt dann wird OCSP bei der Prüfung von Signaturzertifikaten verwendet.

/SSLforceOCSP="yes/no"

Gibt an ob OCSP für den Bezug von Widerrufslisten, für die Prüfung von Serverzertifikaten verwendet werden soll oder nicht. Wird der Parameter auf „yes“ gesetzt dann wird OCSP bei der Prüfung von Serverzertifikaten verwendet.

/LogoFile="filename"

Gibt die Datei an welche das Signaturlogo enthält. Nur Dateien im .xml oder .jpg Format werden akzeptiert. Nur absolute Dateipfade sind erlaubt. Relative Dateipfade werden nicht angenommen.

/RevocationFile="filename"

Gibt die Datei an welche die Einstellungen der Widerrufslisten Konfiguration enthält. Der Dateiname muss „crl.lst“ lauten. Nur absolute Dateipfade sind erlaubt. Relative Dateipfade werden nicht angenommen.

13 Uninstaller Kommandozeilenparameter

Das uninstaller Program (unins???.exe) kann mit optionalen Kommandozeilenparametern aufgerufen werden. Diese Möglichkeit erlaubt es Systemadministratoren oder anderen Programmen den Deinstallationsvorgang nach Wunsch zu beeinflussen.

/SILENT, /VERYSILENT

Dieser Parameter unterdrückt die Dialoge welche vor Beginn, und nach erfolgreichem Abschluss der Deinstallation angezeigt werden. Gemeinsam genutzte Dateien welche nicht mehr in Verwendung sind werden ohne Rückfrage gelöscht. Kritische Fehlermeldungen werden trotzdem noch angezeigt. Bei Verwendung des Parameters '/VERYSILENT' wird die Anzeige des Deinstallations-Fortschritts Fensters unterdrückt. Sollte ein Neustart notwendig sein, und der Parameter '/NORESTART' nicht verwendet worden sein, so wird im Falle der Verwendung des '/VERYSILENT' Parameters der Neustart ohne Rückfrage ausgeführt.

/SUPPRESSMSGBOXES

Dieser Parameter unterdrückt message boxes. Kann nur in Kombination mit '/SILENT' und '/VERYSILENT' verwendet werden. Siehe '/SUPPRESSMSGBOXES' unter Setup Kommandozeilenparameter für Details.

/LOG

Dieser Parameter veranlasst die Erzeugung einer Logdatei im TEMP Verzeichnis des Benutzers, welche alle Dateideinstallations und [UninstallRun] Vorgänge protokolliert welche während der Deinstallation stattfinden.

Jeder Logdatei erhält einen einzigartigen Namen basierend auf dem derzeitigen Datum. (bestehende Datei werden also nicht überschrieben, und es wird auch nichts an diese angefügt)

Die in der Logdatei enthaltenen Informationen sind technischer Natur und nicht für die Auswertung durch einen normalen Endbenutzer gedacht. Die Form wurde nicht speziell für Maschinenlesbarkeit ausgelegt. (parsing) Änderungen am derzeitigen Format sind dem Hersteller vorbehalten.

/NORESTART

Dieser Parameter unterdrückt einen Neustart selbst wenn dieser notwendig wäre.

14 Beispiele silent setup

```
"trustDesk business.exe"
  "/SILENT"
  "/ORGANIZATION=IT Solution GmbH"
  "/REGCODE=00000000000000000000"
```

Oder mit „Run As“

```
RUNAS /user:Administrator
  "\"trustDesk business.exe\"
    \"/SILENT\"
    \"/USERNAME=John Doe\"
    \"/ORGANIZATION=IT Solution GmbH\"
    \"/EMAIL=john.doe@itsolution.at\"
    \"/REGCODE=00000000000000000000\""
```

15 Wörterbuch

Begriff	Erklärung
CT-API Treiber	CT-API, das ist ein allgemeiner Kartenlesertreiber, bei dem die zugehörige CT-API-dll angegeben und konfiguriert werden muss.
elektronische Unterschrift	Siehe „Sichere elektronische Signatur“
Digitale Signatur	Eine sichere digitale Signatur wurde mit einer sicheren Signaturerstellungseinheit unter Verwendung eines „Secure Viewers“ erstellt und ist rechtlich gesehen bis auf wenige Ausnahmen (s. § 4 (2) SigG) Ihrer eigenhändigen Unterschrift gleichgestellt. Demgegenüber kann eine (einfache) digitale Signatur mit einem beliebigen Programm erstellt werden. Die einfache Signatur hat nicht die besondere Rechtswirkung der sicheren digitalen Signatur, ist jedoch ebenfalls als Beweismittel zulässig (Grundsatz der Nichtdiskriminierung einfacher digitaler Signaturen).
Hashwert	Ist jener Wert, der zunächst aus dem zu signierenden Dokument errechnet wird und zum Überprüfen der sicheren digitalen Signatur dient
Kartenlesegerät	Kartenlesegeräte dienen dem Auslesen von Inhalten auf Smartcards. Man unterscheidet die Sicherheitsklassen 1 = Kartenleser ohne Eingabetastatur. Mit solchen Kartenlesegeräten ist keine sichere digitale Signatur möglich 2 = Kartenleser mit eigener Eingabetastatur 3 = Kartenleser mit eigener Eingabetastatur und digitalem Display.
PC/SC Treiber	PC/SC, das ist der Kartenlesertreiber von Windows, der automatisch erkannt und konfiguriert wird. Bei PC/SC ist keine Pineingabe über Pinpad möglich, auch wenn das Gerät über ein solches verfügt.
PIN	Eine PIN (Personal Identification Number) oder ein PIN-Code ist eine Zeichenfolge (zumeist eine numerische Zahl) mehrerer (meist 8) Stellen. Sie/Er ist zum Authentisieren bei der Leistung einer digitalen Signatur vorzuweisen. Die PIN dient Ihnen zur Authentifizierung gegenüber Ihrer sicheren Signaturerstellungseinheit. Sie dürfen diesen Code weder aufschreiben noch auf sonstige Art an Dritte weitergeben. Zusätzlich dürfen Sie in keinem Fall Ihre sichere Signaturerstellungseinheit offen stehen lassen und somit Dritten zugänglich machen. Verschließen Sie Ihre Signaturerstellungseinheit nach der Signaturerstellung und verlassen Sie während der Benutzung von trustView Ihren PC nicht , d.h. lassen Sie bitte zu keinem Zeitpunkt alle Komponenten zur Erstellung einer sicheren digitalen Signatur unbeaufsichtigt.
Qualifizierte Zertifikate	§ 2 Z 9 SigG „qualifizierte Zertifikate“.
Secure Viewer	Ein Secure Viewer ist eine Anwendung zur sicheren Anzeige von Daten. Dies ist vor allem: vor, während und nach der Erstellung einer digitalen Signatur oder Signaturprüfung von Bedeutung.
Sichere elektronische Signatur	§ 2 Z 2 u 3 lit a-e SigG: Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die der Feststellung der Identität des Signators (Authentifizierung) dienen, und die ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind die Identifizierung des Signaturschlüssel-Inhabers ermöglichen mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkennbar ist.

Begriff	Erklärung
	<p>auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und mit einer sicheren Signatur Erstellungseinheit erzeugt werden.</p> <p>Das Signaturgesetz, das die Anwendung digitaler Signaturen regelt, ermöglicht elektronische Dokumente mit einer digitalen Signatur fälschungssicher und rechtsgültig zu versehen. Die sichere digitale Signatur ist einer eigenhändigen Unterschrift gleichstellt und deswegen z.B. in Gerichtsverfahren als Beweismittel zulässig.</p> <p>Für das Benützen der digitalen Signatur ist ein Zertifikat mit zueinander passendem Schlüsselpaar notwendig. Dieses besteht aus dem privaten Schlüssel, der geheim gehalten werden muss, und dem öffentlichen Schlüssel, der frei zugänglich sein kann. Das Zertifikat enthält den öffentlichen Schlüssel. Die Ausstellung solcher Zertifikate ist bei einem so genannten Trustcenter zu beantragen. Der Antragsteller erhält die Smartcard (=Zertifikat) nur, wenn er seine Identität zweifelsfrei durch Vorlage eines amtlichen Lichtbildausweises nachgewiesen hat.</p> <p>Bei der digitalen Unterschrift wird aus dem zu signierenden Dokument zunächst ein Hashwert errechnet.</p> <p>Der Hashwert des Dokumentes wird mit dem privaten Schlüssel des Unterzeichnenden verschlüsselt und gemeinsam mit dem Unterzeichner (=Zertifikat) dem Dokument hinzugefügt.</p> <p>Das Überprüfen der Unterschrift erfolgt nun einerseits durch die Prüfung des Zertifikates, wodurch die Identität des Unterzeichnenden geprüft werden kann, andererseits durch die erneute Berechnung des Hashwertes. Der Hashwert des Dokumentes zum Signaturzeitpunkt wird mit dem öffentlichen Schlüssel des Unterzeichnenden entschlüsselt. Dieser befindet sich im Zertifikat des Unterzeichnenden.</p> <p>Dadurch ist es möglich, den ursprünglich bei der Unterzeichnung berechneten Hashwert mit einem neu errechneten zu vergleichen. Stimmen die beiden Werte überein, ist das Dokument nicht manipuliert.</p>
Signator oder Unterzeichner	§ 2 Z 2 SigG „Signatur Schlüssel-Inhaber“; nicht zu verwechseln mit dem Siemens-Signator®, der eine mögliche Signaturerstellungskomponente ist.
Signaturanwendungskomponente	§ 2 Z 11 SigG „Signaturanwendungskomponente“ (hier der EVG trustView)
Signaturbereich	Dokumentdaten, die von einer digitalen Signatur erfasst werden
Signaturerstellungseinheit	<p>§ 2 Z 5 SigG: Konfigurierte Soft- oder Hardware zur Verarbeitung der Signaturerstellungsdaten; z.B. eine SmartCard.</p> <p>Die Signaturerstellungseinheit muss die sichere Speicherung der Signaturschlüssel (z.B. sichere SmartCard) und eine sichere Authentisierung des Benutzers (z.B. über einen sicheren SmartCard-Leser mit PINPad) ermöglichen. Es ist immer eine Kombination aus Signaturerstellungseinheit und entsprechendem Kartenleser erforderlich. Welche Kartenlesegeräte für welche Karten geeignet sind, erfahren Sie in Ihrem Trustcenter.</p>
Signaturerstellungskomponente	Die Kombination einer sicheren Signatur-Erstellungseinheit (SSEE) nach § 2 Z 5 SigG und einem Modul einer Signaturanwendungskomponente nach § 2 Z 13 SigG .Die SSEE ist beispielsweise eine SmartCard. Diese benötigt zur Verbindung mit dem EVG einen SmartCard-Reader, der ein Modul einer Signaturanwendungskomponente ist.
Signaturprüf Schlüssel	§ 2 Zi 6 SigG „Signaturprüf Schlüssel“ (öffentlicher kryptografischer Schlüssel zur Überprüfung verwendet).
Signaturschlüssel	§ 2 Zi. 4. SigG „Signatur Schlüssel“ (privater kryptografischer Schlüssel zur Signaturerstellung).

Begriff	Erklärung
SmartCard	Siehe „Signaturerstellungskomponente“
SmartCard-Reader	Siehe Kartenlesegerät
Trustcenter	s. Zertifizierungsdiensteanbieter
Viren	Das sind „böartige“ Anwendungsprogramme, um Daten auszuspähen oder Schaden zu verursachen. Dies geschieht, indem diese Programme sich tarnen und versuchen, sich versteckt zu verbreiten (Viren) oder ein anderes Programm nachzumachen (Trojaner), jedoch hinter der gleichen Oberfläche andere (zumeist böartige) Funktionen verursachen.
Zertifikat	<p>§ 2 Z 8 SigG: Eine elektronische Bescheinigung, mit der Signaturprüfdaten (Z 6) einer bestimmten Person zugeordnet werden und deren Identität bestätigt wird.</p> <p>Zertifikate sind, wie bereits erwähnt, bei einem Trustcenter zu beantragen. Ein Zertifikat ist eine elektronische Bindung einer Person an ein Schlüsselpaar, das grundlegende Informationen über den Besitzer des Zertifikates enthält.</p> <p>Es gibt verschiedene Zertifikate, zum Beispiel Signaturzertifikat oder Geheimhaltungszertifikat.</p> <p>Zertifikate werden vom ausstellenden Trustcenter digital signiert und somit vor Manipulationen geschützt, womit ihre Echtheit nachvollziehbar garantiert wird.</p>
Zertifizierungsdiensteanbieter	§ 2 Z 10 SigG: Natürliche oder juristische Person oder sonstige rechtsfähige Einrichtung, die Zertifikate ausstellt oder andere Signatur- und sonstige Zertifizierungsdienste erbringt „