IT Solution GmbH A-1070 Wien, Neubaugasse 12-14

Produktdokumentation

trustDesk basic

Urheberrechtshinweise

Die in dieser Dokumentation beschriebene Software wird auf Grund einer Generallizenz vom Bundeskanzleramt bereitgestellt.

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 2.7 für Windows bis zur Veröffentlichung einer neuen Version der Software und somit dieses Handbuches im Internet.

IT Solution GmbH, A-1070 Wien, Neubaugasse 12-14 ☏ ++431- 524 3 524 - Serie TELEFAX ++431- 524 3 524 - 24
Bank: Hypo NÖ BLZ 53.000 Konto Nr. 1455-00 8251, HG Wien: FN 175262 p, UID ATU 47107704
e-mail: office@itsolution.at www.itsolution.at

Inhaltsverzeichnis

1 IT Solution GmbH 5

2 Sicherheitshinweise 6

3 Systemvoraussetzungen 7

3.1 Hardware 7

3.2 Betriebssystem 7

3.3 Unterstützte Smartcards 7

3.4 Kartenlesegeräte 7

4 Installation 8

4.1 Download aus dem Internet 8

4.2 CD 8

4.3 Installationsschritte für Windows 9

4.3.1 Kartenlesegeräte 9
4.3.2 Lizenzvertrag 10
4.3.3 Installationsverzeichnis 11
4.3.4 Programmordner 12
4.3.5 Autostart-Funktion 13
4.3.6 Root Zertifikat 13

5 Deinstallation 14

5.1 Interaktiv 14

6 Betrieb mit mehreren Kartenlesegeräten 14

6.1 Wechsel des verwendeten Kartenlesers 14

7 Online Update 14

8 Konfiguration 15

8.1 Kartenleser 17

8.1.1 E-Government 18

8.2 SSL Einstellungen 20

8.3 Proxy Server 20

8.4 Cache 21

8.5 Verschlüsselung 22

8.6 Online Update-Möglichkeit 24

9 E Government Funktionen 24

9.1 Security-Layer aktivieren bzw. deaktivieren 24
9.2 Security-Layer mit SSL aktivieren bzw. deaktivieren 24
9.3 Hashwerte anzeigen 24
9.4 Infobox Verwaltung 25
9.5 Neuen einfachen Speicher oder Schlüsselspeicher anlegen 27
9.5.1 Schlüssel in Schlüsselspeicher anlegen 27
9.6 Bezeichnung ändern 27
9.7 Schlüssel aus Schlüsselspeicher löschen 28
9.8 Infobox löschen 28
9.9 Inhalte anzeigen 28
9.10 Einfacher Speicher - Inhalte ändern 29
9.11 Einstellungen anzeigen und ändern 29
9.12 PIN und PUK für Smartcards 30
9.12.1 PIN Änderung 30
9.12.2 Fehler bei der PIN Eingabe 30
9.13 PIN aktivieren (e-Card und o-Card) 30
9.14 Karte mittels PUK entsperren 31
10 Widerrufsmanagement 31
10.1 Signatur- und SSL Zertifikate 31
10.2 Widerrufslisten Verteilungspunkte 33
11 (Vertrauenswürdige) Zertifizierungsstellen 36
11.1 Sicherheitsverwaltung 37
11.2 SSL Client Authentifizierung 39
11.3 Identifikationskette 41
11.4 Authentisierungsklasse 42
11.5 Identifikation 42
11.5.1 Regel bearbeiten 44
12 Stellvertretungen und GDA Token 46
13 Signaturerstellung 47
13.1 Digital unterschreiben 47
14 Häufige Fehlerursachen 48
14.1 Signaturkarte nicht eingelegt 48
14.2 Falsche PIN 49
14.3 Null PIN 49
14.4 Leere Smartcard 49

14.5 Smartcard und Kartenleser passen nicht zusammen 49
14.6 Software PIN nicht aktiviert 49
14.7 Signieren mit trustDesk basic 49
15 XML signieren 49
15.1 Tiff Signatur mit File Referenz 51
16 CMS signieren 52
17 Signaturprüfung 52
17.1 Verifikationsergebnis der Signaturprüfung 52
17.2 XML verifizieren 53
17.3 CMS Signatur verifizieren 54
18 Installationsroutinen für Firmen und Behörden 54
18.1 Silent Installation 54
18.2 Silent Deinstallation 54
18.3 Automatisches Deployment 55
18.3.1 Parameter und gültige Eingabewerte 55
19 Open Source Lizenzen 62
19.1 OpenSSL License 62
19.2 The FreeType Project LICENSE 63
19.3 Zlib general purpose compression library License 66
19.4 LibTIFF - TIFF Library 66
19.5 JPEG image compression library License 66
20 Wörterbuch 68
21 Literaturhinweise 71

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 Signaturerstellungssoft-ware 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 Virenscanner (z.B. McAffee 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 basic 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 2000 oder Windows XP

3.3 Unterstützte Smartcards

Karte	System
A-Trust A-Sign Premium SmartCard	ACOS
A-Trust A-Sign Premium SmartCard	StarCOS 2.3
e-Card	StarCOS 3.1
o-Card	StarCOS 3.1
Estnische EstEID Karte	Micardo 2.1
Italienische Karte*	
Belgische Karte	
Finnische Karte	

* nur in Verbindung mit Kartenleser der Firma Cherry verwendbar

3.4 Kartenlesegeräte

	Bezeichnung	Klasse
	Reiner SCT cyberJack® e-com	3
	Omnikey CardMan Trust 3821 Achtung! Treiberinstallation NUR mit Administratorkennung möglich	3

	Reiner SCT cyberJack® pinpad	2
	SCM CHIPDRIVE® pinpad pro = SCM Microsystems SPR532 (baugleiche Leser)	2
	Omnikey CardMan Trust USB 3621 Achtung! Treiberinstallation NUR mit Administratorkennung möglich	2
	Cherry Smartboard G83-6744LUZxx und G83-6744LBZxx	2
	GemPlus USB-SL	1

4 Installation

Um die Software trustDesk basic 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 Sie wenden sich an ihren Systemadministrator um Hilfe.

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

4.1 Download aus dem Internet

trustDesk basic kann von der Webseite www.cio.gv.at/identity/bku/ durch Doppelklick auf **trustDesk basic Installer** kostenfrei heruntergeladen werden.

Die Dauer des Downloads ist in erster Linie von der Internetverbindung, über die die Software geladen wird, abhängig und kann einige Minuten dauern. 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 basic wird auch auf CD ausgeliefert. Diese muss in ein angeschlossenes CD-Laufwerk eingelegt werden.

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

4.3 Installationsschritte für Windows

Vor dem eigentlichen Installationsvorgang erhalten Sie ein Fenster, in dem die mit der Software ausgelieferte Dokumentation aufgelistet ist.

Buttons

Name	Bedeutung
Lesen	Öffnet das markierte Dokument
Mit der Installation fortfahren	Anzeige der nächsten Maske

4.3.1 Kartenlesegeräte

Zuerst überprüft die Software, ob Sie bereits ein oder mehrere Kartenlesegeräte installiert haben. Werden Kartenlesegeräte gefunden, so listet ein Fenster diese Geräte, getrennt nach CT-API und PC/SC Treibern auf.

Buttons

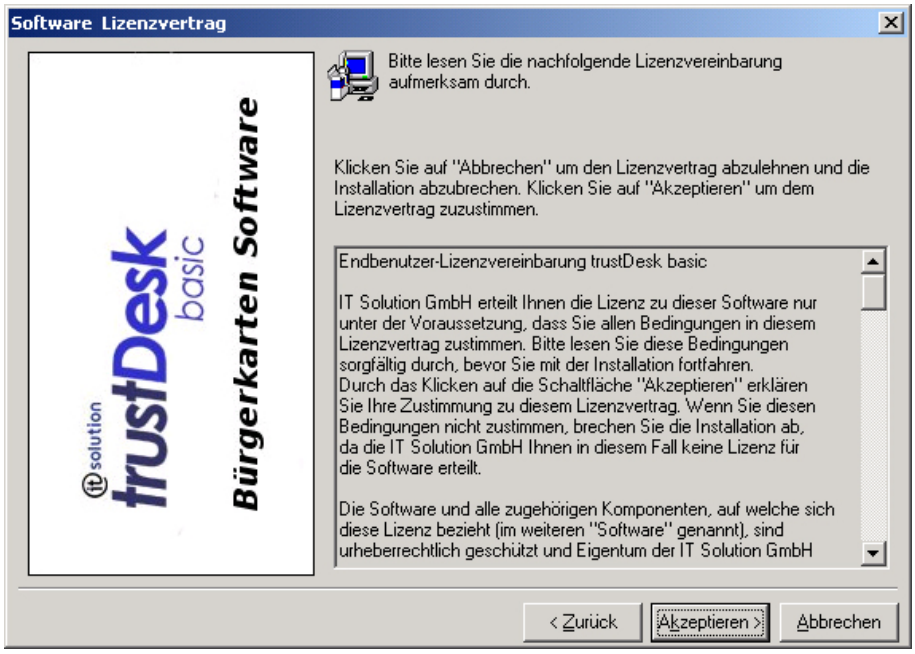
Name	Bedeutung
OK	Installation wird fortgesetzt. Die Karteleserabfrage wird eingeblendet.
Ja	Die Installation wird fortgesetzt
Nein	Installation wird abgebrochen → Meldung *Installation ist nicht vollständig. Senn Sie das Installationsprogramm jetzt beenden, wird das Programm nicht installiert.* Sie können das Installationsprogramm zu einem späteren Zeitpunkt ausführen und die Installation beenden.
Fortsetzen	Anzeige der Maske vor dem Abbruch
Setup beenden	Das Installationsprogramm wird geschlossen. Das Programm wird nicht installiert.

Sollten Sie vor der Installation von trustDesk basic noch keine Kartenlesegeräte installiert haben, so erhalten Sie die Information:

Es wurde keine Kartenleser-Schnittstelle gefunden! Wir empfehlen Ihnen das Setup zu beenden und zuerst ein Kartenlesegerät zu installieren, bevor Sie mit der Installation der Software beginnen.

☞ Für die Installation der Software trustDesk basic ist ein installiertes Kartenlesegerät zwar nicht unbedingt erforderlich, jedoch wird empfohlen, zuerst das/die Kartenlesegerät(e) zu installieren und danach die Software trustDesk basic.

4.3.2 Lizenzvertrag

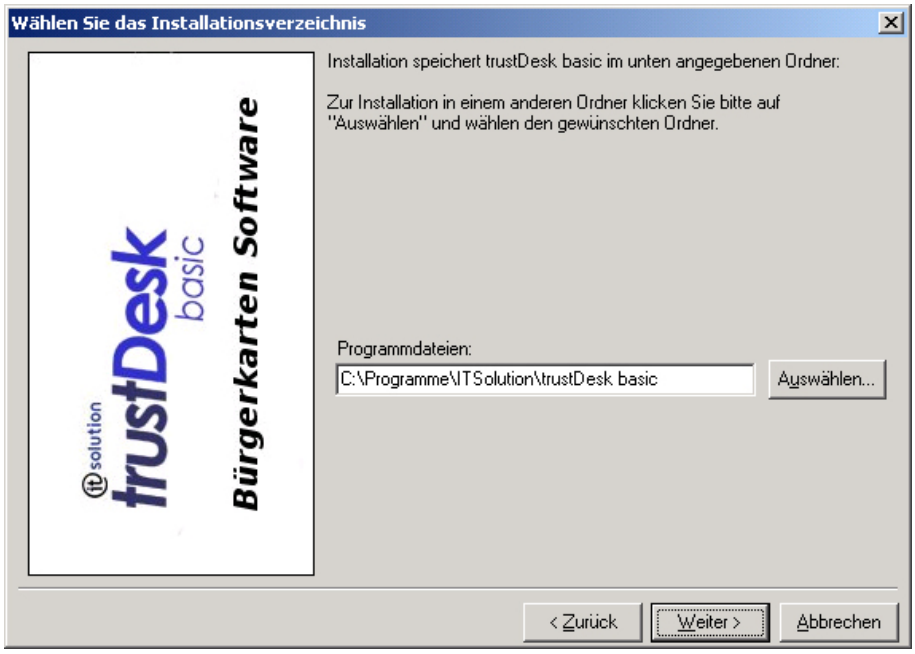


! *Lesen Sie die Lizenzvereinbarungen bitte aufmerksam durch. Sie können durch Klicken auf Zurück einen Schritt in der Installation zurückgehen. Durch Klicken auf Akzeptieren erklären Sie sich mit den Lizenzvereinbarungen einverstanden, und die Installation wird fortgesetzt. Falls Sie mit den Lizenzvereinbarungen nicht einverstanden sind, dann beenden Sie bitte die Installation durch Klicken auf Abbrechen das Programm wird nicht installiert.*

Buttons

Name	Bedeutung
Zurück	Anzeige der vorherigen Maske
Akzeptieren	Zustimmung zum Lizenzvertrag, weiter in der Installation
Abbrechen	Abbruch des Installationsvorganges → Warnmeldung *Installation ist nicht vollständig. Senn Sie das Installationsprogramm jetzt beenden, wird das Programm nicht installiert.* *Sie können das Installationsprogramm zu einem späteren Zeitpunkt ausführen und die Installation beenden.*

4.3.3 Installationsverzeichnis



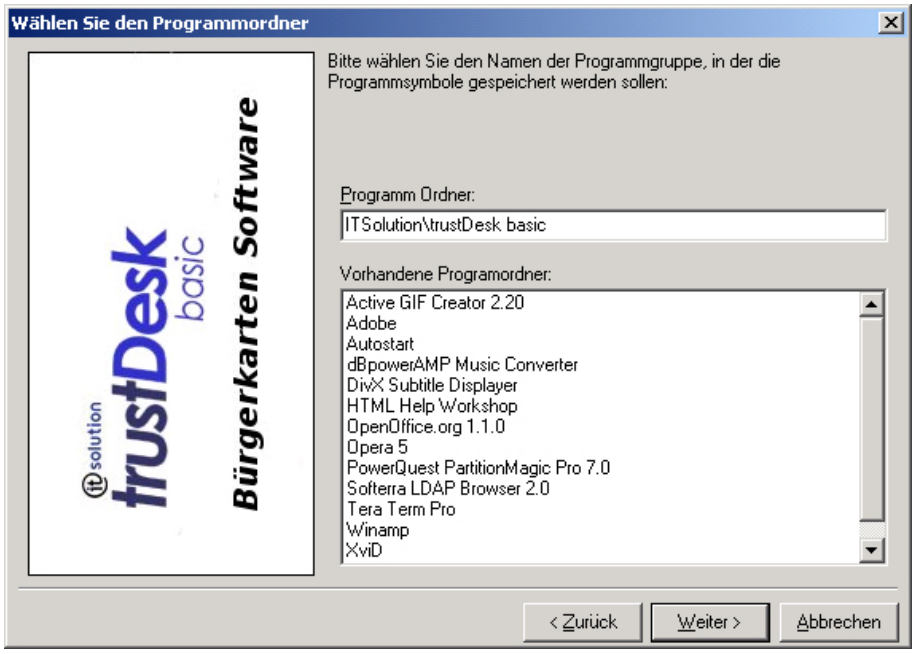
Eingabefelder

Name	Gültige Werte	Bedeutung
Programmdateien	Vorhandenes Verzeichnis	In dieses Verzeichnis werden die Programmdateien von trustDesk basic installiert.

Buttons

Name	Bedeutung
Auswählen	Auswahl des Pfades für die Installationsdateien mithilfe des Windows Browsers
Zurück	Anzeige er vorhergehenden Maske
Weiter	Anzeige der nächsten Maske
Abbrechen	Abbruch des Installationsvorganges → Warnmeldung: *Installation ist nicht vollständig. Senn Sie das Installationsprogramm jetzt beenden, wird das Programm nicht installiert.* *Sie können das Installationsprogramm zu einem späteren Zeitpunkt ausführen und die Installation beenden.*

4.3.4 Programmordner



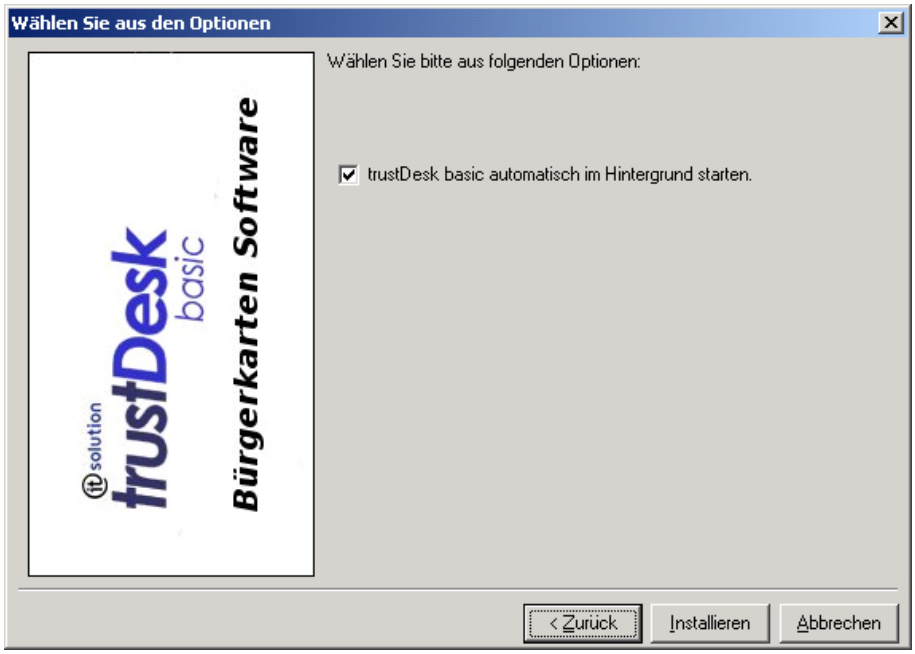
Eingabefelder

Name	Gültige Werte	Bedeutung
Programmordner	alphanumerisch	Unter dieser Programmgruppe können Sie trustDesk basic starten.

Buttons

Name	Bedeutung
Zurück	Anzeige er vorhergehenden Maske
Weiter	Anzeige der nächsten Maske
Abbrechen	Abbruch des Installationsvorganges → Warnmeldung: *Installation ist nicht vollständig. Senn Sie das Installationsprogramm jetzt beenden, wird das Programm nicht installiert.* *Sie können das Installationsprogramm zu einem späteren Zeitpunkt ausführen und die Installation beenden.*

4.3.5 Autostart-Funktion



Eingabefelder

Name	Gültige Werte	Bedeutung
trustDesk basic automatisch im Hintergrund starten	☐	trustDesk basic wird nicht automatisch beim Hochfahren des Computers gestartet
	☑	trustDesk basic beim Hochfahren des Computers automatisch gestartet

Buttons

Name	Bedeutung
Zurück	Anzeige er vorhergehenden Maske
Installieren	Der Installationsvorgang wird gestartet. Vorerst werden die notwendigen Dateien kopiert und anschließend installiert. Das Ende der Installation wird durch die Meldung: *Die Installation wurde erfolgreich beendet*
Abbrechen	Abbruch des Installationsvorganges → Warnmeldung: *Installation ist nicht vollständig. Senn Sie das Installationsprogramm jetzt beenden, wird das Programm nicht installiert.* *Sie können das Installationsprogramm zu einem späteren Zeitpunkt ausführen und die Installation beenden.*

4.3.6 Root Zertifikat

Für das Funktionieren der https-Bindung ist ein Serverzertifikat notwendig. Dieses Zertifikat ist von der IT-Solution CA ausgestellt. Daher muss als letzter Installationsschritt das Root Zertifikat installiert werden:

Mit der Meldung:

SecurityLayer installiert jetzt das Wurzelzertifikat für die SecurityLayer Services. Klicken Sie bitte auf den Button „Wurzelzertifikat installieren“ um den Vorgang durchzuführen Bestätigen Sie bitte den folgenden Windows Systemdialog für die Installation des Wurzelzertifikates mit „Ja“

Dieses Zertifikat wird in den Zertifikatsspeicher unter den vertrauenswürdigen Stammzertifizierungsstellen gespeichert. Prüfen Sie, ob dieses Zertifikat tatsächlich von IT Solution stammt, durch den Vergleich des Fingerabdruckes im Installationsprogramm mit dem auf https://secure.itsolution.at.

Stimmen die beiden überein, dann ist es das Stammzertifikat der IT Solution CA.

5 Deinstallation

5.1 Interaktiv

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

☞ Beachten Sie bitte, dass dabei das Installationsverzeichnis von trustDesk basic zur Gänze (mit allen anderen möglicherweise enthaltenen Dateien) entfernt wird. Sollten Sie also Dokumente oder andere Dateien wie Zertifikate oder Widerrufslisten, die Sie noch benötigen, in den Installationsverzeichnissen von trustDesk basic abgelegt haben, so müssen Sie diese selbst vor dem Deinstallationsvorgang in anderen Verzeichnissen sichern.

Alle bei der Installation erstellten Dateien werden bei der Deinstallation entfernt.

☞ Um die Software deinstallieren zu können, sind Administratorenrechte notwendig!

6 Betrieb mit mehreren Kartenlesegeräten

Wollen Sie trustDesk basic gleichzeitig mit verschiedenen Kartenlesegeräten betreiben, beachten Sie bitte folgendes:

- ❍ Alle verwendeten Kartenleser müssen korrekt und fehlerfrei installiert sein. (Ziehen Sie dazu bitte die Installationsanweisungen des jeweiligen Geräteherstellers zu Rate)
- ❍ Sofern notwendig (Kartenleser mit CT-API Anbindung!) müssen die Kartenleser über das Konfigurationsprogramm von trustDesk basic richtig konfiguriert worden sein.
- ❍ Es ist darauf zu achten, dass immer nur in einem Kartenleser (der gerade verwendet wird) eine Smartcard eingelegt sein darf. Die Software sucht selbständig nach Ihrer Smartcard und arbeitet automatisch mit der ersten Smartcard, die gefunden wird.

6.1 Wechsel des verwendeten Kartenlesers

Es steht Ihnen natürlich frei, jederzeit auf ein anderes Kartenlesegerät umzusteigen. Dabei müssen Sie lediglich darauf achten, dass Sie ein Gerät mit CT-API Anbindung im Konfigurationsprogramm von trustDesk basic korrekt konfigurieren. Geräte mit PC/SC Anbindung werden automatisch erkannt und müssen nicht manuell konfiguriert werden.

7 Online Update

Wird im Internet eine neuere Version der Software gefunden als die auf Ihrem System installierte, Erhalten Sie folgende Meldung.

Für die Software steht ein Update zur Verfügung. Möchten Sie das Update jetzt installieren?

Klicken Sie in diesem Fenster auf **Ja,** um die Software zu aktualisieren bzw. auf **Nein,** um die Software nicht zu aktualisieren.

☞ Dieses Fenster kommt beim nächsten Starten der Software wieder und Sie können zu einem späteren Zeitpunkt das Update durchführen.

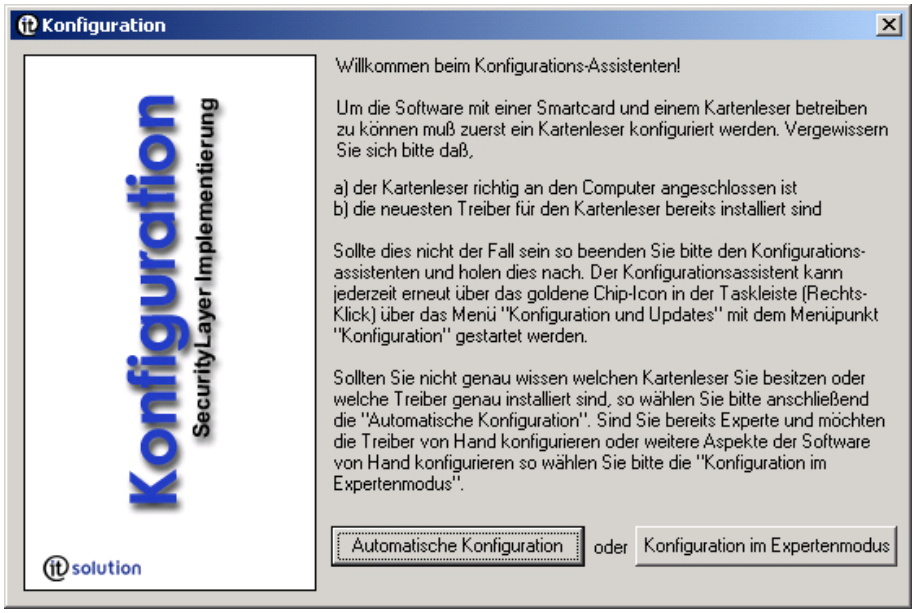
Buttons

Name	Bedeutung
Weiter	Die Installation wird gestartet
Beenden	Das Update wird abgebrochen

8 Konfiguration

Über den Menüpunkt **Konfiguration** gelangen Sie zum Konfigurations-Assistenten. Sie können hier:

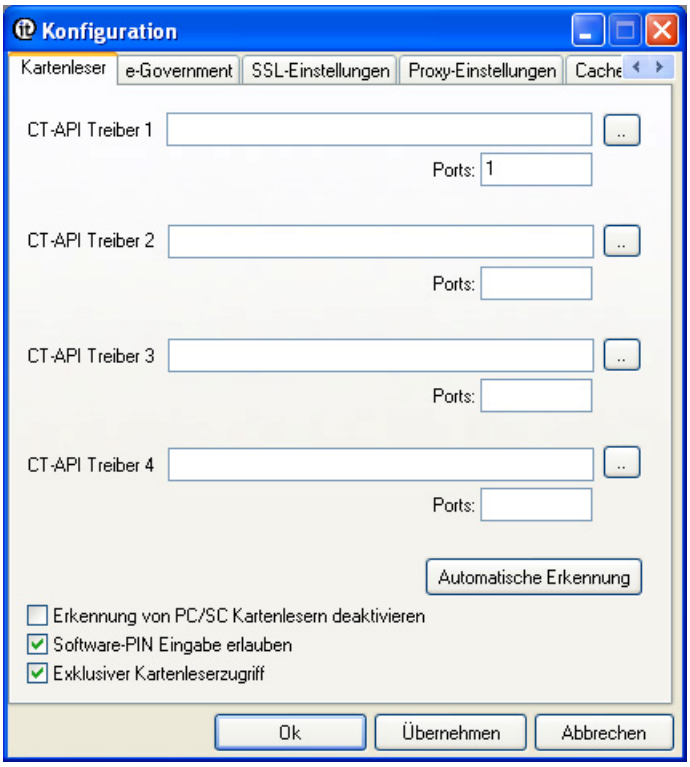
- Alle zu diesem Zeitpunkt installierten Kartenlesegeräte automatisch konfigurieren;
- eine manuelle Konfiguration im Expertenmodus durchführen.



Buttons

Name	Bedeutung
Automatische Konfiguration	Versucht alle installierten Kartenlesegeräte zu erkennen. Nach einer kurzen Suche erhalten Sie eine Liste aller gefundenen Kartenlesegeräte.
Konfiguration im Expertenmodus	Führt zum Konfigurationsassistenten. Beachten Sie bitte, dass für die manuelle Konfiguration entsprechende Kenntnisse über das eigene Computersystem und die Bürgerkartenumgebung vorhanden sein sollten.

8.1 Kartenleser



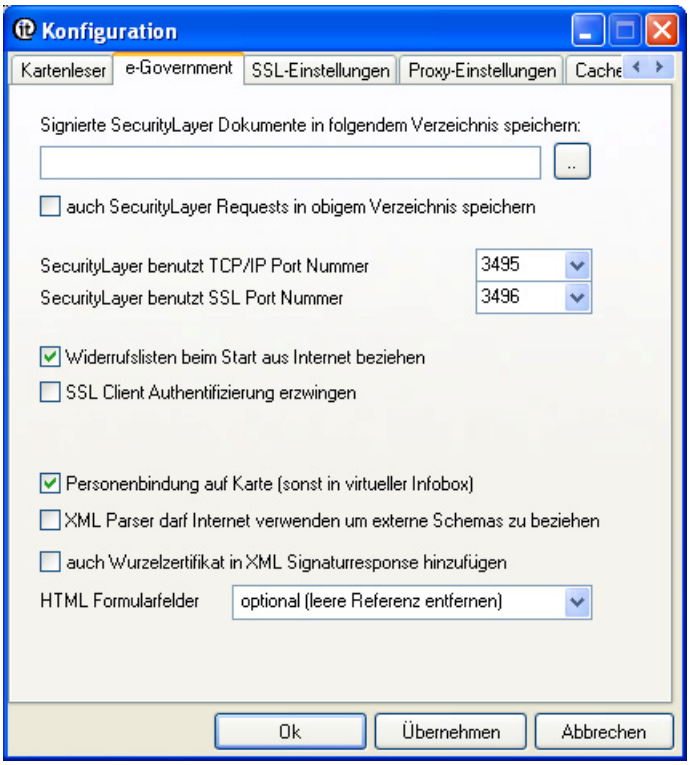
Eingabefelder

Name	Gültige Werte	Bedeutung
CT-API Treiber 1-4		Kein CT-API Treiber ist installiert
	C:\x.dll	Pfad für die Treiberdatei. Sie haben die Möglichkeit, in die Felder Pfad und Name der CT-API Treiber-Datei Ihrer Kartenlesegeräte einzutragen. Mit Klick auf die **'..'** Buttons können Sie den jeweiligen Treiber von Ihrer Festplatte direkt mittels Dialogbox auswählen.
Ports		Kein CT-API Port ist festgelegt
	1	Port unter dem der Kartenleser angesprochen wird.
Erkennung von PC/SC Kartenlesern deaktivieren	☐	Es werden bei der automatischen Erkennung von Kartenlesern auch PC/SC Treiber erkannt
	☑	Treiber von PC/SC Kartenlesern werden nicht in die Suche einbezogen
Software-PIN erlauben	☐	Die PIN kann nicht über die Computertastatur eingegeben werden. . Ist die Auswahlbox nicht aktiviert, erhalten Sie bei der PIN Eingabe folgende Fehlermeldung: Die PIN Eingabe per Software ist derzeit deaktiviert
	☑	Die PIN kann auch über die Tastatur eingegeben werden. Diese Auswahl ist nur bei Kartenlesern möglich, die über PC/SC angebunden sind. Diese Auswahl ist wichtig, wenn Sie ein Kartenlesegerät ohne PIN-Pad (ohne Tastatur zur Eingabe der PIN) verwenden.
Exklusiver Kartenleserzugriff	☐	Der Kartenleser wird nach der PIN Eingabe für andere Applikationen freigegeben
	☑	Der Kartenleser wird erst freigegeben, wenn trustDesk basic beendet wird.

Buttons

Name	Bedeutung
Automatische Erkennung	Versucht alle installierten Kartenlesegeräte zu erkennen. Nach einer kurzen Suche erhalten Sie eine Liste aller gefundenen Kartenlesegeräte. Beachten Sie bitte, dass die automatischen Einstellungen sofort gespeichert werden, auch wenn Sie danach Abbrechen betätigen.
OK	Die eingegebenen Werte werden übernommen, das Programm wird geschlossen.
Übernehmen	Die eingegebenen Werte werden übernommen, das Programm wird nicht geschlossen.
Abbrechen	Die eingegebenen Werte werden nicht übernommen, das Programm wird geschlossen.

8.1.1 E-Government



Buttons

Name	Bedeutung
OK	Die eingegebenen Werte werden übernommen, das Programm wird geschlossen.
Übernehmen	Die eingegebenen Werte werden übernommen, das Programm wird nicht geschlossen.
Abbrechen	Die eingegebenen Werte werden nicht übernommen, das Programm wird geschlossen.

Eingabefelder

Name	Wert	Bedeutung
Signierte SecurityLayer Dokumente in folgendem Verzeichnis speichern		Signierte Dokumente werden nicht automatisch gespeichert
	C:\	In dieses Verzeichnis werden Ihre signierten SecurityLayer Dokumente (SecurityLayer Response) gespeichert. Mittels Klick auf den **'..'** Button können Sie den gewünschten Pfad direkt über eine Dialogbox auswählen.
Auch SecurityLayer Requests in obigem Verzeichnis speichern	☑	Neben den signierten Dokumenten werden auch die SecurityLayer Requests im angegebenen Verzeichnis gespeichert
	☐	SecurityLayer Requests werden nicht im angegebenen Verzeichnis gespeichert.
SecurityLayer benutzt TCP/IP Port Nummer	3495	Standardmäßig wird Port 3495 für http:- und tcp-Protokolle benutzt.
SecurityLayer benutzt SSL Port Nummer	3496	Port 3496 ist für https: und tls voreingestellt
Widerrufslisten beim Start aus dem Internet beziehen	☑	Beim Start des trustDesk basic werden die aktuellen Widerrufslisten aus dem Internet geladen. Widerrufslisten werden benötigt, um die Gültigkeit von Zertifikaten zu prüfen. Sie sollten jedenfalls **vor** der Prüfung eines Zertifikates aktualisiert werden.
	☐	Die aktuellen Widerrufslisten werden beim Starten nicht geladen. Dies beschleunigt den Startvorgang.
SSL Client Authentifizierung erzwingen	☑	Die Authentifizierung von SSL Clients ist notwendig. Diese Option hat keine Auswirkung auf das SecurityLayer SSL Server Zertifikat. Der SecurityLayer selbst authentifiziert sich immer mit einem mitgelieferten SSL Server Zertifikat, dessen geheimer Schlüssel durch Triple-DES/CBC 168 Bit-Verschlüsselung geschützt ist.
	☐	SSL Clients müssen sich nicht notwendigerweise autentifizieren
Personenbindung auf Karte	☑	Die Personenbindung wird auf der Karte gespeichert
	☐	Die Personenbindung wird in einer virtuellen Infobox gespeichert.
XML Parser darf Internet verwenden um externe Schemas zu beziehen	☑	Der XML Parser darf eine Internetverbindung nutzen, um benötigte externe Schemas zu beziehen. Es wird empfohlen diese Funktion zu aktivieren.
	☐	Der XML Parser darf keine Internetverbindung nutzen, um benötigte externe Schemas zu beziehen. Es wird empfohlen diese Funktion zu aktivieren.
Auch Wurzelzertifikat in XML Signaturresponse hinzufügen	☑	Das Wurzelzertifikat wird bei XML Signatureresponses hinzugefügt.
	☐	Das Wurzelzertifikat wird bei XML Signatureresponses nicht hinzugefügt.

Name	Wert	Bedeutung
HTML Formularfelder	Entfernen	Leere Referenzen in HTML Formularfeldern werden entfernt.
	Durch Leerzeichen ersetzen	Leere Referenzen in HTML Formularfeldern werden durch Leerzeichen ersetzt
	Fehlermeldung	Bei leeren Referenzen in HTML Formularfeldern wird eine Fehlermeldung ausgegeben.

! *Folgende Ports in der (personal) Firewall müssen nach außen freigeschalten sein:*
389 – ldap service für Zertifikatsprüfung und CRL
443 – https
80 - http
8080 – E-Government-Applikationen und Online-Update

! *Die Änderungen werden erst aktiv, nachdem die Software trustDesk basic neu gestartet wurde, oder nachdem die betroffenen Protokoll-Bindungen innerhalb der Software einmal geschlossen und wieder geöffnet wurden.*

8.2 SSL Einstellungen

Liegt ein falscher Domänenname vor, kann wie folgt verfahren werden:

Eingabefelder

Name	Wert	Bedeutung
Bei falschem Domänennamen im SSL Serverzertifikat	Verbindung abbrechen	die Verbindung wird automatisch abgebrochen
	Verbindung trotzdem aufbauen	die Verbindung wird mit jeder Domäne aufgebaut
	Benutzer fragen	der Benutzer wird jedes Mal benachrichtigt und kann entscheiden, ob er die Verbindung zulassen möchte.

Buttons

Name	Bedeutung
OK	Die eingegebenen Werte werden übernommen, das Programm wird geschlossen.
Übernehmen	Die eingegebenen Werte werden übernommen, das Programm wird nicht geschlossen.
Abbrechen	Die eingegebenen Werte werden nicht übernommen, das Programm wird geschlossen.

8.3 Proxy Server

Eingabefelder

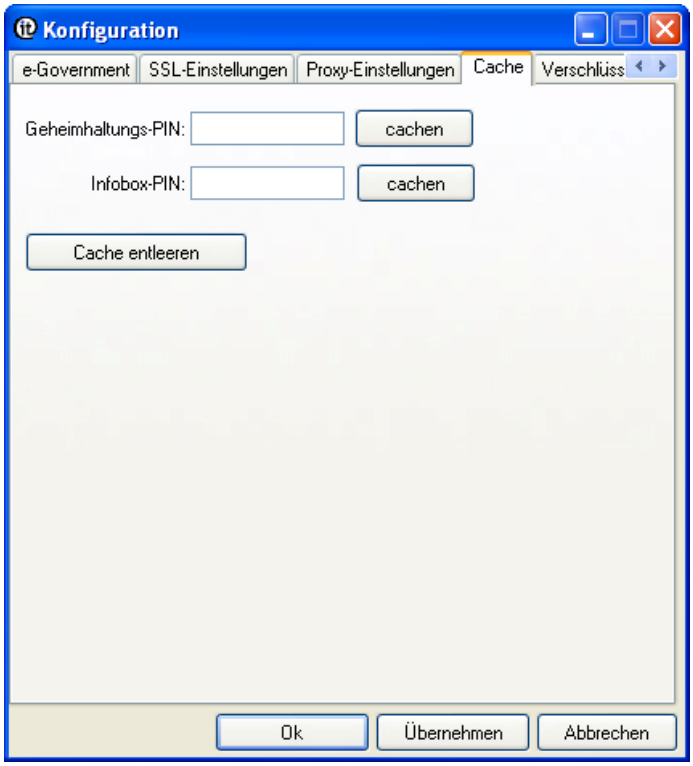
Name	Wert	Bedeutung
Proxy Server verwenden	☑	Soll ein Proxyserver verwendet werden, muss die Checkbox aktiviert sein.

Name	Wert	Bedeutung
	☐	Gibt an, dass keine Proxy Server verwendet werden soll.
Proxy		Name des Servers
Proxyserver für lokale Adressen umgehen	☑	Für lokale Adresse wird der Proxy nicht benutzt
	☐	Proxy wird auch für lokale Adressen benutzt
Für die Adressen, die wie folgt beginnen, keinen Proxyserver verwenden		
	servername; servername	Eingabe der Servernamen. Trennzeichen ist das Semikolon
Benutzer	Alphanumerisch	Benutzername für die Proxy Authentifizierung
Kennwort	Alphanumerisch	Kennwort für die Proxy Authentifizierung

Buttons

Name	Bedeutung
OK	Die eingegebenen Werte werden übernommen, das Programm wird geschlossen.
Übernehmen	Die eingegebenen Werte werden übernommen, das Programm wird nicht geschlossen.
Abbrechen	Die eingegebenen Werte werden nicht übernommen, das Programm wird geschlossen.

8.4 Cache



Eingabefelder

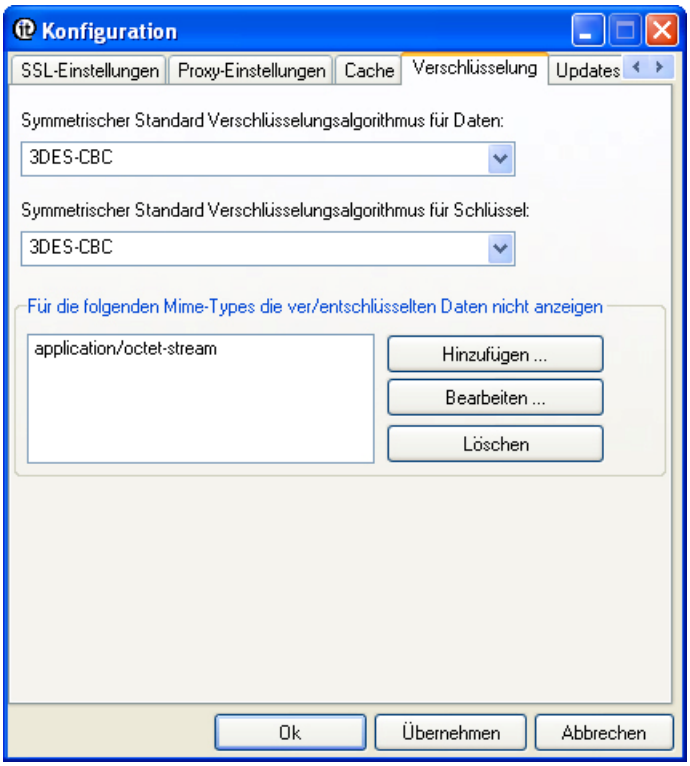
Name	Wert	Bedeutung
Geheimhaltungs-PIN		PIN wird nicht gespeichert
	0 -9	Wird die PIN eingegeben und anschließend **cachen** geklickt bleibt die Geheimhaltungs-PIN gespeichert und braucht nicht bei jedem Request eingegeben werden.
Infobox-PIN		PIN wird nicht gespeichert
	0 -9	Wird die PIN eingegeben und anschließend **cachen** geklickt bleibt die Geheimhaltungs-PIN gespeichert und braucht nicht bei jedem Request eingegeben werden.

Buttons

Name	Bedeutung
cachen	Die eingegebenen Werte werden übernommen.
Cache entleeren	Alle eingegebenen Werte werden aus dem Zwischenspeicher gelöscht.
OK	Die eingegebenen Werte werden übernommen, das Programm wird geschlossen.
Übernehmen	Die eingegebenen Werte werden übernommen, das Programm wird nicht geschlossen.
Abbrechen	Die eingegebenen Werte werden nicht übernommen, das Programm wird geschlossen.

8.5 Verschlüsselung

Hier stellen Sie ein, nach welchem Algorithmus die Verschlüsselung für Daten bzw. Schlüssel erfolgen soll.



Eingabefelder

Name	Gültige Werte	Bedeutung
Symetrischer Standard Verschlüsselungsalgorithmus für Daten	AES128-CBC | AES192-CBC | AES256-CBC | 3DES-CBC	
Symetrischer Standard Verschlüsselungsalgorithmus für Daten	AES128-CBC | AES192-CBC | AES256-CBC | 3DES-CBC	
	application/octet-stream	Gibt an, für welche mime-types die ver-/entschlüsselten Daten angezeigt werden sollen
	application/my-type	

Buttons

Name	Bedeutung
Hinzufügen	Die Eingabemaske für Mime Types wird aufgerufen.
Bearbeiten	Der markierte Datensatz kann auf einer Folgemaske bearbeitet werden.
Löschen	Der markierte Datensatz wird ohne weitere Warnmeldung gelöscht.
OK	Die eingegebenen Werte werden übernommen, das Programm wird geschlossen.

Name	Bedeutung
Übernehmen	Die eingegebenen Werte werden übernommen, das Programm wird nicht geschlossen.
Abbrechen	Die eingegebenen Werte werden nicht übernommen, das Programm wird geschlossen.

8.6 Online Update-Möglichkeit

Eingabefelder

Name	Gültige Werte	Bedeutung
	0	Es wird nicht nach Software Updates gesucht.
	1 - 24	Im angegebenen Intervall wird im Internet nach Aktualisierungen gesucht.

Buttons

Name	Bedeutung
OK	Die eingegebenen Werte werden übernommen, das Programm wird geschlossen.
Übernehmen	Die eingegebenen Werte werden übernommen, das Programm wird nicht geschlossen.
Abbrechen	Die eingegebenen Werte werden nicht übernommen, das Programm wird geschlossen.

9 E Government Funktionen

9.1 Security-Layer aktivieren bzw. deaktivieren

Durch einen Linksklick auf diese Option können Sie festlegen ob der Security-Layer aktiviert bzw. deaktiviert werden soll.

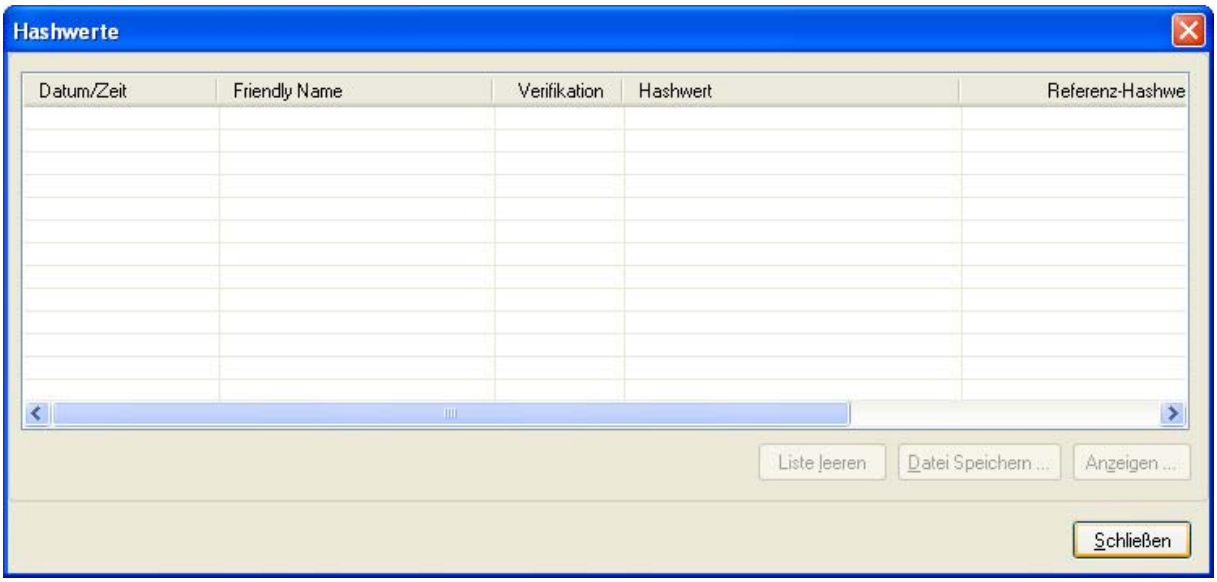
9.2 Security-Layer mit SSL aktivieren bzw. deaktivieren

Durch einen Linksklick auf diese Option können Sie festlegen ob der Security-Layer mit SSL aktiviert bzw. deaktiviert werden soll.

9.3 Hashwerte anzeigen

Ein Hashwert ist eine Prüfsumme die aus einem Dokument oder Datensatz berechnet wird. Die dabei verwendeten Hashalgorithmen sorgen dafür, dass derselbe Hashwert nicht für mehr als ein Dokument vergeben werden kann.

Durch die Funktion **Hashwert Anzeigen**, haben Sie die Möglichkeit, alle innerhalb der aktuellen Session generierten Hashwerte anzuzeigen.



Ausgabefelder

Name	Bedeutung
Datum/Zeit	
Friendly Name	
Hashwert	
Hashalgorithmus	

Buttons

Name	Bedeutung
Liste leeren	Die Liste der Hashwerte wird geleert
Datei speichern	Die Datei, zu der der Hashwert berechnet wurde, wird auf der Festplatte gespeichert
Anzeigen	Die Datei, zu der der Hashwert berechnet wurde, wird angezeigt. Manche Dokumente, wie z.B. .pdf Dateien, werden allerdings nicht in einem neuen Fenster geöffnet sondern mit der für die Ausführung dieser Dokumente benötigten Applikation aufgerufen.
Schließen	Das Fenster wird geschlossen.

9.4 Infobox Verwaltung

Infoboxen sind Datenspeicher, die Informationen in der Form von XML Dokumenten und/oder binären Daten enthalten. Es gibt zwei Arten von Infoboxen:

- Einfacher Speicher – enthält Daten
- Schlüsselspeicher – enthält einen oder mehrere Schlüssel

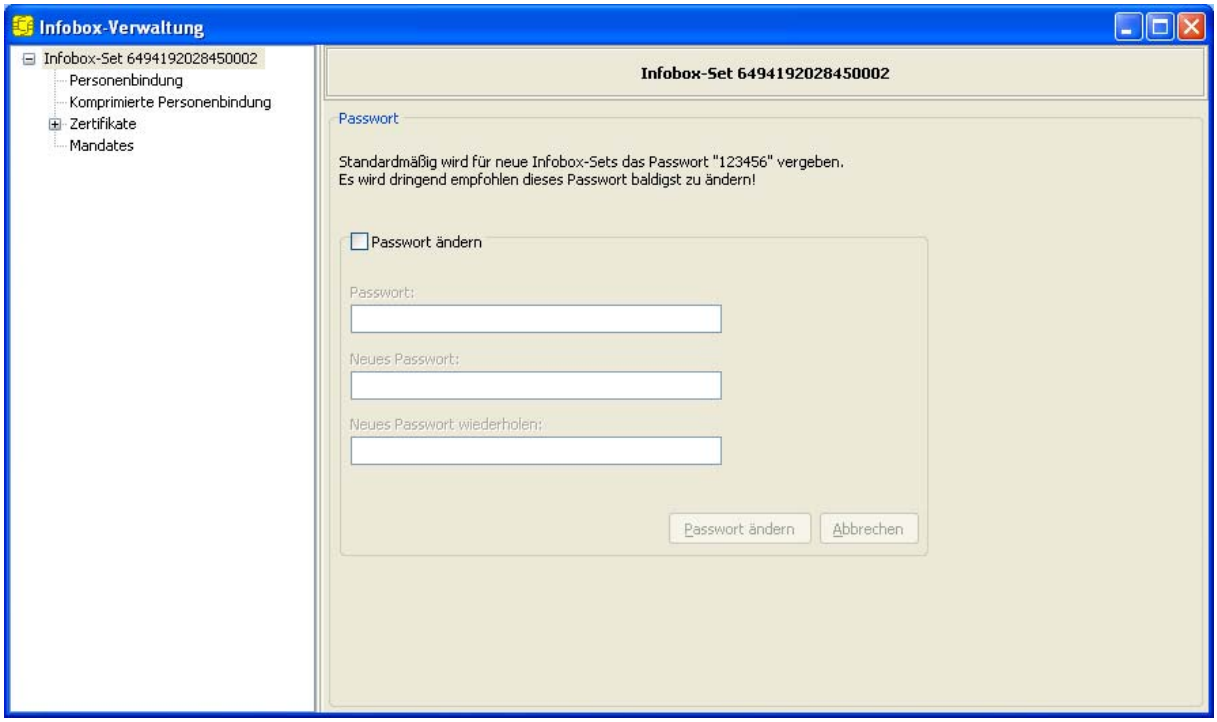
Mit der Infobox-Verwaltung können Sie in trustDesk basic Infoboxen auf Ihrer Festplatte speichern und administrieren, auch wenn Ihre Chipkarte das Speichern von Infoboxen nicht zulässt (oder zu wenig Speicherplatz besitzt).

Da Ihre Infobox-Sets der Bürgerkarte zugeordnet sind, muss sich die Karte zu dem Zeitpunkt in Ihrem Kartenlesegerät befinden.

Ist die Karte korrekt eingelegt, wird sie gelesen und die Infobox Verwaltung gestartet.

☞ Um die Karte während des Lesens zu wechseln, legen Sie die neue Bürgerkarte in ihr Kartenlesegerät ein, klicken mit der linken Maustaste in das weiße Feld der Maske und drücken Sie die F5.

Nach dem Lesen der Karte, sehen sie auf der linken Seite die Bezeichnung ihres Infobox-Sets.



Ein Infobox-Set besteht immer aus mehreren Infoboxen.

Die Infoboxen

- ❍ Personenbindung
- ❍ Komprimierte Personenbindung
- ❍ Zertifikate
- ❍ Mandates

sind auf allen Bürgerkarten vorhanden.

Eingabefelder

Name	Gültige Werte	Bedeutung
Passwort ändern	☐	Das Passwort kann nicht geändert weden

Name	Gültige Werte	Bedeutung
	☑	Die Passwortänderung ist aktiviert. Für neue Infobox-Sets wird standardmäßig das Passwort „123456“ vergeben. Es wird dringend empfohlen dieses Passwort schnellstmöglich gegen ein neues Passwort ihrer Wahl zu ersetzen!
Passwort	Alphanumerisch	
Passwort wiederholen	Alphanumerisch	

Buttons

Name	Bedeutung
Passwort ändern	Das Passwort wird geändert. Achten Sie bitte darauf ein Passwort zu verwenden, das Sie sich auch merken können. Haben Sie Ihr Passwort vergessen, kann es nicht wieder hergestellt werden. Der Zugriff auf die Infobox ist nicht mehr möglich.
Abbrechen	Eingegebene Daten werden nicht gespeichert. Das Programm muss mit dem roten x geschlossen werden.

9.5 Neuen einfachen Speicher oder Schlüsselspeicher anlegen

Die Infobox Verwaltung bietet die Möglichkeit neue Speicher sowohl auf der Karte, als auch auf der Festplatte anzulegen.

Klicken Sie bitte mit der rechten Maustaste in das leere weiße Feld im linken Bereich des Fensters. Im darauf folgenden Menü, wählen Sie **Neuen einfachen Speicher anlegen** bzw. **Neuen Schlüsselspeicher anlegen.** Unter der Bezeichnung „Unbenannt“ finden Sie den neuen Speicher oder Schlüsselspeicher nun in der Liste. Benennen Sie nun den angelegten einfachen Speicher oder Schlüsselspeicher um.

! *Bitte beachten Sie, dass es nicht möglich ist zwei einfache Speicher oder Schlüssel mit der gleichen Bezeichnung zu versehen. Es ist daher notwendig die Bezeichnung eines neu angelegten einfachen Speichers immer zu ändern, bevor ein weiterer einfacher Speicher angelegt wird.*

9.5.1 Schlüssel in Schlüsselspeicher anlegen

Klicken Sie bitte mit der rechten Maustaste auf den Schlüsselspeicher, in dem Sie den neuen Schlüssel anlegen möchten. Im darauf folgenden Menü, wählen Sie **Neuen Schlüssel anlegen.** Unter der Bezeichnung „Unbenannt“ finden Sie den neuen Schlüssel nun in der Liste. Benennen Sie nun den angelegten einfachen Schlüssel um.

! *Bitte beachten Sie, dass es nicht möglich ist zwei Schlüssel im selben Schlüsselspeicher mit der gleichen Bezeichnung zu versehen. Es ist daher notwendig die Bezeichnung eines neu angelegten einfachen Speichers immer zu ändern, bevor ein weiterer einfacher Speicher angelegt wird.*

9.6 Bezeichnung ändern

Durch einen Rechtsklick auf die Bezeichnung einfachen Speichers, Schlüsselspeichers oder Schlüssels, können Sie über die Auswahl **Umbenennen** die Bezeichnung ändern.

9.7 Schlüssel aus Schlüsselspeicher löschen

Zum Löschen wählen Sie den Schlüssel mit Rechtsklick und Klicken auf die Auswahl **Schlüssel löschen.**

☞ Bitte beachten Sie, dass die Schlüssel „Signaturzertifikat“ und „Entschlüsselungszertifikat“ ihrer Bürgerkarte nicht gelöscht werden können.

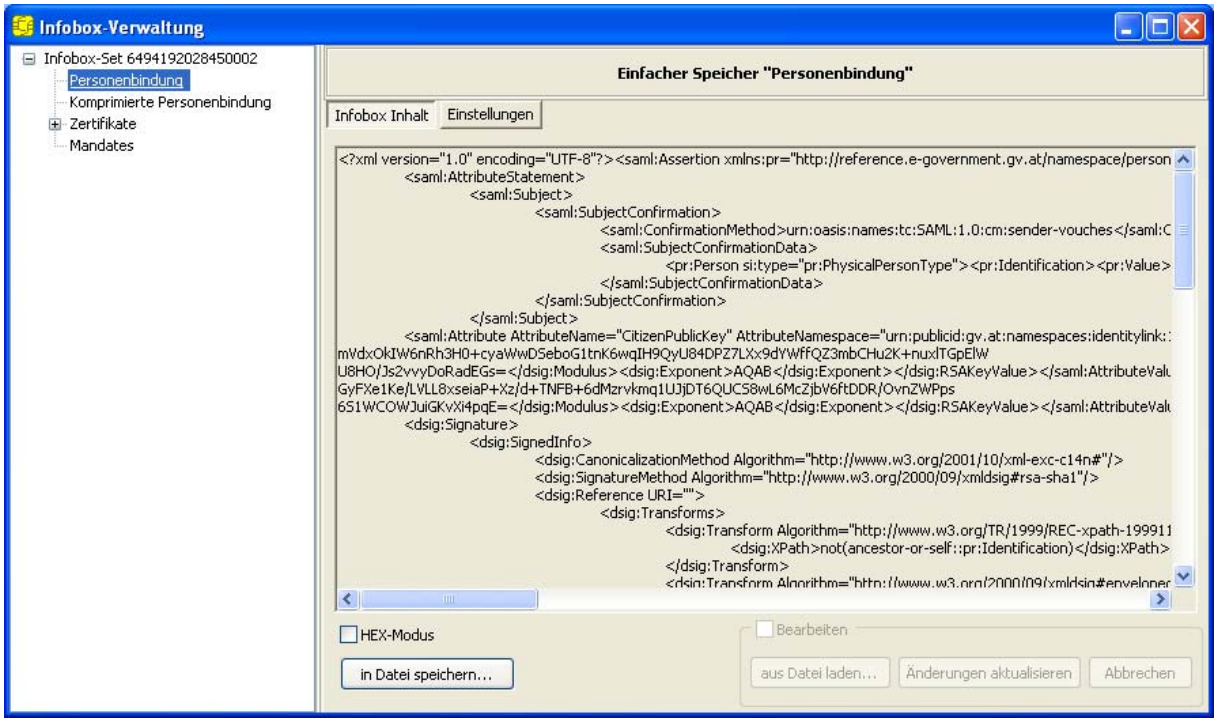
9.8 Infobox löschen

Um eine Infobox (einfacher Speicher oder Schlüsselspeicher) zu löschen, wählen Sie die Infobox durch Rechtsklicken auf die Bezeichnung aus. Wählen Sie den Punkt **Infobox löschen**. Die gewählte Infobox wird aus der Liste gelöscht.

☞ Bitte beachten Sie dass die Infoboxen „Personenbindung“, „Komprimierte Personenbindung“, „Zertifikate“ und „Mandates“ ihrer Bürgerkarte nicht gelöscht werden können.

9.9 Inhalte anzeigen

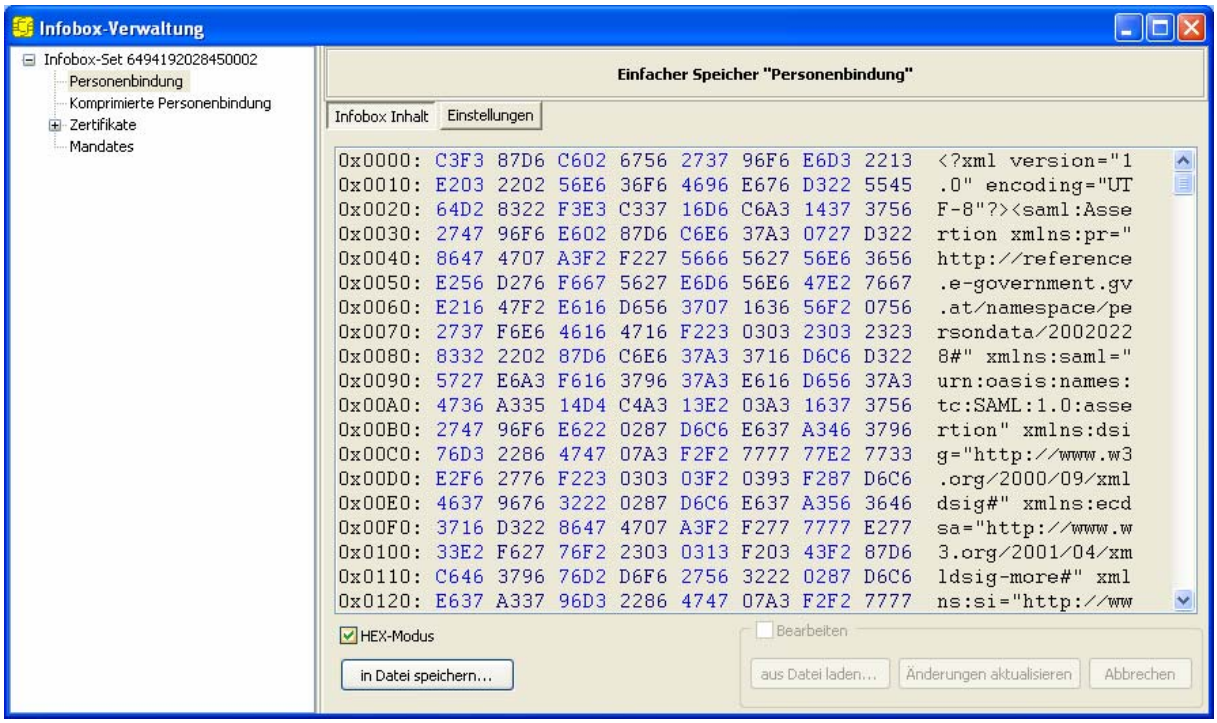
Wählen Sie den einfachen Speicher oder den Schlüsselspeicher durch Klick auf die Bezeichnung aus. Die Inhalte des gewählten Speichers werden in der rechten Fensterhälfte angezeigt. Für einfache Speicher und Schlüssel können sowohl der Infobox Inhalt als auch die Einstellungen angezeigt werden, für Schlüsselspeicher können nur die Einstellungen angezeigt werden.



Bei einem einfachen Speicher und bei Schlüsseln wird zuerst der Infobox Inhalt angezeigt. Diesen Inhalt sehen Sie in der Mitte des Fensters. Schlüssel müssen einzeln aus den Schlüsselspeichern gewählt werden:

Mit Hilfe der **Scrollbalken** können Sie den gesamten Inhalt ansehen.

Wird die Checkbox **HEX-Modus** aktiviert, werden die Daten im Hexadezimalsystem angezeigt.



In Datei speichern... öffnet einen Dateidialog mit dessen Hilfe der Inhalt der Infobox in eine Datei exportiert werden kann.

9.10 Einfacher Speicher - Inhalte ändern

Zum Bearbeiten aktivieren Sie die Checkbox **Bearbeiten.** Die Daten können nun direkt in der Anzeige bearbeitet werden.

☞ Bitte beachten Sie das die Infoboxen „Personenbindung“ und „Komprimierte Personenbindung“, „Signaturzertifikat“ und „Entschlüsselungszertifikat“ nicht editiert werden können.

Durch einen erneuten Klick auf die Checkbox **Bearbeiten** verlassen Sie den Bearbeitungsmodus, ohne die Änderungen zu speichern.

Die Änderungen bleiben hierbei jedoch in der Anzeige stehen und können durch erneutes Aufrufen des Bearbeitungsmodus mit Klick auf **Änderungen aktualisieren** auf die Infobox geschrieben werden.

Ebenfalls besteht die Möglichkeit Daten für ihre Infobox aus einer Datei zu laden. Betätigen Sie **aus Datei laden**. Über den folgenden Dateidialog wählen Sie die Datei aus, die die Daten, die geladen werden sollen, enthält.

Durch einen Klick auf **Abbrechen**, können Sie aus dem Bearbeitungsmodus aussteigen, ohne die vorgenommenen Änderungen zu speichern. Die Änderungen gehen dabei verloren.

9.11 Einstellungen anzeigen und ändern

Um die Einstellungen der Infobox anzuzeigen oder zu bearbeiten, klicken Sie auf die Auswahl **Einstellungen**. Die Einstellungen können sowohl für einfache Speicher als auch für Schlüsselspeicher angezeigt und geändert werden.

Ersteller

Hier können Sie den Namen des Erstellers der Infobox eingeben.

Zweck

Hier können Sie den Zweck, also eine Beschreibung des Inhaltes dieser Infobox eingeben.

9.12 PIN und PUK für Smartcards

trustDesk basic bietet die Möglichkeit, die PIN auf Ihrer Karte zu ändern bzw. eine gesperrte PIN mit einem PUK zu entsperren.

9.12.1 PIN Änderung

Hier haben Sie die Möglichkeit die PINs Ihrer Karte zu ändern. Dazu ist es erforderlich das die Karte korrekt im Kartenlesegerät eingelegt ist.

Vorerst müssen Sie auswählen, welche PIN geändert werden soll.

! *Welche PINs geändert werden dürfen, ist von der Art Ihrer Karte abhängig.*

Klicken Sie die PIN die Sie verändern möchten und anschließend auf **Ok.**

Folgen Sie diesen Anweisungen, um die PIN-Änderung durchzuführen. Nach erfolgter Änderung erhalten Sie eine Bestätigungsmeldung.

9.12.2 Fehler bei der PIN Eingabe

Sollte Ihnen bei der Eingabe Ihrer alten oder neuen PIN ein Fehler unterlaufen oder ungültig sein, erscheint eine Fehlermeldung.

! *Je nach Karte und Trustcenter ist die Anzahl der erlaubten Fehlversuche bei PIN Eingabe mit Smartcards beschränkt! Für gewöhnlich wird nach der dritten Fehleingabe die betroffene Smartcard gesperrt und ist permanent deaktiviert.*

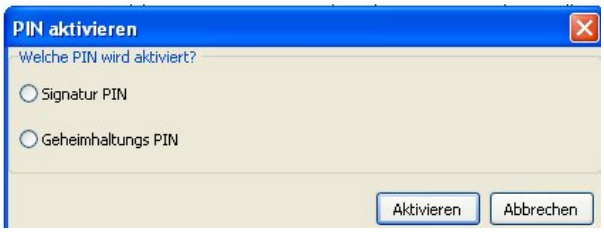
9.13 PIN aktivieren (e-Card und o-Card)

Bei e-Cards und o-Cards muss die PIN aktiviert werden.

Dazu ist es erforderlich das sich die betreffende Smartcard korrekt eingelegt in Ihrem Kartenlesegerät befindet.

Zuerst erhalten Sie ein Fenster mit wichtigen Hinweisen zur PIN Aktivierung. Bitte lesen Sie dieses aufmerksam durch.

Klicken Sie auf **OK** um mit der Aktivierung fortzufahren oder auf **Abbrechen** um die Aktivierung abzubrechen.



☞ Ist eine PIN bereits aktiviert, kann sie nicht mehr zur Aktivierung ausgewählt werden.

Durch Klick auf **Aktivieren** werden Sie aufgefordert zweimal ihre PIN einzugeben.

☞ Warten Sie bis die Eingabefelder für die PIN zu sehen sind, da vorheriges Eingeben nicht zielführend ist.

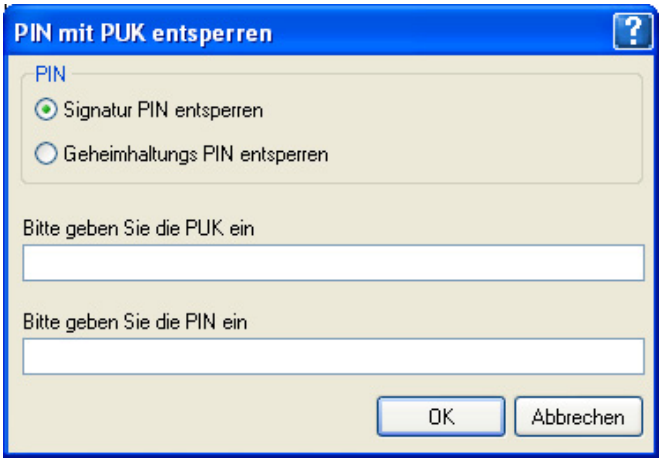
! *Manche Kartenlesegeräte unterstützen das Setzen einer InitialPIN nur über die PIN Änderungsfunktion. In diesem Fall müssen Sie eine beliebige alte PIN eingeben.*

! *Bei Kartenleser SPR 532 und bei Chipdrive Pinpad pro ist es notwendig N U R F Ü R D I E A K T I V I E R U N G auf den PCSC Treiber und erlauben die PIN Eingabe für Software (= Tastatur) umzuschalten. Anschließend schalten Sie wieder auf den CTAPI Treiber um und Sie können mit der aktivierten Karte arbeiten.*

9.14 Karte mittels PUK entsperren

Hier haben Sie die Möglichkeit die PINs Ihrer Karte zu entsperren.

Dazu ist es erforderlich das sich die Karte korrekt eingelegt in Ihrem Kartenlesegerät befindet.



Legen Sie fest, welche PIN entsperrt werden soll geben Sie diese PIN sowie Ihren PUK ein.

Durch Klick auf **OK** wird die Entsperrung durchgeführt, mit **Abbrechen** können Sie den Vorgang jederzeit beenden.

☞ Dieser Vorgang ist bei manchen Karten (z.B. a.sign premium) nur mit der Geheimhaltungs PIN möglich, nicht aber mit der Signatur PIN. Für nähere Fragen wenden Sie sich bitte an jenes Trustcenter, welches Ihre Signaturkarte ausgestellt hat.

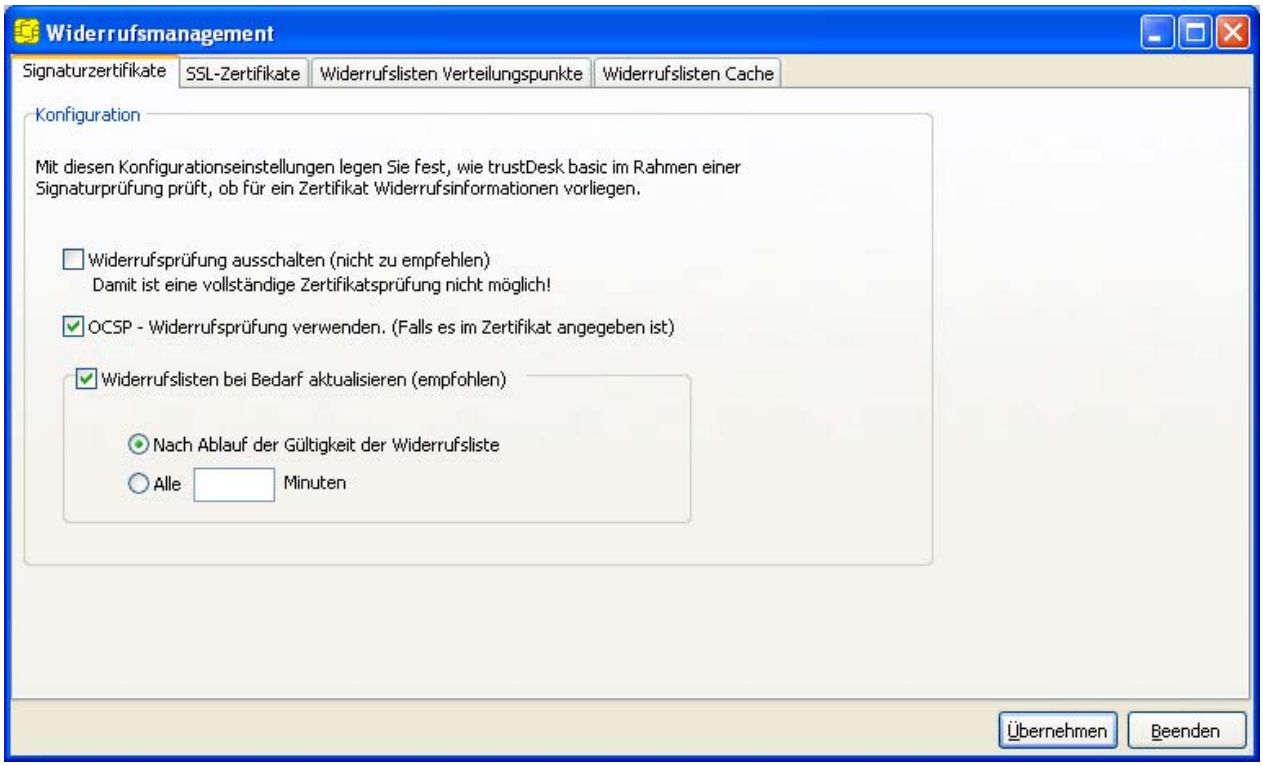
10 Widerrufsmanagement

Um die Gültigkeit von Zertifikaten überprüfen zu können, werden so genannte Widerrufslisten benötigt.

10.1 Signatur- und SSL Zertifikate

Mit diesen Konfigurationseinstellungen legen Sie fest, wie das Vorliegen von Widerrufsinformationen geprüft wird. Diese Informationen können festgelegt werden für

- ❍ Signaturzertifikate im Rahmen einer Signaturprüfung
- ❍ SSS-Zertifikate im Rahmen eines SSL-Verbindungsaufbaus zu einem Applikationsserver



Eingabefelder

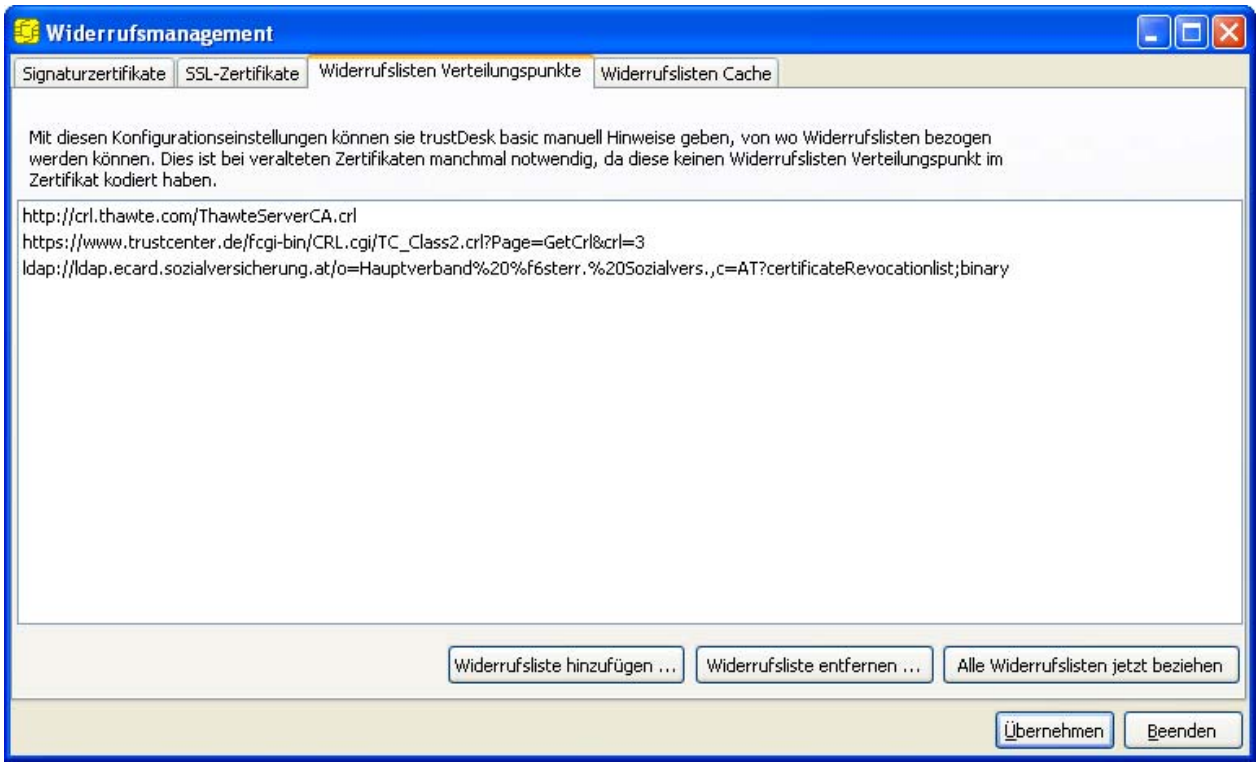
Name	Wert	Bedeutung
Widerrufsprüfung ausschalten	☑	Widerrufsprüfung wird nicht durchgeführt. Eine sinnvolle Signaturprüfung ist unter diesen Umständen nicht mehr möglich, da nicht sicher festgestellt werden kann, ob das Zertifikat zum Signaturzeitpunkt gültig war.
	☐	Widerrufsprüfung wird durchgeführt
OCSP Widerrufsprüfung verwenden	☑	Wenn im Zertifikat angegeben wird OCSP zur Widerrufsprüfung verwendet.
	☐	Es wird nie über OCSP eine Widerrufsprüfung gemacht
Nach Ablauf der Gültigkeit der Widerrufsliste	☑	Widerrufsliste wird nach Ablauf ihrer Gültigkeit aktualisiert
	☐	
Alle xx Minuten	1 - 60	Die Widerrufsliste wird im angegebenen Intervall aktualisiert

Buttons

Name	Bedeutung
Übernehmen	Die eingegebenen Werte werden übernommen, das Programm wird nicht geschlossen.
Beenden	Die eingegebenen Werte werden übernommen, das Programm wird geschlossen.

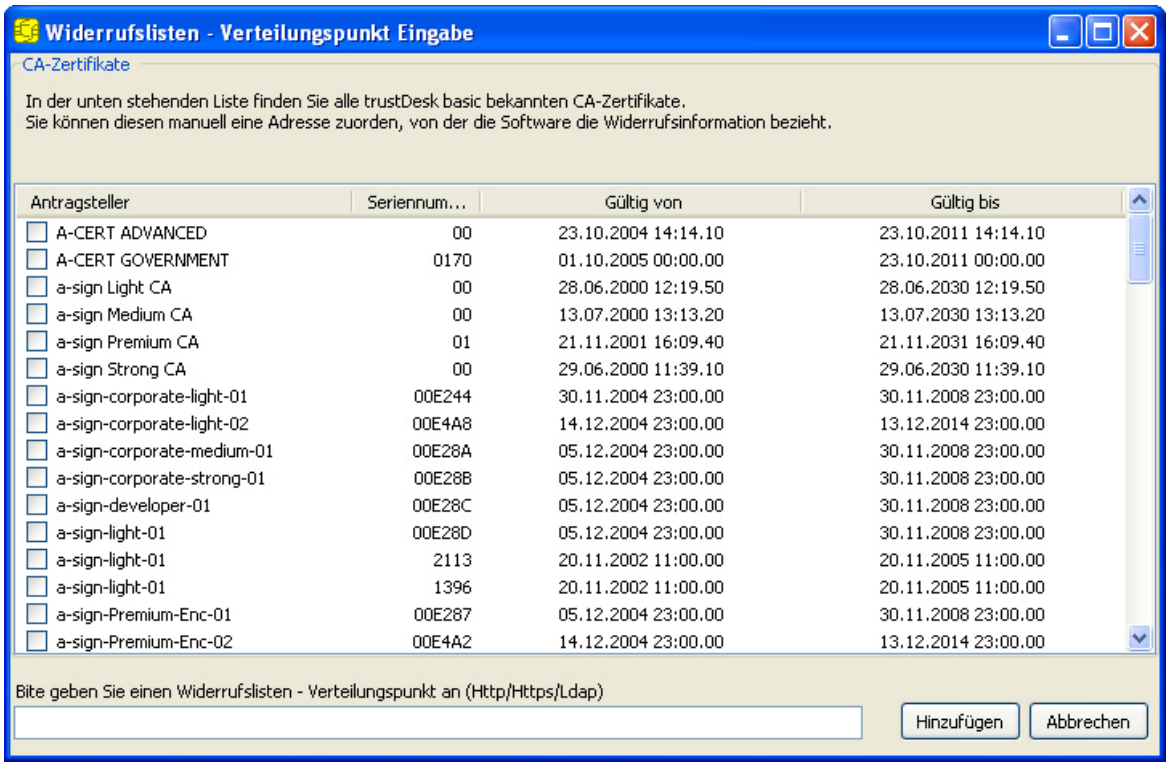
10.2 Widerrufslisten Verteilungspunkte

Bei einigen älteren Zertifikaten ist es notwendig die Verteilungspunkte also die Internetadressen an denen sich diese Widerrufslisten befinden manuell anzugeben. Hier haben Sie die Gelegenheit die Adressen dieser Widerrufslisten einzutragen um trustDesk basic den Bezug dieser Widerrufslisten zu ermöglichen.



Widerrufsliste hinzufügen

Die Liste aller als vertrauenswürdig eingestuften Wurzelzertifikate wird aufgelistet.



Durch Aktivierung der Checkbox neben der Bezeichnung eines Wurzelzertifikates können Sie die Wurzelzertifikate auswählen für die ein neuer Widerrufslisten-Verteilungspunkt angegeben werden soll. Tragen Sie die Adresse des Widerrufslisten-Verteilungspunktes in das Textfeld ein.

! *Es muss sich dabei um eine gültige http, Https oder Ldap Adresse handeln.*

Durch einen Klick auf **Hinzufügen** können Sie den ausgewählten Wurzelzertifikaten die im Textfeld eingegebene Widerrufslisten-Verteilungspunkt Adresse zuordnen.

Durch einen Klick auf **Abbrechen** schließen Sie das Fenster ohne Änderungen vorzunehmen.

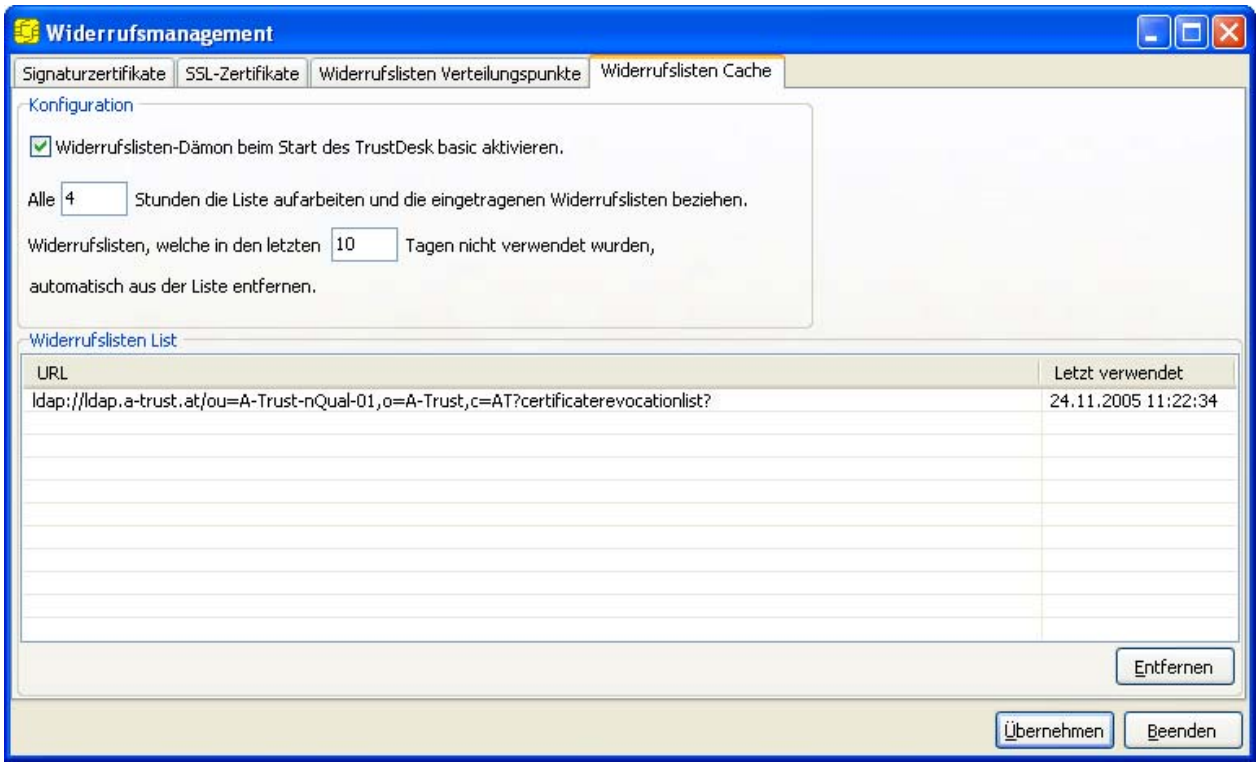
Widerrufsliste entfernen

Wählen Sie die Widerrufsliste, die entfernt werden mittels Klick aus der Liste aus. Wenn Sie die **Strg Taste** gedrückt halten, während Sie Widerrufslisten auswählen, können Sie mehrere Widerrufslisten auswählen. Betätigen Sie **Widerrufsliste entfernen**, die ausgewählten Widerrufslisten werden ohne weitere Rückfrage gelöscht.

Alle Widerrufslisten jetzt beziehen

Durch Klick auf **Alle Widerrufslisten jetzt beziehen** können Sie trustDesk basic dazu veranlassen sämtliche in der Liste befindlichen Widerrufslisten sofort aus dem Internet zu beziehen. Nachdem alle Widerrufslisten aktuell heruntergeladen sind, erhalten Sie eine Meldung.

Der **Widerrufslisten Dämon** dient dazu häufig benötigte Widerrufslisten in gewissen Zeitabständen zu **aktualisieren**. Dies bietet den Vorteil das die Widerrufslisten sobald Sie gebraucht werden nicht mehr neu heruntergeladen werden müssen vorrausgesetzt das sie noch aktuell sind.



Eingabefelder

Name	Wert	Bedeutung
Widerrufsdämon beim Starten von trustDesk aktivieren	☑	Widerrufsdämon wird gestartet. Dies verzögert den Aufruf des Programmes
	☐	Dämon wird nicht gesartet
Alle xx Stunden die Liste aufarbeiten und die eingetragenen Widerrufslisten beziehen	2 - 24	Zeitintervall, in dem der Dämon die Widerrufslisten auf Ihre Aktualität hin überprüfen und gegebenenfalls neu bezieht
Widerrufslisten, die in den letzten xx Tagen nicht benutzt wurden aus der Liste entfernen	2 - 24	Zeitraum, nach dessen Ablauf eine unbenutzte Widerrufsliste aus der Liste entfernt werden soll.

Buttons

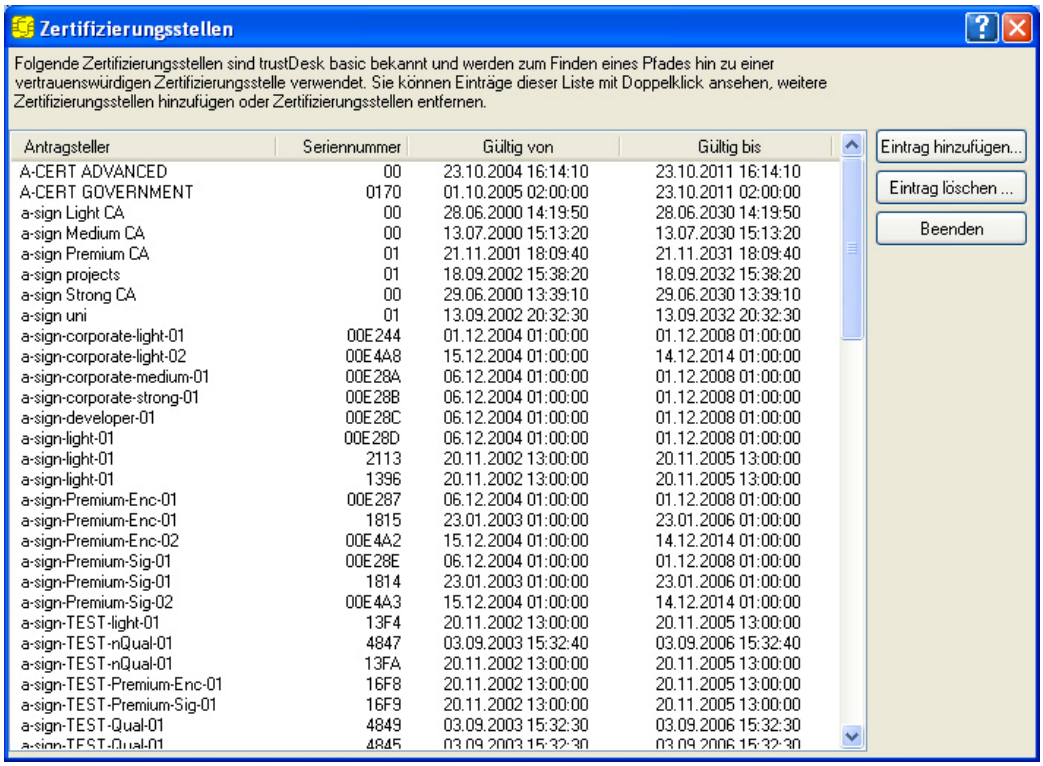
Name	Bedeutung
Entfernen	Entfernt die markierte Widerrufsliste ohne weitere Warnmeldung
Übernehmen	Die eingegebenen Werte werden übernommen, das Programm wird nicht geschlossen.

Beenden	Die eingegebenen Werte werden übernommen, das Programm wird geschlossen.

11 (Vertrauenswürdige) Zertifizierungsstellen

Hier haben Sie die Möglichkeit die Zertifizierungsstellen bzw. die als vertrauenswürdig eingestuften Zertifizierungsstellen zu Verwalten die trustDesk basic bekannt sind. Die hier eingetragenen Zertifizierungsstellen werden verwendet um einen Pfad zu einer vertrauenswürdigen Zertifizierungsstelle zu finden.

Ziehen Sie Ihren Mauszeiger über einer bestimmten Zertifizierungsstelle, werden Aussteller und Antragssteller des Wurzelzertifikates der betreffenden Zertifizierungsstelle angezeigt. Durch einen Doppelklick auf eine der Zertifizierungsstellen können Sie sich zusätzliche Informationen zu dem Wurzelzertifikat dieser Zertifizierungsstelle in einem neuen Fenster anzeigen lassen. Durch einen Klick auf **Beenden** können Sie das Fenster schließen.



Antragsteller	Seriennummer	Gültig von	Gültig bis
A-CERT ADVANCED	00	23.10.2004 16:14:10	23.10.2011 16:14:10
A-CERT GOVERNMENT	0170	01.10.2005 02:00:00	23.10.2011 02:00:00
a-sign Light CA	00	28.06.2000 14:19:50	28.06.2030 14:19:50
a-sign Medium CA	00	13.07.2000 15:13:20	13.07.2030 15:13:20
a-sign Premium CA	01	21.11.2001 18:09:40	21.11.2031 18:09:40
a-sign projects	01	18.09.2002 15:38:20	18.09.2032 15:38:20
a-sign Strong CA	00	29.06.2000 13:39:10	29.06.2030 13:39:10
a-sign uni	01	13.09.2002 20:32:30	13.09.2032 20:32:30
a-sign-corporate-light-01	00E244	01.12.2004 01:00:00	01.12.2008 01:00:00
a-sign-corporate-light-02	00E4A8	15.12.2004 01:00:00	14.12.2014 01:00:00
a-sign-corporate-medium-01	00E28A	06.12.2004 01:00:00	01.12.2008 01:00:00
a-sign-corporate-strong-01	00E28B	06.12.2004 01:00:00	01.12.2008 01:00:00
a-sign-developer-01	00E28C	06.12.2004 01:00:00	01.12.2008 01:00:00
a-sign-light-01	00E28D	06.12.2004 01:00:00	01.12.2008 01:00:00
a-sign-light-01	2113	20.11.2002 13:00:00	20.11.2005 13:00:00
a-sign-light-01	1396	20.11.2002 13:00:00	20.11.2005 13:00:00
a-sign-Premium-Enc-01	00E287	06.12.2004 01:00:00	01.12.2008 01:00:00
a-sign-Premium-Enc-01	1815	23.01.2003 01:00:00	23.01.2006 01:00:00
a-sign-Premium-Enc-02	00E4A2	15.12.2004 01:00:00	14.12.2014 01:00:00
a-sign-Premium-Sig-01	00E28E	06.12.2004 01:00:00	01.12.2008 01:00:00
a-sign-Premium-Sig-01	1814	23.01.2003 01:00:00	23.01.2006 01:00:00
a-sign-Premium-Sig-02	00E4A3	15.12.2004 01:00:00	14.12.2014 01:00:00
a-sign-TEST-light-01	13F4	20.11.2002 13:00:00	20.11.2005 13:00:00
a-sign-TEST-nQual-01	4847	03.09.2003 15:32:40	03.09.2006 15:32:40
a-sign-TEST-nQual-01	13FA	20.11.2002 13:00:00	20.11.2005 13:00:00
a-sign-TEST-Premium-Enc-01	16F8	20.11.2002 13:00:00	20.11.2005 13:00:00
a-sign-TEST-Premium-Sig-01	16F9	20.11.2002 13:00:00	20.11.2005 13:00:00
a-sign-TEST-Qual-01	4849	03.09.2003 15:32:30	03.09.2006 15:32:30
a-sign-TEST-Qual-01	4845	03.09.2003 15:32:30	03.09.2006 15:32:30

Durch einen Klick auf **Eintrag hinzufügen** können Sie Ihrer Liste neue Zertifizierungsstellen hinzufügen. Geben den Namen des Wurzelzertifikats der betreffenden Zertifizierungsstelle ein, oder wählen Sie es mit Doppelklick direkt von Ihrer Festplatte aus.

☞ Bitte beachten Sie das Zertifizierungsstellen die der Liste der vertrauenswürdigen Zertifizierungsstellen hinzugefügt werden gleichzeitig auch der Liste der herkömmlichen Zertifizierungsstellen hinzugefügt werden.

Wählen Sie die Zertifizierungsstelle aus und Klicken Sie auf' **Eintrag löschen**. Sie erhalten ein Dialogfenster in dem Sie das Löschen bestätigen müssen. Erst danach wird die Zertifizierungsstelle wirklich gelöscht wird.

11.1 Sicherheitsverwaltung

trustDesk basic bietet Ihnen eine umfangreiche Sicherheitsverwaltung an, die es Ihnen erlaubt, zweifelhafte Server und SSL Zertifikate zu blockieren.

Überprüfung anhand von URLs

Wurde im Konfigurationsprogramm von trustDesk basic die Option **Sicherheitsverwaltung aktivieren (Überprüfung von URLs)** aktiviert, werden Sie vor jedem Datenaustausch mit einem Server informiert, wohin die Daten geschickt werden und müssen bestätigen, dass Sie dies zulassen möchten.

Handelt es sich dabei um eine sichere https Verbindung, so können Sie das Serverzertifikat dieses Servers durch einen Klick auf **Serverzertifikat anzeigen** anzeigen.

Wenn Sie in der Auswahlbox **zulassen** auswählen, werden die Daten übertragen, wählen Sie jedoch **ablehnen**, wird der Vorgang ohne Daten zu übertragen abgebrochen.

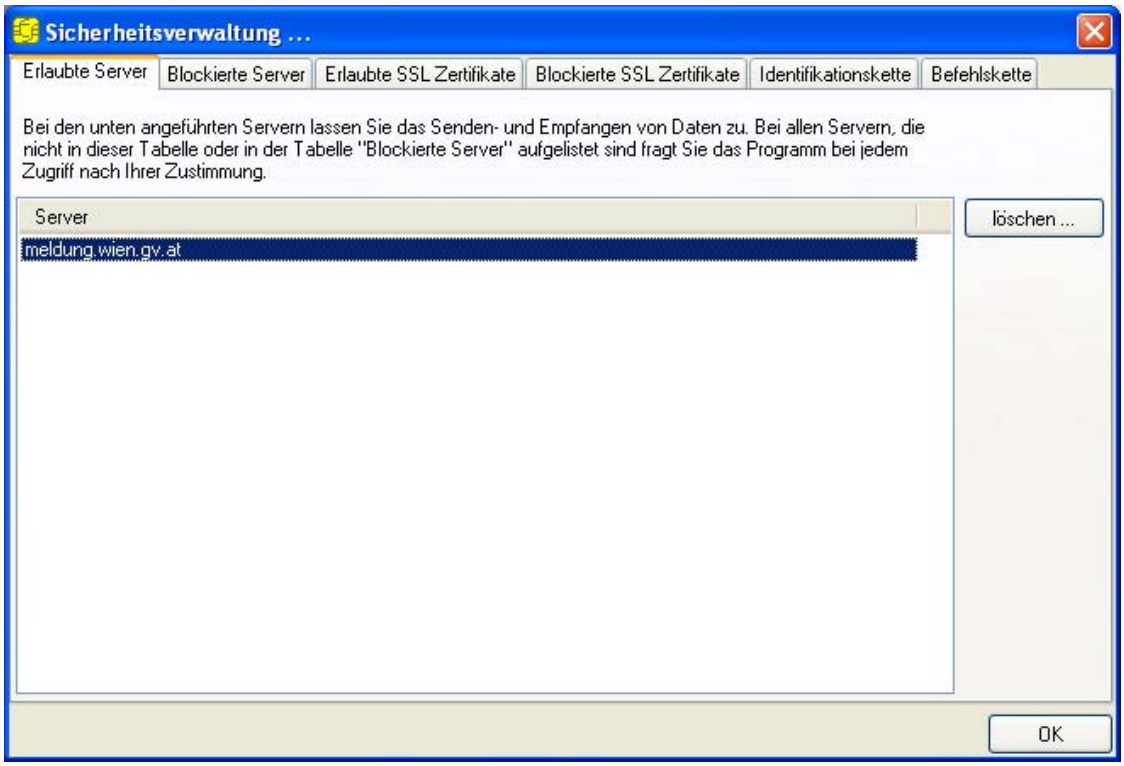
Da dieser Vorgang bei jeder Datenübertragung etwas aufwändig ist, können über die Checkbox **Für diesen Server immer die oben gewählte Einstellung verwenden** in Kombination mit der der Auswahlbox die Option **zulassen** wählen, wodurch bei Kommunikation mit diesem Server die Information und die Notwendigkeit der Bestätigung entfällt (= erlaubter Server). Die gegenteilige Wirkung hat die Checkbox in Kombination mit der Option **ablehnen** in der Auswahlbox. Dieser Server wird in die Liste der blockierten Server aufgenommen und es findet keine Datenübertragung statt.

Hier sehen Sie die Sicherheitsabfrage bei aktivierter Überprüfung von URLs bei http Protokoll

Diese Maske zeigt die Sicherheitsabfrage bei aktivierter Überprüfung von URLs bei https Protokoll

Erlaubte Server

Diese Liste zeigt jene Server, die Sie mit dem oben beschriebenen Vorgang als „vertrauenswürdig“ definiert haben.

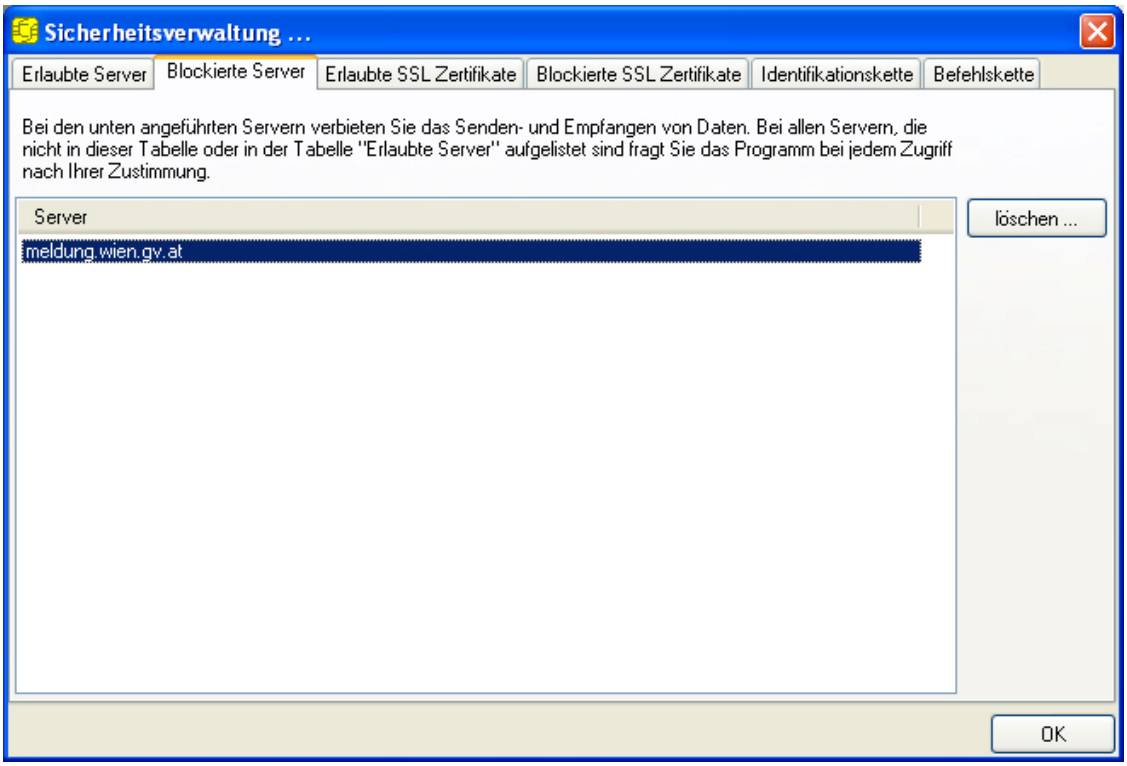


Möchten Sie einen der Server entfernen, markieren Sie ihn mit einem Linksklick und Klick auf **löschen**.

- Dieser Server wird aus der Liste der erlaubten Server gelöscht
- Bei der nächsten Kommunikation mit diesem Server findet eine Sicherheitsabfrage statt.

Blockierte Server

Diese Liste zeigt jene Server, die Sie mit dem oben beschriebenen Vorgang als „unsicher“ definiert haben.



Möchten Sie einen der Server entfernen, markieren Sie Ihn mit einem Linksklick und Klick auf **löschen**.

- ❍ Dieser Server wird aus der Liste der blockierten Server gelöscht
- ❍ Bei der nächsten Kommunikation mit diesem Server findet eine Sicherheitsabfrage statt.

11.2 SSL Client Authentifizierung

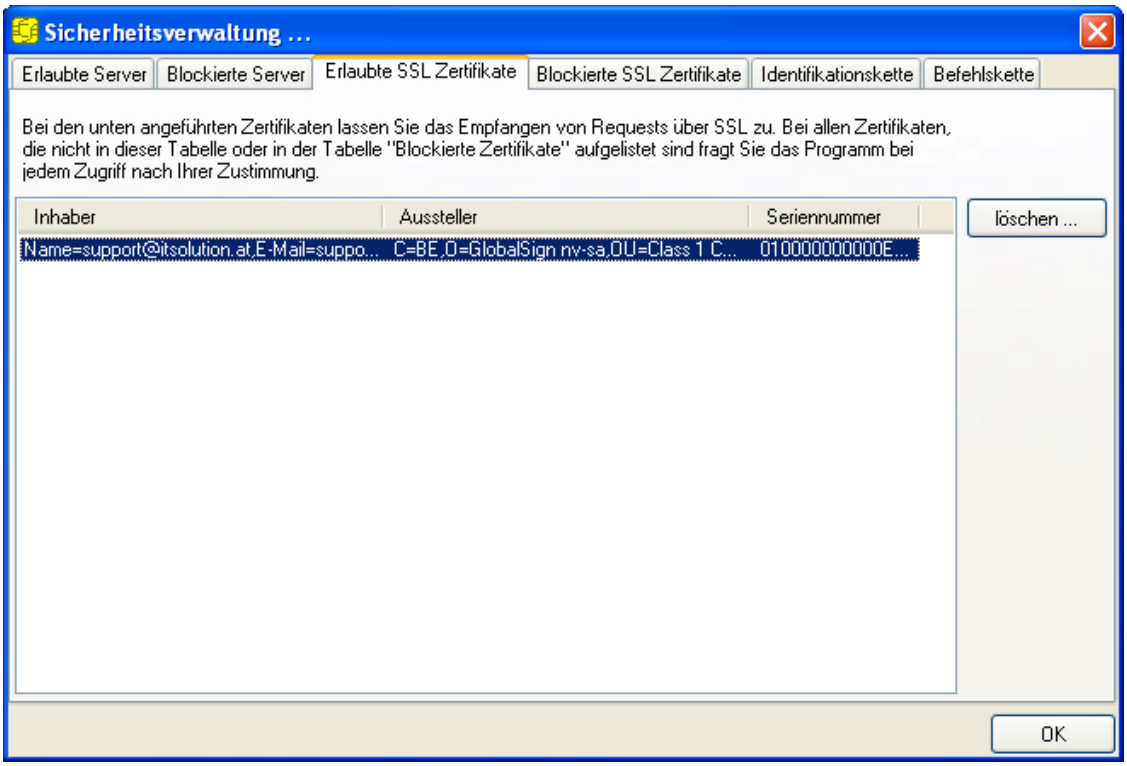
Wurde im Konfigurationsprogramm von trustDesk basic die Option **SSL Client Authentifizierung erzwingen** aktiviert, werden Sie bei jedem Versuche einer SSL Kommunikation einer Applikation mit dem Security-Layer, informiert und müssen bestätigen, dass Sie dies zulassen möchten.

Wenn Sie in der Auswahlbox **zulassen** auswählen, findet die Kommunikation statt, wählen Sie jedoch **ablehnen**, wird der Vorgang abgebrochen.

Da diese Vorgehensweise bei jede versuchten Kommunikation etwas aufwändig ist, können über die Checkbox **Für dieses Zertifikat immer die oben gewählte Einstellung verwenden** in Kombination mit der der Auswahlbox die Option **zulassen** wählen, wodurch bei Kommunikation bei diesem Zertifikat immer stattfindet. Die Information und die Notwendigkeit der Bestätigung entfällt (= erlaubtes SSL Zertifikat). Die gegenteilige Wirkung hat die Checkbox in Kombination mit der Option **ablehnen** in der Auswahlbox. Dieses Zertifikat wird in die Liste der blockierten Zertifikate aufgenommen und es findet keine Kommunikation statt.

Erlaubte SSL Zertifikate

Diese Liste zeigt jene Zertifikate, die Sie mit dem oben beschriebenen Vorgang als „vertrauenswürdig“ definiert haben.

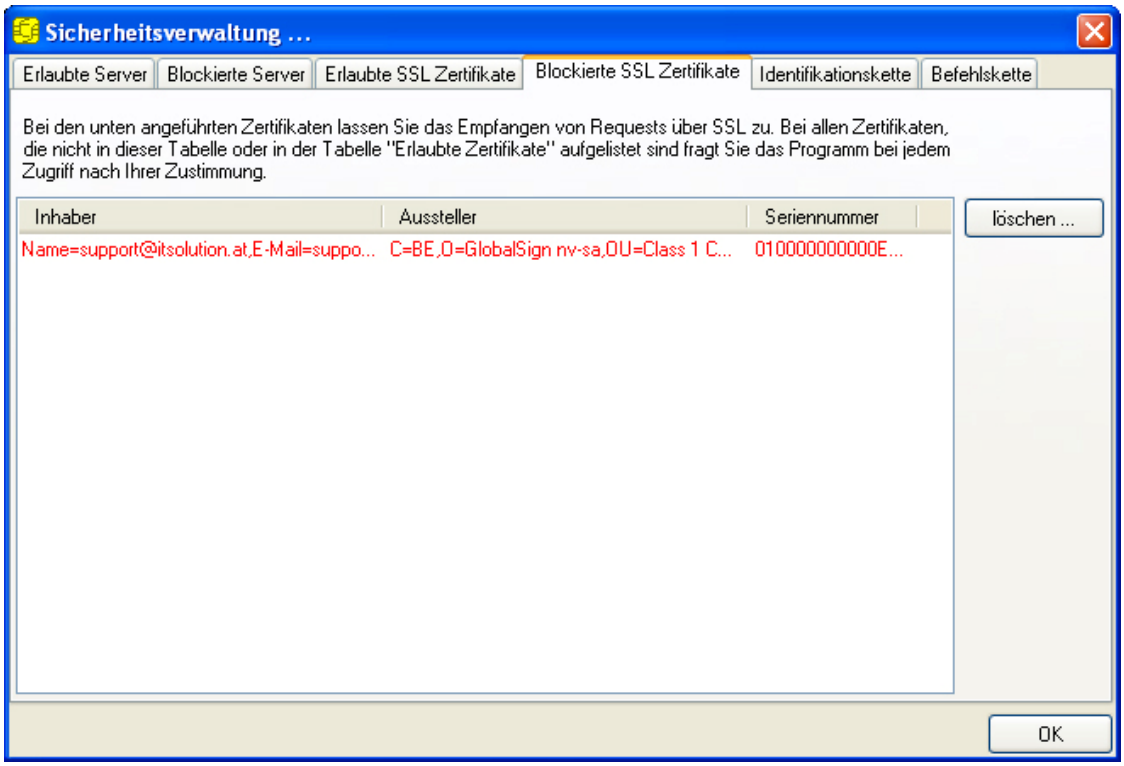


Möchten Sie eine Zertifikat entfernen, markieren Sie es mit einem Linksklick und Klick auf **löschen**.

- ❍ Dieses Zertifikat wird aus der Liste der erlaubten Zertifikat gelöscht
- ❍ Bei der nächsten Kommunikation mit diesem Zertifikat findet eine Sicherheitsabfrage statt.

Blockierte SSL Zertifikate

Diese Liste zeigt jene Zertifikate, die Sie mit dem oben beschriebenen Vorgang als „unsicher“ definiert haben.



Möchten Sie ein Zertifikat entfernen, markieren Sie es mit einem Linksklick und Klick auf **löschen**.

- ❍ Dieses Zertifikat wird aus der Liste der blockierten Zertifikate gelöscht
- ❍ Bei der nächsten Kommunikation mit diesem Zertifikat findet eine Sicherheitsabfrage statt.

Falscher Domänenname im SSL Serverzertifikat

Stimmt der Domänenname im SSL Serverzertifikat nicht mit dem Domänennamen in der Ziel-Url für die Befehlsantwort überein, werden Sie informiert.

Sie können sich das Serverzertifikat durch Klick auf **Serverzertifikat anzeigen** anzeigen.

Wenn Sie **Trotzdem senden** betätigen werden die Daten übertragen, wählen Sie jedoch **Ablehnen**, wird der Vorgang ohne Datenübertragung.

☞ Die Verfahrensweise für falsche Domainnamen im SSL Serverzeirtifikat kann im Konfigurationsprogramm voreingestellt werden.

11.3 Identifikationskette

Die Identifikationskette enthält Regeln, die, abhängig vom Ursprung des versuchten Zugriffes steuern, ob der Zugriff gestattet bzw. verwährt wird.

Diese Regeln sind in Ketten organisiert das heißt, sie werden immer von oben nach unten abgearbeitet. Die erste zutreffende Regel wird angewandt.

Nach der Installation sind standardmäßig Regeln vordefiniert. Diese können geändert werden.

Diese Regeln stellen eine Verknüpfung eingehender Daten mit einer daraus resultierenden Aktion dar.

Jede Regel in der Identifikationskette besteht aus folgenden Einträgen:

11.4 Authentisierungsklasse

Die Authentisierungsklasse gibt an, über welche Verbindung bzw. von welcher URL der Zugriff erfolgt. Diese gilt dann als mindestens erforderliche Klasse damit die Regel zutrifft.

Gültige Authentisierungsklassen sind:

- Anonym
  Zugriff über TCP/HTTP/TLS/HTTPS mit einsehbarer IP Adresse.
- Pseudo-anonym
  Zugriff über HTTP/HTTPS mit einsehbarer IP Adresse und Authentifizierung mittels Client-Zertifikat oder Übergabe der für die Bürgerkartenfunktion relevanten Parameter der HTTP-Bindung.
- Certified
  Zugriff über TLS-Bindung oder HTTP/HTTPS mit Übergabe der für die Bürgerkartenfunktion relevanten Parameter der HTTP-Bindung, welche eine verschlüsselte und authentisierte Verbindung beschreiben.
- CertifiedGovAgency
  Zusätzlich zu den Merkmalen Authentisierungsklasse „Certified“ muss eine der folgenden Bedingungen erfüllt sein
- der Domain der relevanten URL matched “*.gv.at“
- das Zertifikat enthält die Kodierung der Behördeneigenschaft mittels OID.

11.5 Identifikation

Die Identifikation gibt den Typ der Ursprungsquelle des abzuarbeitenden Requests eingetragen.

Gültige Werte sind:

- Namen der Transport-Bindungen
- TCP
- TLS
- HTTP
- HTTPS
- Name der Data-URL, die im Rahmen der Befehlskaskadierung Ursprung eines Requests sein kann
- * bedeutet: alle Ursprungsquellen

Aktion

Gültige Aktionen für Regeln sind

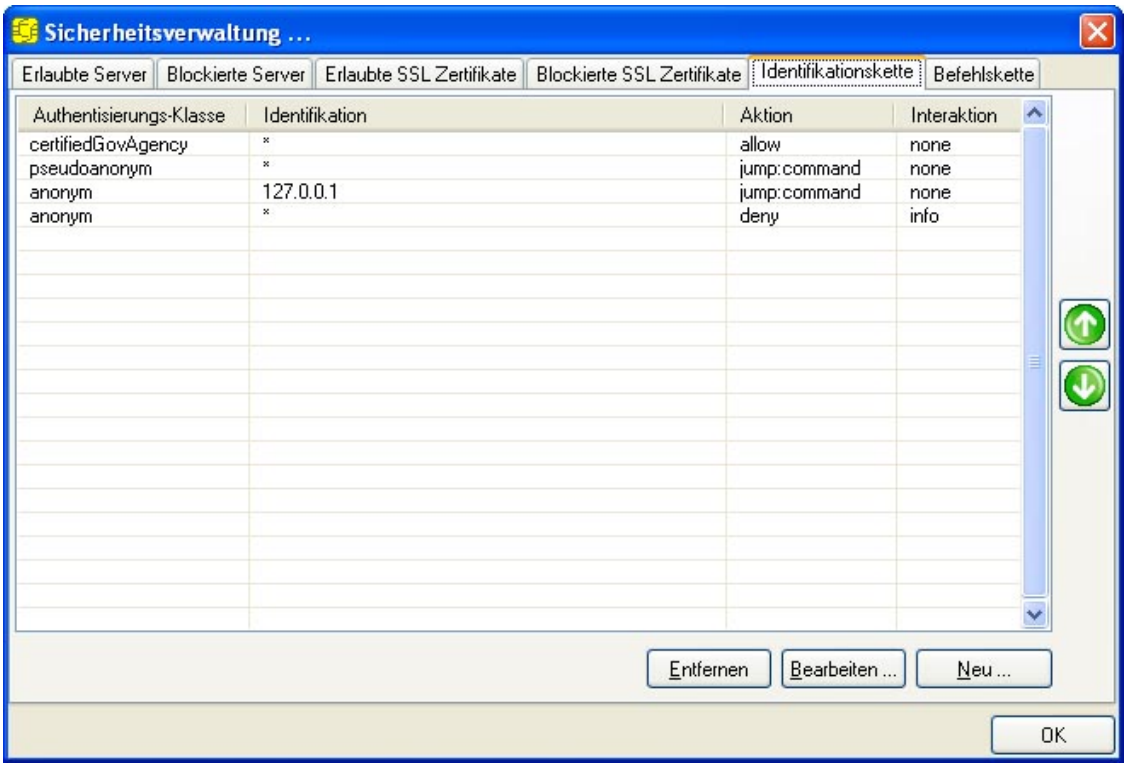
- Allow
  der Funktionsaufruf zugelassen und durchgeführt
- Deny
  der Funktionsaufruf wird weder zugelassen noch ausgeführt

- Jump:Command
  Sprung zur ersten Regel der Befehlskette

Interaktion

Gültige Interaktionen für Regeln sind

- None
  die Aktion wird ohne Informationsmeldung durchgeführt
- Info
  ein Meldungsfenster in Form einer Sprechblase über dem Icon Tray informiert über die Aktion
- Confirm
  die Ausführung der Aktion muss bei jeder Aktion dezidiert erlaubt oder verweigert werden



Die Oberfläche bietet folgende Möglichkeiten:

Liste nach oben/unten blättern

mit Hilfe der Pfeiltasten am rechten Fensterrand können Sie in der Liste der Regeln blättern.

Neue Regel erstellen

Um eine neue Regel zu erstellen klicken Sie auf **Neu**

Geben Sie **Authentisierungsklasse, Identifikation**, **Aktion** und **Interaktion** ein. Die Felder **Befehlsname** und **Befehlsparameter** sind nicht aktiv und können daher auch nicht editiert werden.

Durch Klicken auf **Übernehmen** wird die neue Regel aufgenommen, durch Klicken auf **Abbrechen** verwerfen Sie Ihre Eingaben.

Regel entfernen

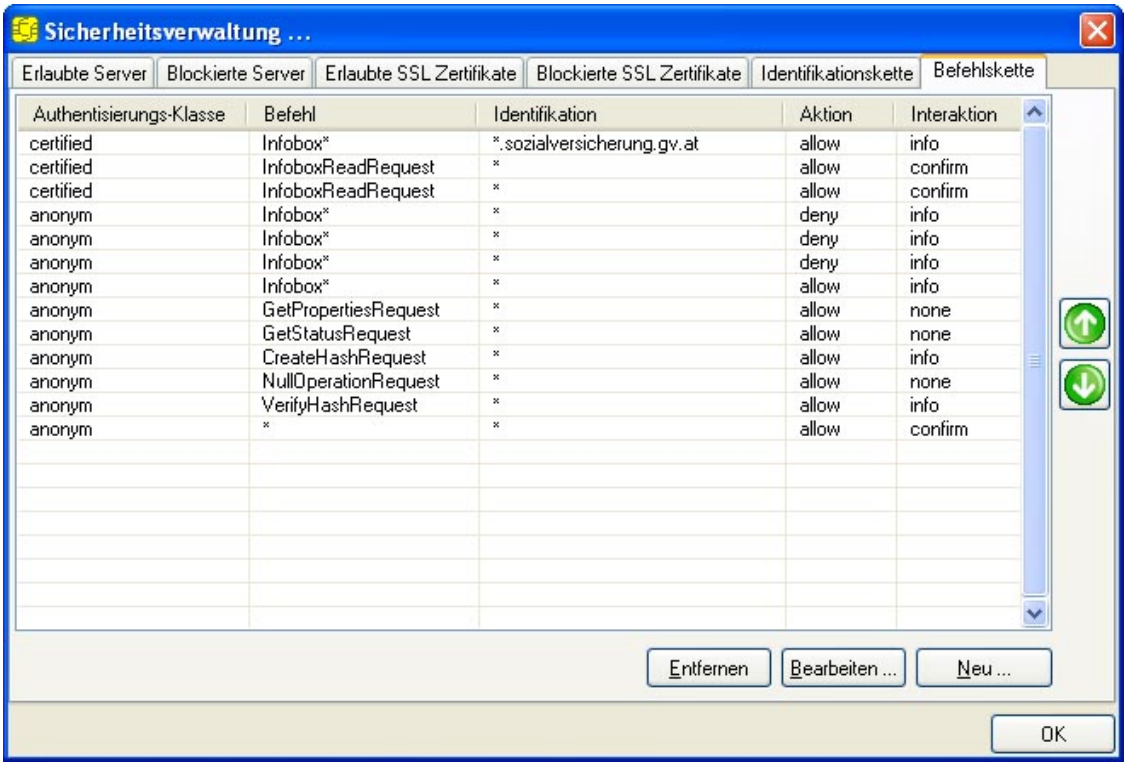
Um eine Regel zu entfernen markieren Sie bitte die gewünschte Regel und klicken dann auf **Entfernen**.

11.5.1 Regel bearbeiten

Um eine Regel zu bearbeiten markieren Sie bitte die gewünschte Regel und klicken dann auf den Button "Bearbeiten".

Befehlskette

Die Befehlskette enthält, ähnlich wie die Identifikationskette Regeln, die angewandt werden, wenn versucht wird auf Funktionen der Bürgerkartenumgebung zuzugreifen. In der Befehlskette werden die Regeln abhängig von dem im Request enthaltenen Befehl eingetragen. Auch hier wird die Kette sequentiell von oben nach unten abgearbeitet, und die erste zutreffende Regel wird angewandt.



Authentisierungsklassen

Siehe Interaktionskette

Befehl

Name des Befehls an den Security-Layer. Gültige Befehle sind:

- der gesamte Name des Befehls (InfoboxReadRequest)
- Teile des Names des Befehls ("Infobox*" für alle Infobox-Requests)
- * alle Requests

Interaktion

Gültige Interaktionen für Regeln sind

None
die Aktion wird ohne Informationsmeldung durchgeführt

Info
ein Meldungsfenster in Form einer Sprechblase über dem Icon Tray informiert über die Aktion

Confirm
die Ausführung der Aktion muss bei jeder Aktion dezidiert erlaubt oder verweigert werden

ConfirmWithSecret
die Erlaubnis für die Ausführung der Aktion muss durch Eingabe eines Passwortes erteilt werden.

Bedienung der Kettenbearbeitungs-Oberfläche

Die Bedienung erfolgt analog der Bedienung der Identifikationsketten. Die Oberfläche bietet ebenfalls die Möglichkeiten

- Liste nach oben/unten blättern
- Regel bearbeiten
- Regel entfernen
- Neue Regel erstellen

In der Mitte des Fensters sehen Sie die **Liste der Befehls Parameter**.

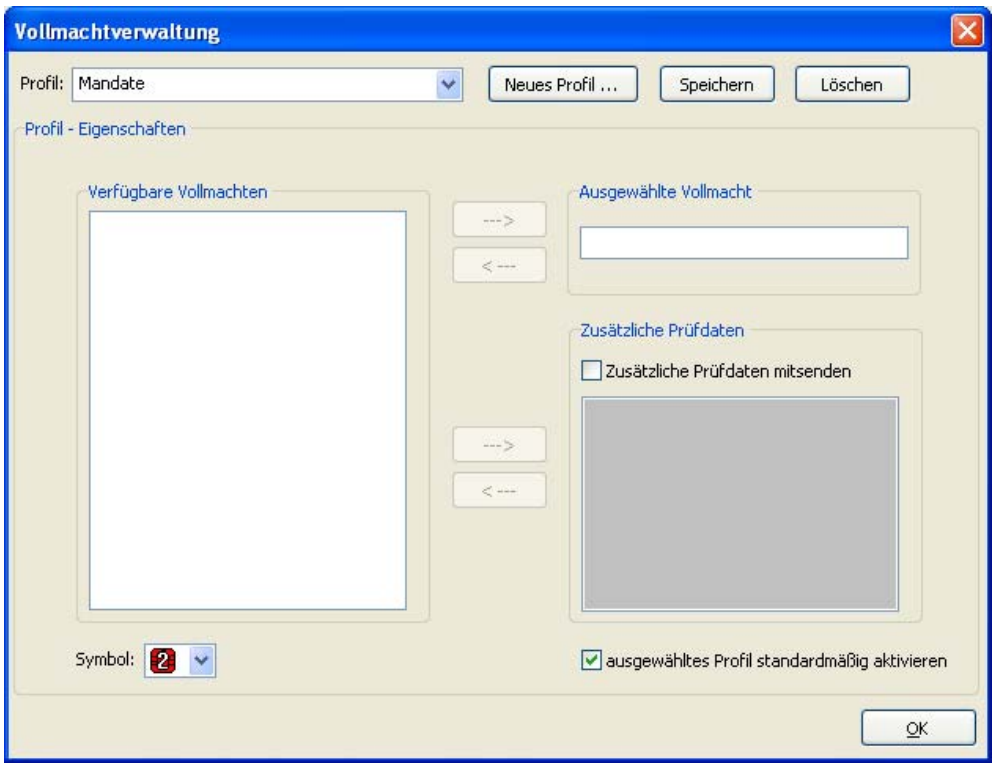
Um einen **Parameter** zu **entfernen** markieren Sie bitte den gewünschten Parameter mit einem Linksklick und klicken dann auf den Button „Entfernen“.

Um einen neuen **Parameter hinzuzufügen** klicken Sie bitte auf den Button „Hinzufügen“. Daraufhin erscheint ein kleines Fenster mit **zwei Textfeldern** in denen Sie den **Namen** und den **Wert** des jeweiligen **Parameters** eintragen können.

Haben Sie die nötigen Einstellungen für die neue Regel getätigt, so können Sie diese in die Liste übernehmen indem Sie auf **Übernehmen** klicken. Möchten Sie die Regel verwerfen klicken Sie auf **Abbrechen**.

- ParamName
  Hier wird der Name eines Parameters angegeben.
- ParamValue
  Die Parameter sind abhängig vom jeweiligen Security-Layer Request. Bei Infobox-Befehlen ist der Parameter der Name der Infobox, bei Befehlen die auf Schlüssel zugreifen, der Name der Keybox. Beim Auslesen der Infoboxen IdenitityLink und Mandates ist ein zusätzlicher Parameter erforderlich welcher angibt, ob die enthaltenen Stammzahlen natürlicher Personen im Klartext (plain-text SZ) übermittelt werden würden. Die Verwendung einer einfachen Wildcard '*' die alle Infoboxen und Keyboxen matched ist zulässig.

12 Stellvertretungen und GDA Token



Stellvertretungen werden in der virtuellen Infobox **Mandates** gespeichert. Die Vollmacht wird über eine Webapplikation beantragt.

Beispiel: Person A darf für Person B Post in Empfang nehmen.

Die Person, für die eine Vollmacht beantragt wurde, erhält über einen „**InfoboxUpdateRequest**“, die notwendige virtuelle Infobox.

Existiert für eine Person eine Vollmacht und es erfolgt eine Anmeldung an einer Applikation, die Vollmachten verarbeiten kann, werden die Autorisierungsdaten mitgeschickt und von der Applikation verarbeitet, wenn:

- Die Funktion **Auswahl bei Anfrage** aktiviert ist
- Ein Vollmachtsprofil beim Start von trustDesk basic standardmäßig aktiviert wird.

Sollen keine Stellvertretungsdaten geschickt werden, muss der **Stellvertretung Modus** über das Kontextmenü deaktiviert werden.

Eingabefelder

Name	Wert	Bedeutung
Profil	alphanumerisch	Name des Profils
Ausgewähltes Profil standardmäßig aktivieren	☑	Das angezeigte Profil wird beim Wechsel in den Vollmachtsmodus ausgewählt
	☐	Das angezeigte Profil wird beim Wechsel in den Vollmachtsmodus nicht ausgewählt
Symbol		Bei Auswahl des Vollmachtsprofiles wird das goldene Trayicon durch das ausgewählte Icon erstetzt.

Buttons

Name	Bedeutung
Neues Profil	Ein neues Profil kann angelegt werden
Speichern	Die zum angegebenen Profilnamen eingegebenen Werte werden gespeichert
Löschen	Das Profil wird mitsamt den angegebenen Werten gelöscht.

13 Signaturerstellung

Um Dokumente gemäß des Signaturgesetzes und der Signaturverordnung signieren zu können, ist neben der Signaturerstellungeinheit und dem dazugehörenden Kartenleser der Secure Viewer trustView, der in trustDesk basic enthalten ist, erforderlich.

Smartcards, die zu Signatur und Verschlüsselung geeignet sind, verfügen üblicherweise über zwei PINs:

- Die Signatur PIN für die digitale Unterschrift und
- die Geheimhaltungs PIN zum Ver- und Entschlüsseln von Daten.

☞ Eine „sichere“ Signatur ist nur mit einem qualifizierten Zertifikat und einer sicheren Signatur PIN möglich. Wird ein nicht qualifiziertes Zertifikat und ein Geheimhaltungs PIN verwendet, entsteht nur eine einfache elektronische Signatur.

☞ Softwarezertifikate entsprechen nicht den hohen Sicherheitsanforderungen und sind deshalb mit trustView nicht verwendbar.

Folgende Arten von Daten können mit trustView digital signiert werden:

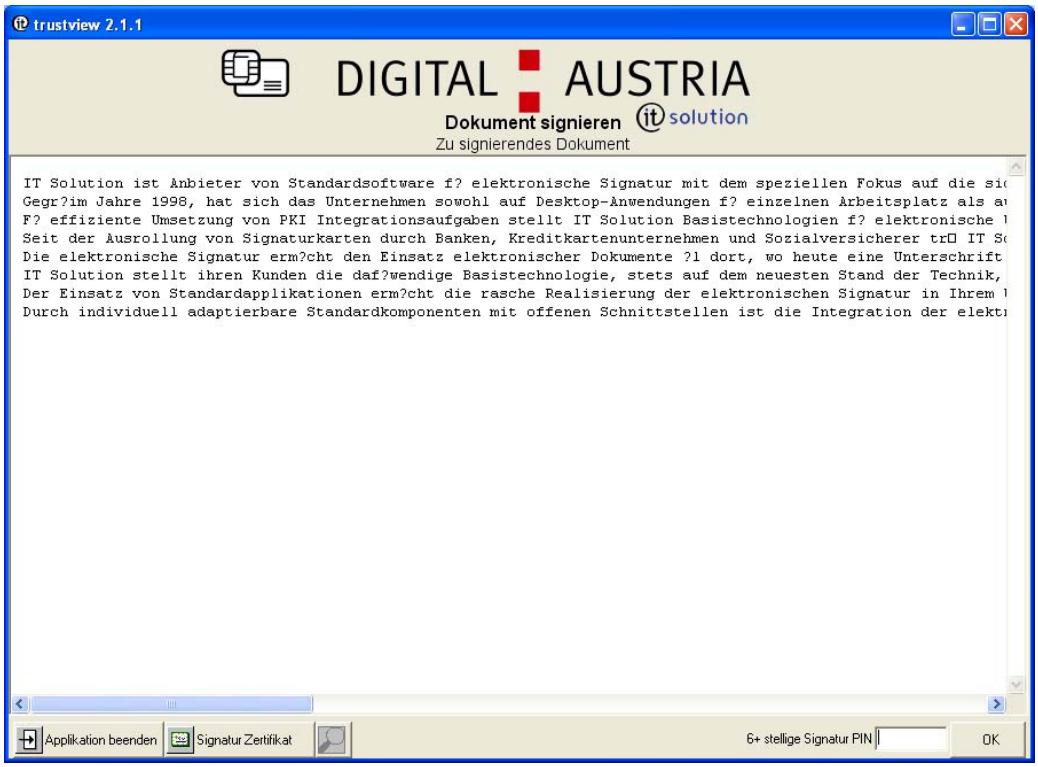
- Text
- XHTML
- HTM
- HTML
- XML.

! *Nicht signiert werden können folgende Daten:*

- Dynamische Inhalte, da diese nicht dem Signaturgesetz entsprechen;
- Dokumente mit dem Contentype HTML, die keinem gültigen XHTML Schema entsprechen;
- binäre Daten und
- referenzierte Datenobjekte, auf die nicht zugegriffen werden kann.

13.1 Digital unterschreiben

Nach Aufruf des Dokumentes, das Sie digital unterschreiben möchten, werden die Daten mit trustView angezeigt:



Applikation beenden

Soll das angezeigte Dokument nicht digital unterschrieben werden, klicken Sie auf **Applikation beenden**.

Signatur Zertifikat

Zeigt das Zertifikat der Smartcard an, die im Lesegerät steckt.

Ist ein Dokument größer als die Bildschirmseite, kann mit dem **Scrollbalken** das Dokument horizontal und vertikal verschoben werden um eine visuelle Überprüfung zu gewährleisten.

Enthält ein Dokument mehrere Datenobjekte oder Seiten, wird ein Button eingeblendet, der Ihnen über die Pfeiltasten das Blättern und mit Klick auf die Zahlen die Eingabe einer bestimmten Seite ermöglicht:

Unterschreiben

! *Vergewissern Sie sich unbedingt v o r jeder digitalen Signatur, dass das richtige Dokument angezeigt wird, die Anzeige des zu signierenden Dokumentes nicht manipuliert ist und die Systemzeit Ihres PCs die richtige Uhrzeit anzeigt.*

Nach der PIN Eingabe ist das Dokument digital unterschrieben.

14 Häufige Fehlerursachen

14.1 Signaturkarte nicht eingelegt

Kann trustView auf die Karte nicht zugreifen, weil sie nicht oder nicht richtig eingelegt ist, erhalten Sie folgende Meldung:

Ein Problem mit der Signaturkarte ist aufgetreten! Ist die richtige Karte eingelegt?

Durch Klick auf **OK** gelangen Sie zur Anzeige des zu signierenden Dokuments und können nochmals versuchen, das Dokument zu signieren.

Bitte stellen Sie sicher, dass ihre Signaturkarte korrekt in den Kartenleser eingelegt ist.

14.2 Falsche PIN

Haben Sie eine falsche PIN eingegeben, erhalten Sie folgende Fehlermeldung:

Die eingegebene PIN ist falsch!

Durch Klick auf **OK** gelangen Sie zur Anzeige des zu signierenden Dokuments und können nochmals versuchen, das Dokument zu signieren.

! *Je nach Karte und Trustcenter ist die Anzahl der möglichen Fehleingaben beschränkt! Nach Erreichen dieser Eingaben wird die Karte gesperrt! Diese Einschränkung dient in erster Linie Ihrer eigenen Sicherheit! Manche Smartcards können mit Hilfe einer PUK, die Sie bei Ihrem zuständigen Trustcenter erhalten, wieder entsperrt werden.*

14.3 Null PIN

Manche Smartcards werden mit einer so genannten Null-PIN ausgeliefert, die vor einem Einsatz der Karte durch eine persönliche PIN zu ersetzen ist. Zur Klärung dieses Problems kontaktieren Sie bitte Ihr Trustcenter.

14.4 Leere Smartcard

Der Signaturchip Ihrer Karte enthält kein Signaturzertifikat. Wenden Sie sich in diesem Fall an Ihr Trustcenter.

14.5 Smartcard und Kartenleser passen nicht zusammen

Ihr Trustcenter stellt Regeln für den Umgang mit Ihrer PIN und Signaturkomponente zur Verfügung. Bitte halten Sie diese Regeln ein! Kontaktieren Sie bitte in diesem Fall Ihr Trustcenter. Die Liste der empfohlenen Kartenlesegeräte entnehmen Sie bitte:

http://www.a-trust.at

14.6 Software PIN nicht aktiviert

Bei Kartenlesern, die kein eigenes PIN Pad, sondern eine eigene Tastatur zur Eingabe der PIN haben, muss im Konfigurationsmenü die Auswahlbox **Software PIN Eingabe erlauben** aktiviert werden. Ist dies nicht der Fall, erhalten Sie die Meldung:

Die PIN Eingabe per Software ist derzeit deaktiviert. Ändern Sie bitte die Konfiguration der Software um die PIN Eingabe per Software zu aktivieren.

14.7 Signieren mit trustDesk basic

Daten, die Sie signieren möchten, können einerseits durch Applikationen wie beispielsweise E-Government - Applikationen erstellt werden, andererseits durch trustDesk basic. Die E-Government Funktionen im Hauptmenü bieten die Möglichkeit, beliebige Daten zu signieren. Grundsätzlich ist zu unterscheiden zwischen

- XML Signaturen, die nur gültige Dokumente im Format XML signieren können und
- CMS Signaturen, die nur gültige Dokumente im Format CMS signieren können.

15 XML signieren

Wählen Sie aus dem Hauptmenü die **E-Government Funktionen** und **XML signieren**.

Wählen Sie über den Datei-Dialog die zu signierende XML Datei aus.

Es wird nun geprüft, ob die gewählte Datei eine gültige Datei ist; wenn nicht, wird der Vorgang abgebrochen und eine Fehlermeldung angezeigt.

Mit XML können folgende Dateien signiert werden:

- .txt
- .html
- .htm
- .xml
- .xhtml.
- Tiff (nur über Request)

Ist die Datei gültig, haben Sie die Möglichkeit eine XSLT Transformation hinzuzufügen.

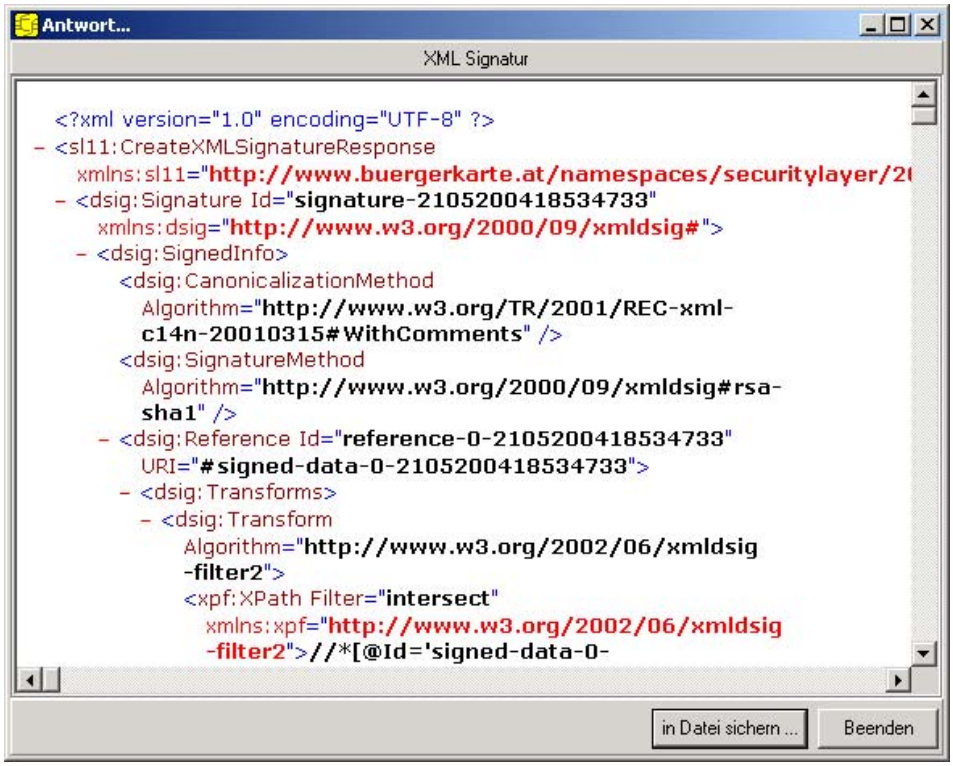
Durch diese Transformation kann festgelegt werden, in welcher Form (xml, html, text) das Ergebnis ausgegeben werden soll.

Mit Klick auf **Ja** erhalten Sie denselben Datei-Dialog wie bei der Auswahl des XML Dokumentes, aus dem Sie eine Datei mit der Endung *.xsl angeben, die die Transformationsinformationen beinhaltet.

Auch diese Datei wird auf Ihre Gültigkeit hin überprüft. Ist das Prüfergebnis negativ, wird der Vorgang abgebrochen und eine Fehlermeldung angezeigt.

Bei gültiger Auswahl werden die Daten mit trustView angezeigt und können wie oben beschrieben signiert werden.

Der XML-Signature-Response, also die Antwort von trustView auf die Aufforderung, diese Daten zu signieren, wird als XML Dokument angezeigt und kann gespeichert werden.



15.1 Tiff Signatur mit File Referenz

```
[01]    <?xml version="1.0" encoding="UTF-8"?>
[02]    <sl:CreateXMLSignatureRequest
[03]    xmlns:sl="http://www.buergerkarte.at/namespaces/securitylayer/1.2#">
[04]       <sl:KeyboxIdentifier>CertifiedKeypair</sl:KeyboxIdentifier>
[05]       <sl:DataObjectInfo Structure="detached">
[06]          <sl:DataObject Reference=""/>
[07]          <sl:TransformsInfo>
[08]             <dsig:Transforms xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
[09]                <dsig:Transform
       Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
[10]             </dsig:Transforms>
[11]             <sl:FinalDataMetaInfo>
[12]                <sl:MimeType>application/xml</sl:MimeType>
[13]             </sl:FinalDataMetaInfo>
[14]          </sl:TransformsInfo>
[15]       </sl:DataObjectInfo>
[16]       <sl:DataObjectInfo Structure="detached">
[17]          <sl:DataObject Reference="file:Urkunde.tif"/>
[18]          <sl:TransformsInfo>
[19]             <sl:FinalDataMetaInfo>
[20]                <sl:MimeType>image/tiff</sl:MimeType>
[21]             </sl:FinalDataMetaInfo>
[22]          </sl:TransformsInfo>
[23]       </sl:DataObjectInfo>
[24]       <sl:SignatureInfo>
[25]          <sl:SignatureEnvironment Reference="file:Dossier.xml"/>
[26]          <sl:SignatureLocation xmlns:doc="urn:Document"
       Index="4">/Dossier</sl:SignatureLocation>
[27]       </sl:SignatureInfo>
[28]    </sl:CreateXMLSignatureRequest>
[29]
```

In Zeile 17 wird das zu signierende Dokument im TIFF Format angegeben. Die Angabe erfolgt relativ zum übergebenen Arbeitsvezeichnis.

Zeile 25 enthält den Namen der XML Datei, in die die Signatur eingebettet wird, und Zeile 26 das Element innerhalb dieser XML Struktur.

Beispiel für eine solche XML Struktur:

```
[01]    <?xml version="1.0" encoding="UTF-8"?>
[02]    <Dossier xmlns="http://www.cyberdoc.at/CyberDOC07/1.0"
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="http://www.cyberdoc.at/CyberDOC07/1.0
        .\CyberDOC07_1.0.xsd">
[03]       <DossierProfile>
[04]          <Subject>Subject</Subject>
[05]          <Description>Description</Description>
[06]       </DossierProfile>
[07]       <Documents>
[08]          <Document>
[09]             <DocumentProfile>
                    <SourceLocation>file:Urkunde.tif</SourceLocation>
[10]                <MimeType>image/tiff</MimeType>
[11]             </DocumentProfile>
[12]             <ds:Object/>
[13]          </Document>
[14]       </Documents>
[15]    </Dossier>
```

16 CMS signieren

Mit CMS können folgende Dateien signiert werden:

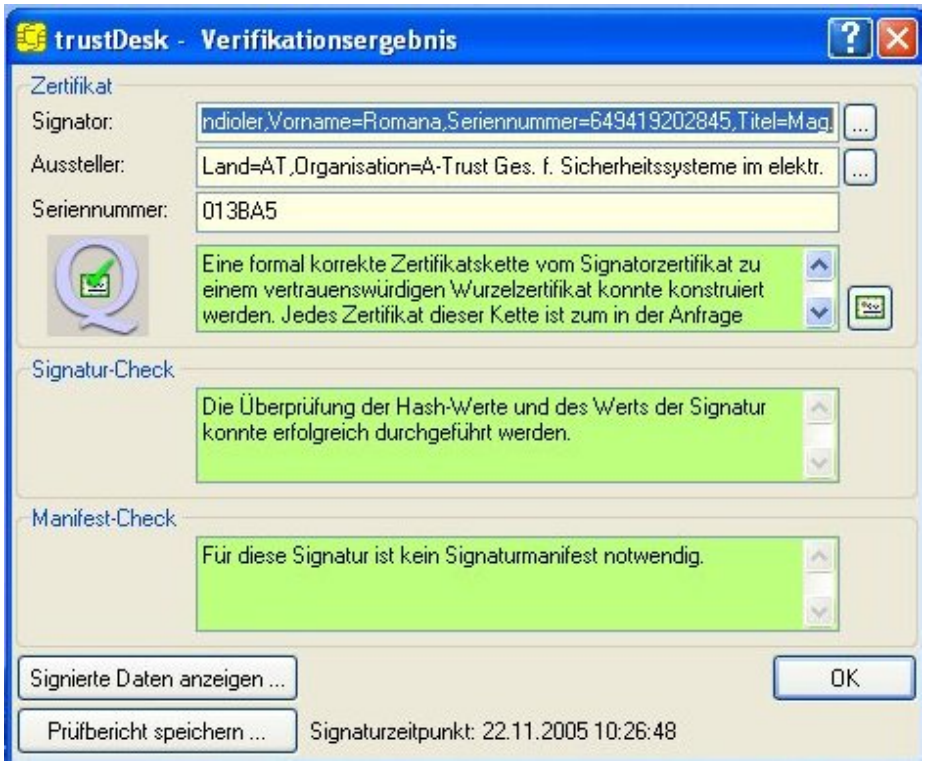
- .txt
- .html
- .htm
- .xml
- .xhtml.

Das CMS Signieren ist analog zum XML Signieren, wobei jedoch keine XSLT Transformation hinzugefügt werden kann.

17 Signaturprüfung

trustDesk basic bietet die Möglichkeit digitale Signaturen auf Ihre Gültigkeit hin zu überprüfen. Über das Kontextmenü wählen Sie **Verifizieren**.

17.1 Verifikationsergebnis der Signaturprüfung



Signator

Name der Person oder der Stelle, die die Daten signiert hat. Durch Klick auf **„...“** erhalten Sie weitere Angaben zum Signator.

Aussteller

Name des Trustcenters, das das Zertifikat des Signators ausgestellt hat. Durch Klick auf **„...“** erhalten Sie weitere Angaben zum Aussteller.

Seriennummer

Die Nummer des Zertifikates.

Ergebnis der Zertifikatsprüfung

Zeigt an, ob das verwendete Zertifikat zum Zeitpunkt der Unterschrift gültig war.

Durch Klick auf wird das Zertifikat selbst am Bildschirm angezeigt.

Signatur-Check

Der Signatur-Check zeigt das Ergebnis der Überprüfung des Hash-Wertes und der Signatur.

Manifest-Check

Diese Anzeige informiert Sie über das Ergebnis der Überprüfung des Signaturmanifestes.

Signaturzeitpunkt

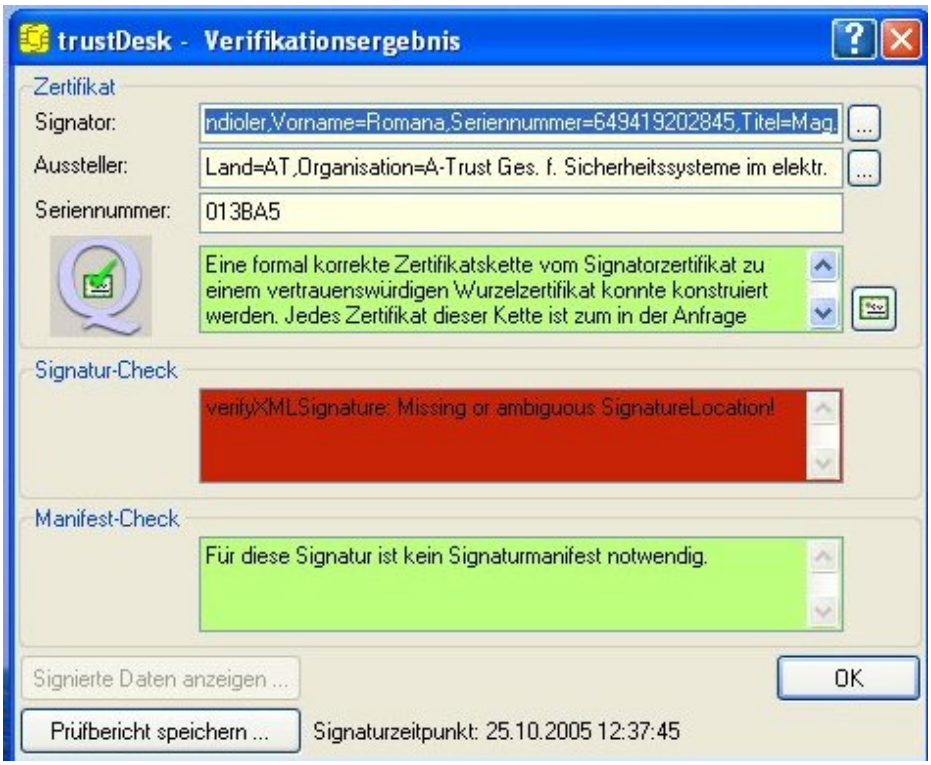
Datum und Uhrzeit, wann das Dokument signiert wurde.

Signierte Daten anzeigen

Die signierten Daten werden in einem eigenen Fenster angezeigt.

Durch Klicken auf **OK** schließen Sie das Fenster wieder.

Ein positives Prüfergebnis wird grün hinterlegt, Warnungen gelb und Fehler rot.



Sind in einem Dokument mehrere Signaturen enthalten, können Sie diese Signaturen sowohl hintereinander als auch gleichzeitig prüfen:

17.2 XML verifizieren

Diesen Menüpunkt wählen Sie aus dem Hauptmenü und den E-Government Funktionen.

Im darauf folgenden Datei-Dialog geben Sie eine XML Datei an, deren Signatur verifiziert werden soll. Ist die Datei zulässig, wird das Ergebnis der Signaturprüfung auf dem Bildschirm angezeigt, ansonsten erscheint eine entsprechende Fehlermeldung.

17.3 CMS Signatur verifizieren

Diesen Menüpunkt wählen Sie aus dem Hauptmenü und den E-Government Funktionen.

Im darauf folgenden Datei-Dialog geben Sie eine Datei an, deren CMS Signatur verifiziert werden soll. Ist die Datei zulässig, wird das Ergebnis der Signaturprüfung auf dem Bildschirm angezeigt, ansonsten erscheint eine entsprechende Fehlermeldung.

18 Installationsroutinen für Firmen und Behörden

18.1 Silent Installation

Diese dient dazu, trustDesk basic ohne Benutzerinteraktion zu installieren.

Diese Art der Installation ist zu benutzen, wenn Software zentral und/oder programmgesteuert installiert wird bzw. Updates nicht vom einzelnen Benutzer durchgeführt werden sollen.

Grundsätzlich sollte der Benutzer die Interaktive Installation wählen.

Um die **Silent Installation** zu starten, muss das Setup Programm von trustDesk basic mit einer Kombination folgender Parameter aufgerufen werden.

Aufruf Syntax:

setup.exe [-silent] [-destination directory] [-folder folder] [-log [logfile]] [-4currentUser] [-dou]

Parameter	Bedeutung
-silent	Dieser Parameter ruft die unbeaufsichtigte Installation auf. Die anderen Parameter werden nur in Verbindung mit diesem Parameter aktiv.
-destination	Dieser Parameter gibt das gewünschte Installationsverzeichnis an, das ein absoluter Pfad mit Laufwerksangabe sein muss. Wird der Parameter nicht angegeben, dann wird die Software in das Default Verzeichnis „C:\Programme\ITSolution\trustDesk basic“ kopiert.
-folder	Dieser Parameter gibt den gewünschten Programmordner an, in dem die Programmsymbole abgelegt werden sollen. Wird der Parameter nicht verwendet, dann werden die Programmsymbole im Standardordner „ITSolution\trustDesk basic“ abgelegt.
-log	Dieser Parameter gibt ein Logfile an, in dem der Installationsvorgang protokolliert wird. Wird der Parameter nicht übermittelt, dann wird im Verzeichnis „user/temp“ ein Standard Logfile angelegt.
-4currentUser	Dieser Parameter veranlasst, dass die Startup-Menü-Einträge nur für den aktuellen Benutzer anstatt für alle Benutzer vorgenommen werden.
-dou	Dieser Parameter deaktiviert das automatische Online-Update.
-autodep	Gibt an, ob die Autodeployment Datei nach der Installation kopiert werden soll. Nach dem Parameter –autodep muss die Pfadangabe für die Autodeploymentdatei folgen

☞ Die Konfiguration der Kartenlesegeräte wird beim ersten Start von trustDesk basic vorgenommen.

18.2 Silent Deinstallation

Wie die Silent Installation dient die Silent Deinstallation dazu, trustDesk basic ohne Benutzerinteraktion zu deinstallieren. Grundsätzlich sollte der Benutzer die Interaktive Deinstallation wählen.

Um die **Silent Deinstallation** zu starten, wird das Setup Programm des trustDesk basic mit einer Kombination folgender Parameter aufgerufen.

☞ Das Silent Deinstallationsprogramm muss immer aus dem Verzeichnis aufgerufen werden, aus dem das Programm gelöscht werden soll

Aufruf Syntax:

setup.exe [-su] [-app [SecurityLayer] [-log [logfile]]

Parameter	Bedeutung
-su	Dieser Parameter ruft die unbeaufsichtigte Deinstallation auf. Die anderen Parameter werden nur in Verbindung mit diesem Parameter aktiv.
-app	Dieser Parameter gibt den Namen der Applikation an, die deinstalliert werden soll. Für trustDesk basic lautet der Parameter immer „SecurityLAYER2
-log	Dieser Parameter gibt ein Logfile an, in dem der Installationsvorgang protokolliert wird. Wird der Parameter nicht übermittelt, dann wird im Verzeichnis „user/temp“ ein Standard Logfile angelegt.

☞ Bei der Silent Deinstallation werden die Verzeichnisse ITSolution und trustDesk basic nicht gelöscht. Diese müssen manuell von der Festplatte entfernt werden.

18.3 Automatisches Deployment

Zur Ausrollung der BKU in Behörden-, Magistrats- oder Firmennetzwerken ist das automatische Deployment gedacht.

Für ein gezieltes, automatisches Deployment ist, unabhängig davon, ob die Installation interaktiv oder silent gestartet wird, die Möglichkeit zur Konfiguration des Installationsvorganges erforderlich.

Die Angaben für das automatische Deployment finden sich in einer vom Benutzer selbst zu erstellenden Autodeployment Datei, deren Name frei gewählt werden kann.

Der Aufruf erfolgt entweder über interaktiv über den Aufruf der Datei setup.exe –autodep [Pfadangabe der ini-Datei] oder über die silent installation.

Parameter und deren Bedeutung finden Sie bei der Beschreibung der Einstellungen auf den entsprechenden Masken.

18.3.1 Parameter und gültige Eingabewerte

```
[ReadersSettings]
apidll0=c:\x.dll
apidll1=
apidll2=
apidll3=
ports0=0,1
ports1=1
ports2=1
ports3=1
ports4=1
forcenopcsc=yes | no
swpinallowed=yes | no

[eGovSettings]
SaveDir=c:\
SaveIncludeRequest=yes | no
SLPort=3495
SSLPort=3496
```

CRLOnStartUp=yes | no
SSLClientAuth=yes | no
CardIdentityLink=yes | no
ResolveOnline=yes | no
AppendRootCert=yes | no
HandleEmptyFormFields=dropref | space | error

[SSLSettings]
ACTION_MM_DOMAIN=block | allow | ask

[ProxySettings]
useProxy=yes | no
proxyServer=
proxyServerPort=

[EncryptionSettings]
defaultsymalg= AES128-CBC | AES192-CBC | AES256-CBC | 3DES-CBC
defaultsymkeyalg= AES128-CBC | AES192-CBC | AES256-CBC | 3DES-CBC
mime0=application/octet-stream
mime1=application/my-type

[updateSettings]
autoCheckInterval=0-24

[CRLSettings]
SIGCHECK=yes | no
SIGforceOCSP=yes | no
SIGONEXPIRY=yes | no
SIGXXMINUTES=60
SSLCHECK=yes | no
SSLforceOCSP=yes | no
SSLONEXPIRY=yes | no
SSLXXMINUTES=60

[DaemonSettings]
startCrlDaemon=yes | no
ProcessList=10
RemoveCRL=5

[CAManagement]
CADir=c:\debug
trustedCADir=c:\debug2

[RootCAInstallation]
silent=yes | no

Name	Key	Wert	Bedeutung
CT-API Treiber 1-4	apidll0 - 3	Leer	Kein CT-API Treiber ist installiert
		C:\x.dll	Pfad für die Treiberdatei

Name	Key	Wert	Bedeutung
Ports	ports0 – 3	Leer	Kein CT-API Port ist festgelegt
		1	Port unter dem der Kartenleser angesprochen wird.
Erkennung von PC/SC Kartenlesern deaktivieren	forcenopcsc	yes	Treiber von PC/SC Kartenlesern werden nicht in die Suche einbezogen
		no	Es werden bei der automatischen Erkennung von Kartenlesern auch PC/SC Treiber erkannt
Software-PIN erlauben	swpinallowed	yes	PIN Eingabe über die Computertastatur ist erlaubt
		no	Die PIN kann nicht über die Computertastatur eingegeben wrden
Exklusiver Kartenleserzugriff	remoteapi	no	Der Kartenleser wird nach der PIN Eingabe für andere Applikationen freigegeben
		yes	Der Kartenleser wird erst freigegeben, wenn trustDesk basic beendet wird.
Signierte SecurityLayer Dokumente in folgendem Verzeichnis speichern	SaveDir	Leer	Signierte Dokumente werden nicht automatisch gespeichert
		C:\	In dieses Verzeichnis werden Ihre signierten SecurityLayer Dokumente (SecurityLayer Response) gespeichert. Mittels Klick auf den **'..'** Button können Sie den gewünschten Pfad direkt über eine Dialogbox auswählen.
Auch SecurityLayer Requests in obigem Verzeichnis speichern	SaveIncludeRequest	yes	Neben den signierten Dokumenten werden auch die SecurityLayer Requests im angegebenen Verzeichnis gespeichert
		no	SecurityLayer Requests werden nicht im angegebenen Verzeichnis gespeichert.

Name	Key	Wert	Bedeutung
SecurityLayer benutzt TCP/IP Port Nummer	SLPort	3495	Standardmäßig wird Port 3495 für http:- und tcp-Protokolle benutzt.
SecurityLayer benutzt SSL Port Nummer	SSLPort	3496	Port 3496 ist für https: und tls voreingestellt
Widerrufslisten beim Start aus dem Internet beziehen	CRLOnStartUp	yes	Beim Start des trustDesk basic werden die aktuellen Widerrufslisten aus dem Internet geladen. Widerrufslisten werden benötigt, um die Gültigkeit von Zertifikaten zu prüfen. Sie sollten jedenfalls **vor** der Prüfung eines Zertifikates aktualisiert werden.
		no	Die aktuellen Widerrufslisten werden beim Starten nicht geladen. Dies beschleunigt den Startvorgang.
SSL Client Authentifizierung erzwingen	SSLClientAuth	yes	Die Authentifizierung von SSL Clients ist notwendig. Diese Option hat keine Auswirkung auf das SecurityLayer SSL Server Zertifikat. Der SecurityLayer selbst authentifiziert sich immer mit einem mitgelieferten SSL Server Zertifikat, dessen geheimer Schlüssel durch Triple-DES/CBC 168 Bit-Verschlüsselung geschützt ist.
		no	SSL Clients müssen sich nicht notwendigerweise autentifizieren
Personenbindung auf Karte	CardIdentityLink	yes	Die Personenbindung wird auf der Karte gespeichert
		no	Die Personenbindung wird in einer virtuellen Infobox gespeichert.

Name	Key	Wert	Bedeutung
XML Parser darf Internet verwenden um externe Schemas zu beziehen	ResolveOnline	yes	Legt fest, ob der XML Parser eine Internetverbindung nutzen darf, um eventuell benötigte externe Schemas zu beziehen. Es wird empfohlen diese Funktion zu aktivieren.
Auch Wurzelzertifikat in XML Signaturresponse hinzufügen	AppendRootCert	yes	Soll das Wurzelzertifikat bei XML Signatureresponses hinzugefügt werden soll.
		no	
HTML Formularfelder	HandleEmptyFormFields	dropref	Leere Referenzen in HTML Formularfeldern werden entfernt. oder durch Leerzeichen ersetzt werden sollen oder eine Fehlermeldung ausgegeben werden soll.
		space	Leere Referenzen in HTML Formularfeldern werden durch Leerzeichen ersetzt
		error	Bei leeren Referenzen in HTML Formularfeldern wird eine Fehlermeldung ausgegeben.
Bei falschem Domänennamen im SSL Serverzertifikat	ACTION_MM_DOMAIN	block	Verbindung abbrechen - die Verbindung wird automatisch abgebrochen
		allow	Verbindung trotzdem aufbauen - die Verbindung wird mit jeder Domäne aufgebaut
		ask	Benutzer fragen – der Benutzer wird jedes Mal benachrichtigt und kann entscheiden, ob er die Verbindung zulassen möchte.
Proxy Server verwenden	useProxy	yes	Soll ein Proxyserver verwendet werden, muss der Wert hier yes sein.

Name	Key	Wert	Bedeutung
		no	Gibt an, dass keine Proxy Server verwendet werden soll.
Proxy	proxyServer		Name des Servers
Proxyserver für lokale Adressen umgehen	noProxyForLocal	yes	Für lokale Adresse wird der Proxy nicht benutzt
		no	Proxy wird auch für lokale Adressen benutzt
Für die Adressen, die wie folgt beginnen, keinen Proxyserver verwenden	ignoreServerList	leer	
		servername; servername	Eingabe der Servernamen. Trennzeichen ist das Semikolon
Symetrischer Standard Verschlüsselungsalgorithmus für Daten	defaultsymalg	AES128-CBC | AES192-CBC | AES256-CBC | 3DES-CBC	
Symetrischer Standard Verschlüsselungsalgorithmus für Daten	defaultsymkeyalg	AES128-CBC | AES192-CBC | AES256-CBC | 3DES-CBC	
	mime0	application/octet-stream	
	mime1	application/my-type	
	silent	yes	Der Rootzertifikatsdialog wird bei der Installation nicht angezeigt
		No	Der Benutzer wird über die Installation des Rootzertifikats informiert.
In Stunden neue Updates im Internet suchen	autoCheckInterval	0	Es wird nicht nach Software Updates gesucht.
		1 - 24	Im angegebenen Intervall wird im Internet nach Aktualisierungen gesucht.
Widerrufsprüfung ausschalten	SIGCHECK	yes	Widerrufsprüfung wird nicht durchgeführt
		no	Widerrufsprüfung wird durchgeführt
OCSP Widerrufsprüfung verwenden	SIGforceOCSP	yes	Wenn im Zertifikat angegeben wird OCSP zur Widerrufsprüfung verwendet.

Name	Key	Wert	Bedeutung
		no	Es wird nie über OCSP eine Widerrufsprüfung gemacht
Nach Ablauf der Gültigkeit der Widerrufsliste	SIGONEXPIRY	yes	Widerrufsliste wird nach Ablauf ihrer Gültigkeit aktualisiert
		no	
Alle xx Minuten	SIGXXMINUTES	1 - 60	Die Widerrufsliste wird im angegebenen Intervall aktualisiert
Widerrufsprüfung ausschalten	SSLCHECK	yes	Widerrufsprüfung wird nicht durchgeführt
		no	Widerrufsprüfung wird durchgeführt
OCSP Widerrufsprüfung verwenden	SSLforceOCSP	yes	Wenn im Zertifikat angegeben wird OCSP zur Widerrufsprüfung verwendet.
		no	Es wird nie über OCSP eine Widerrufsprüfung gemacht
Nach Ablauf der Gültigkeit der Widerrufsliste	SSLONEXPIRY	yes	Widerrufsliste wird nach Ablauf ihrer Gültigkeit aktualisiert
		no	
Alle xx Minuten	SSLXXMINUTES	1 - 60	Die Widerrufsliste wird im angegebenen Intervall aktualisiert
Widerrufsdämon beim Starten von trustDesk aktivieren	startCrlDaemon	yes	Widerrufsdämon wird gestartet. Dies verzögert den Aufruf des Programmes
		no	Dämon wird nicht gesartet
Alle xx Stunden die Liste aufarbeiten und die eingetragenen Widerrufslisten beziehen	ProcessList	2 - 24	Zeitintervall, in dem der Dämon die Widerrufslisten auf Ihre Aktualität hin überprüfen und gegebenenfalls neu bezieht
Widerrufslisten, die in den letzten xx Tagen nicht benutzt wurden aus der Liste entfernen	RemoveCRL	2 - 24	Zeitraum, nach dessen Ablauf eine unbenutzte Widerrufsliste aus der Liste entfernt werden soll.
.	CADir	c:\debug	
	trustedCADir	c:\debug2	

19 Open Source Lizenzen

Diese Software enthält DynamicLinkLibraries (DLLs), die

- OpenSSL Code
- Freetype Project
- Zlib general purpose compression library
- LibTIFF - TIFF Library und
- JPEG image compression library

enthalten.

Für diese gelten folgende Lizenzen (OpenSSL License, Original SSLeay License):

19.1 OpenSSL License

Copyright (c) 1998-2001 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL. This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com). Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

19.2 The FreeType Project LICENSE

2000-Feb-08 Copyright 1996-2000 by David Turner, Robert Wilhelm, and Werner Lemberg

Introduction

The FreeType Project is distributed in several archive packages; some of them may contain, in addition to the FreeType font engine, various tools and contributions which rely on, or relate to, the FreeType Project.

This license applies to all files found in such packages, and which do not fall under their own explicit license. The license affects thus the FreeType font engine, the test programs, documentation and makefiles, at the very least.

This license was inspired by the BSD, Artistic, and IJG (Independent JPEG Group) licenses, which all encourage inclusion and use of free software in commercial and freeware products alike. As a consequence, its main points are that:

We don't promise that this software works. However, we will be interested in any kind of bug reports. (`as is' distribution)

You can use this software for whatever you want, in parts or full form, without having to pay us. (`royalty-free' usage)

You may not pretend that you wrote this software. If you use it, or only parts of it, in a program, you must acknowledge somewhere in your documentation that you have used the FreeType code. (`credits')

We specifically permit and encourage the inclusion of this software, with or without modifications, in commercial products. We disclaim all warranties covering The FreeType Project and assume no liability related to The FreeType Project.

Legal Terms

Definitions

Throughout this license, the terms `package', `FreeType Project', and `FreeType archive' refer to the set of files originally distributed by the authors (David Turner, Robert Wilhelm, and Werner Lemberg) as the `FreeType Project', be they named as alpha, beta or final release.

`You' refers to the licensee, or person using the project, where `using' is a generic term including compiling the project's source code as well as linking it to form a `program' or `executable'. This program is referred to as `a program using the FreeType engine'.

This license applies to all files distributed in the original FreeType Project, including all source code, binaries and documentation, unless otherwise stated in the file in ist original, unmodified form as distributed in the original archive. If you are unsure whether or not a particular file is covered by this license, you must contact us to verify this.

The FreeType Project is copyright (C) 1996-2000 by David Turner, Robert Wilhelm, and Werner Lemberg. All rights reserved except as specified below.

1. No Warranty

THE FREETYPE PROJECT IS PROVIDED `AS IS' WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT WILL ANY OF THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY DAMAGES CAUSED BY THE USE OR THE INABILITY TO USE, OF THE FREETYPE PROJECT.

2. Redistribution

This license grants a worldwide, royalty-free, perpetual and irrevocable right and license to use, execute, perform, compile, display, copy, create derivative works of, distribute and sublicense the FreeType Project (in both source and object code forms) and derivative works thereof for any purpose; and to authorize others to exercise some or all of the rights granted herein, subject to the following conditions:

Redistribution of source code must retain this license file (`LICENSE.TXT') unaltered; any additions, deletions or changes to the original files must be clearly indicated in accompanying documentation. The copyright notices of the unaltered, original files must be preserved in all copies of source files.

Redistribution in binary form must provide a disclaimer that states that the software is based in part of the work of the FreeType Team, in the distribution documentation. We also encourage you to put an URL to the FreeType web page in your documentation, though this isn't mandatory.

These conditions apply to any software derived from or based on the FreeType Project, not just the unmodified files. If you use our work, you must acknowledge us. However, no fee need be paid to us.

3. Advertising

Neither the FreeType authors and contributors nor you shall use the name of the other for commercial, advertising, or promotional purposes without specific prior written permission.

We suggest, but do not require, that you use one or more of the following phrases to refer to this software in your documentation or advertising materials: `FreeType Project', `FreeType Engine', `FreeType library', or `FreeType Distribution'.

As you have not signed this license, you are not required to accept it. However, as the FreeType Project is copyrighted material, only this license, or another one contracted with the authors, grants you the right to use, distribute, and modify it.

Therefore, by using, distributing, or modifying the FreeType Project, you indicate that you understand and accept all the terms of this license.

4. Contacts

There are two mailing lists related to FreeType:

freetype@freetype.org

Discusses general use and applications of FreeType, as well as future and wanted additions to the library and distribution. If you are looking for support, start in this list if you haven't found anything to help you in the documentation.

devel@freetype.org

Discusses bugs, as well as engine internals, design issues, specific licenses, porting, etc.

http://www.freetype.org

Holds the current FreeType web page, which will allow you to download our latest development version and read online documentation.

You can also contact us individually at:

David Turner <david.turner@freetype.org>

Robert Wilhelm <robert.wilhelm@freetype.org>

Werner Lemberg <werner.lemberg@freetype.org>

end of LICENSE.TXT

19.3 Zlib general purpose compression library License

zlib.h -- interface of the 'zlib' general purpose compression library version 1.2.1, November 17th, 2003

Copyright (C) 1995-2003 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

19.4 LibTIFF - TIFF Library

Use and Copyright

Copyright (c) 1988-1997 Sam Leffler

Copyright (c) 1991-1997 Silicon Graphics, Inc.

Permission to use, copy, modify, distribute, and sell this software and its documentation for any purpose is hereby granted without fee, provided that (i) the above copyright notices and this permission notice appear in all copies of the software and related documentation, and (ii) the names of Sam Leffler and Silicon Graphics may not be used in any advertising or publicity relating to the software without the specific, prior written permission of Sam Leffler and Silicon Graphics.

THE SOFTWARE IS PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EXPRESS, IMPLIED OR OTHERWISE, INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

IN NO EVENT SHALL SAM LEFFLER OR SILICON GRAPHICS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES OF ANY KIND, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER OR NOT ADVISED OF THE POSSIBILITY OF DAMAGE, AND ON ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

19.5 JPEG image compression library License

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

This software is copyright (C) 1991-1998, Thomas G. Lane.

All Rights Reserved except as specified below.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch, sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA.

ansi2knr.c is NOT covered by the above copyright and conditions, but instead by the usual distribution terms of the Free Software Foundation; principally, that you must include source code if you redistribute it. (See the file ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part of any program generated from the IJG code, this does not limit you more than the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf.

It is copyright by the Free Software Foundation but is freely distributable.

The same holds for its supporting scripts (config.guess, config.sub, ltconfig, ltmain.sh). Another support script, install-sh, is copyright by M.I.T. but is also freely distributable.

It appears that the arithmetic coding option of the JPEG spec is covered by patents owned by IBM, AT&T, and Mitsubishi. Hence arithmetic coding cannot legally be used without obtaining one or more licenses. For this reason, support for arithmetic coding has been removed from the free JPEG software.

(Since arithmetic coding provides only a marginal gain over the unpatented Huffman mode, it is unlikely that very many implementations will support it.)

So far as we are aware, there are no patent restrictions on the remaining code.

The IJG distribution formerly included code to read and write GIF files. To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce "uncompressed GIFs". This technique does not use the LZW algorithm; the resulting GIF files are larger than usual, but are readable by all standard GIF decoders.

We are required to state that

The Graphics Interchange Format(c) is the Copyright property of

CompuServe Incorporated. GIF(sm) is a Service Mark property of CompuServe Incorporated."

20 Wörterbuch

Begriff	Erklärung
Bürgerkarte	Elektronischer Ausweis, meistens in Form einer Chipkarte, die die sichere elektronische Abwicklung von Verwaltungsverfahren und Behördengängen ermöglicht. Die Bürgerkarte ist ein Konzept, das die sichere elektronische Abwicklung von Verwaltungsverfahren und Behördengängen ermöglicht. Das bedeutet, dass sie keine genau vorgeschriebene Art von Karte ist, sondern ein Sicherheitskonzept mit definierten Schnittstellen. Für gewöhnlich findet man Bürgerkarten heute in Form von Chipkarten (sog. Smartcards). Das Konzept ist jedoch nicht auf diese Art der Technologie beschränkt, sondern kann auch andere Formen annehmen; so könnten z.B. Bürgerkarten in Zukunft auch Mobiltelefone oder USB-Geräte sein. Im Wesentlichen kann man sich die physische Bürgerkarte als einen elektronischen Ausweis vorstellen, der es erlaubt, sich auf elektronischem Wege gegenüber Behörden und Ämtern auszuweisen und rechtsgültige elektronische Unterschriften zu leisten. Mehr Informationen zum Thema Bürgerkarte und ein aktuelles Verzeichnis der Anbieter für Bürgerkarten in Österreich finden Sie auf der Webseite des österreichischen Zentrums für sichere Informationstechnologie(A-SIT) unter der URL: http://www.buergerkarte.at
Bürgerkartenumgebung	Software, die mit der Bürgerkarte kommuniziert
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 signie-renden Dokument errechnet wird und zum Überprüfen der sicheren digitalen Signatur dient
	Infoboxen sind Datenspeicher, die mit einer Bürgerkarte verknüpfte Informationen enthalten. Es gibt zwei Arten der Speicherung von Infoboxen: Infobox Üblicherweise befindet sich die Infobox auf Ihrer Smartcard und enthält zum Beispiel Ihre Personenbindung für E-Government. Virtuelle Infobox Virtuelle Infoboxen können auf der Platte Ihres Computers oder auf der Smartcard erstellt, gelesen, aktualisiert und gelöscht werden. Folgende Infoboxen stehen Ihnen auf vielen Karten standardmäßig zur Verfügung: Personenbindung.

Begriff	Erklärung
	Diese Infobox enthält die Personenbindung des Bürgers. Das ist ein vom zentralen Melderegister elektronisch signierter Datensatz, der die beiden Standard-Schlüssel der Bürgerkarte an die ZMR-Nummer des Bürgers bindet, wodurch der Bürger eindeutig identifiziert werden kann, wenn er sich an eine Behörde wendet. Mehr Informationen zur Personenbindung finden Sie auf der Homepage des Konzepts Bürgerkarte (www.buergerkarte.at) Zertifikate Diese Infobox enthält die oben bereits erwähnten Zertifikate mit den öffentlichen Schlüsseln einer Person (standardmäßig bei der Bürgerkarte die Zertifikate zu Signatur-Schlüsselpaar und Geheimhaltungs-Schlüsselpaar); Mandates (Vollmachten) Diese Infobox enthält die Vollmachten des Bürgers.
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 elektronische oder qualifizierte digitale Signatur	Siehe „Sichere elektronische Signatur
Qualifizierte Zertifikate	§ 2 Z 9 SigG „qualifizierte Zertifikate“.
SecurityLayer	XML Schnittstelle zwischen Bürgerkartenumgebung und Applikationen, die mit dieser arbeiten
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 Fest-stellung 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

Begriff	Erklärung
	nachträgliche Veränderung der Daten erkennbar ist. auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und mit einer sicheren Signatur Erstellungseinheit erzeugt werden. 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. 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. Bei der digitalen Unterschrift wird aus dem zu signierenden Dokument zunächst ein Hashwert errechnet. Der Hashwert des Dokumentes wird mit dem privaten Schlüssel des Unterzeichnenden verschlüsselt und gemeinsam mit dem Unterzeichner (=Zertifikat) dem Dokument hinzugefügt. 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. 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.
Signator oder Unterzeichner	§ 2 Z 2 SigG „Signaturschlüssel-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	§ 2 Z 5 SigG: Konfigurierte Soft- oder Hardware zur Verarbeitung der Signaturerstellungsdaten; z.B. eine SmartCard. 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.
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 Signatur-anwendungskomponente ist.
Signaturprüfschlüssel	§ 2 Zi 6 SigG „Signaturprüfschlüssel“ (öffentlicher kryptografischer Schlüssel zur Überprüfung verwendet).
Signaturschlüssel	§ 2 Zi. 4. SigG „Signaturschlüssel“ (privater kryptografischer Schlüssel

Begriff	Erklärung
	zur Signaturerstellung).
SmartCard	Siehe „Signaturerstellungskomponente“
SmartCard-Reader	Siehe „Signaturerstellungskomponente“
Trustcenter	s. Zertifizierungsdiensteanbieter
Viren	Das sind „bösartige“ 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 bösartige) Funktionen verursachen.
XML	XML oder eXtended Markup Language ist ein nach bestimmten Standardrichtlinien der Organisation W3C erstelltes Dokument. Wurden diese W3C-Richtlinien bei der Erstellung des Dokuments nicht eingehalten, kann es nicht in der sicheren Anzeige von trustView geladen werden.
Zertifikat	§ 2 Z 8 SigG: Eine elektronische Bescheinigung, mit der Signaturprüfdaten (Z 6) einer bestimmten Person zugeordnet werden und deren Identität bestätigt wird. 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. Es gibt verschiedene Zertifikate, zum Beispiel Signaturzertifikat oder Geheimhaltungszertifikat. Zertifikate werden vom ausstellenden Trustcenter digital signiert und somit vor Manipulationen geschützt, womit ihre Echtheit nachvollziehbar garantiert wird.
Zertifizierungsdiensteanbieter	§ 2 Z 10 SigG: Natürliche oder juristische Person oder sonstige rechtsfähige Einrichtung, die Zertifikate ausstellt oder andere Signatur- und sonstige Zertifizierungsdienste erbringt „

21 Literaturhinweise

E-GovG	E-Government-Gesetz
SigG	Signaturgesetz
SigV	Signaturverordnung