



Ihre Sozialversicherung im Internet

SIGNATUR MIT BÜRGERKARTE

Handbuch

Dokumentenverwaltung

Berechtigungen

Aktion	Name	QS	Teilnehmer
Änderung	Fiala	Intern	
Prüfung	Schuller	Extern	
Freigabe	Schuller		

Änderungsverlauf

Version	Datum	Autor	Änderungshinweis	Status
1.0	14.04.2005	Fiala		freigegeben
1.1	01.09.2005	Fiala	Proxyeinstellungen bei Trust Desk basic Kapitel Problemlösungen	freigegeben
1.2	19.10.2005	Schuller	e-card Bürgerkarte	freigegeben
1.3	22.03.2007	Fiala	Redaktionelle Korrekturen Entfall Testformular	freigegeben
				offen

Offene Punkte

Lfd.Nr.	Datum	Autor	Beschreibung	Status
				offen

Vertraulichkeit: öffentlich

Unterschrift: elektronisch signiert

Ablage: I:\eSV\CC\Support-Betriebsführung\Signatur mit Bürgerkarte\in Arbeit\Handbuch Signatur mit Bürgerkarte V1.3.doc

Inhaltsverzeichnis

1. AUFGABEN DES HANDBUCHS	4
2. VORAUSSETZUNGEN	4
2.1. Signaturkarte.....	4
2.1.1. Aufbringung des Zertifikates auf Ihrer Bankomatkarte	4
2.1.2. Ausstellung einer a-sign Premium Signaturkarte	4
2.1.3. Ausstellung einer e-Card Bürgerkarte.....	5
2.2. Chipkarten Lesegerät.....	5
2.2.1. Bescheinigungen der Aufsichtsstelle für elektronische Signaturen	5
2.2.2. Empfehlungen des Zertifizierungsdiensteanbieters	5
2.2.3. Erfahrungen des Betreibers des Internetportals der österreichischen Sozialversicherung	5
2.3. Bürgerkartenumgebung.....	5
2.3.1. itsolution trustDesk basic	5
2.3.2. BDC HotSign	6
3. INSTALLATION VON CHIPKARTEN LESEGERÄT UND BÜRGERKARTENUMGEBUNG	6
3.1. Installation und Anschluss des Chipkarten Lesegeräts	6
3.2. Installation der Bürgerkartenumgebung.....	7
3.2.1. Installation von itsolution trustDesk basic	7
3.2.2. Installation von BDC HotSign	10
4. VERWENDUNG DER BÜRGERKARTENUMGEBUNG IN EINEM NETZWERK 14	
4.1. Ermitteln des Proxy-Servers	14
4.1.1. Ermitteln des Proxy-Servers mit MS Internet Explorer	14
4.2. Konfiguration eines Proxy-Servers bei Verwendung des itsolution trustdesk.....	16
4.3. Konfiguration eines Proxy Servers bei Verwendung von BDC HotSign	18
5. PROBLEMLÖSUNGEN BEI SPEZIELLEN SIGNATURPROBLEMEN.....	19
5.1. Probleme mit den Widerrufslisten bei itsolution trustdesk	19

1. Aufgaben des Handbuchs

Dieses Dokument beschreibt die Voraussetzungen und die Anwendung der Bürgerkartenumgebung für die Erstellung einer sicheren Signatur oder Verwaltungssignatur.

2. Voraussetzungen

Damit Sie signieren können, benötigen Sie folgende Komponenten:

- Signaturkarte
- Chipkarten Lesegerät
- Bürgerkartenumgebung

2.1. Signaturkarte

Die Signaturkarte enthält Ihr persönliches Zertifikat.

Dabei wird zwischen einem Signaturzertifikat und einem Verschlüsselungszertifikat unterschieden.

Das **Signaturzertifikat** ermöglicht Ihnen das Signieren von Daten („Sichere Signatur“). Das **Verschlüsselungszertifikat** ermöglicht Ihnen das Verschlüsseln von Daten.

Die beiden Zertifikate werden durch unterschiedliche PINs geschützt, die Ihnen bei der Ausstellung der Karte bekannt gegeben wurden.

Im Moment gibt es folgende Möglichkeiten, eine Signaturkarte zu erhalten:

2.1.1. Aufbringung des Zertifikates auf Ihrer Bankomatkarte

Nur Bankomatkarten, die seit Ende Jänner 2005 ausgestellt wurden, verfügen über diese Funktion. Sie erkennen dies prinzipiell daran, dass auf der Rückseite Ihrer Bankomatkarte folgender Schriftzug steht: „a-sign **premium**“. (Bei manchen Banken (z.B. Bank Austria) wird der Schriftzug allerdings nicht aufgebracht – bitte fragen Sie bei Unklarheiten bei Ihrer Bank nach).

Nähere Informationen dazu finden Sie unter

<http://www.a-trust.at/info.asp?node=610&lang=GE&ch=1>

2.1.2. Ausstellung einer a-sign Premium Signaturkarte

Nähere Informationen dazu finden Sie unter

<http://www.a-trust.at/info.asp?node=337&ch=1&lang=GE>

2.1.3. Ausstellung einer e-Card Bürgerkarte

Nähere Informationen dazu finden Sie unter
<http://www.sozialversicherung.at/e-card>

2.2. Chipkarten Lesegerät

2.2.1. Bescheinigungen der Aufsichtsstelle für elektronische Signaturen

Nähere Informationen dazu finden Sie unter
<http://www.signatur.rtr.at/de/providers/products.html>

2.2.2. Empfehlungen des Zertifizierungsdiensteanbieters

Beachten Sie bitte auch die Empfehlungen Ihres Zertifizierungsdiensteanbieters. Er kann am besten beurteilen, welche Chipkarten Lesegeräte für sein Produkt geeignet sind.

Empfehlungen für Bankomatkarten und a-sign Premium Signaturkarten

Eine vollständige Liste der von A-Trust empfohlenen Kartenleser finden Sie unter
<http://www.a-trust.at/default.asp?lang=GE&ch=1&node=556>

2.2.3. Erfahrungen des Betreibers des Internetportals der österreichischen Sozialversicherung

Mit folgenden Kartenlesern haben wir gute Erfahrungen gemacht:

- Reiner SCT cyberJack® Chipkartenleser
- Towitoko CHIPDRIVE® pinpad / SCM Microsystems SPR532

2.3. Bürgerkartenumgebung

Die Bürgerkartenumgebung ist die Software, die das Signieren von Daten ermöglicht. Die Bürgerkartenumgebung übernimmt dabei die Kommunikation mit dem Chipkarten Lesegerät bzw. der eingelegten Karte.

2.3.1. itsolution trustDesk basic

Downloadmöglichkeit: Homepage Bürgerkarte des Bundes
<http://www.buergerkarte.at>

(BKU für a-sign Premium für Microsoft Windows 2000/XP)

Downloadmöglichkeit: Internetportal der österreichischen Sozialversicherung
<http://www.sozialversicherung.at/e-card>

(BKU für a-sign Premium und e-Card Bürgerkarte für Microsoft Windows 2000/XP)

Das Handbuch des trustDesk basic finden Sie hier
<http://www.buergerkarte.at>

Hersteller: itsolution GmbH
<http://www.itsolution.at>

Aktuelle Version: 2.7.1

2.3.2. BDC HotSign

Downloadmöglichkeit: Homepage der A-Trust GmbH.
<http://www.a-trust.at/clientsw/>
(Bereich Privat, Link "Download Software" rechts oben)

Das Handbuch des BDC HotSign finden Sie hier:
<http://www.a-trust.at/clientsw/downloads/hotSign/hotSign-Benutzerhandbuch%20V0.9.pdf>

Hersteller: BDC Consulting GmbH
<http://www.bdc.at>

Aktuelle Version: 1.3

3. Installation von Chipkarten Lesegerät und Bürgerkartenumgebung

Wenn Sie die oben angeführten Voraussetzungen erfüllen, empfehlen wir folgendes Vorgehen:

- Installation und Anschluss des Chipkarten Lesegeräts.
- Installation der Bürgerkartenumgebung
- Verwendung der Signatur

3.1. Installation und Anschluss des Chipkarten Lesegeräts

Legen Sie die Setup-CD, die bei Ihrem Chipkarten Lesegerät mitgeliefert wird, ein und installieren Sie die Treiber Ihres Chipkarten Lesegeräts. Das Installationsprogramm sollte sich automatisch nach dem Einlegen der CD starten. Befolgen Sie die Anweisungen des Installationsprogramms.

Sobald die Treiber erfolgreich installiert sind, können Sie das Chipkarten Lesegerät anschließen. Bei Geräten mit Anschlussmöglichkeit über USB ist dabei kein Neustart des Rechners erforderlich.

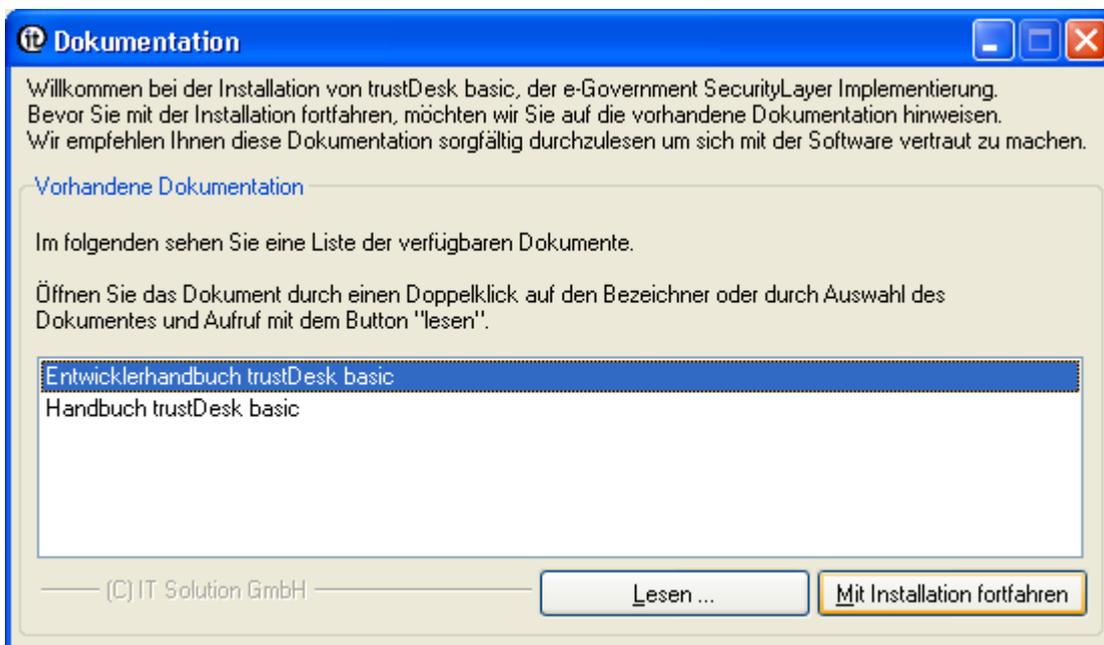
3.2. Installation der Bürgerkartenumgebung

Sofern das Chipkarten Lesegerät ordnungsgemäß installiert und angeschlossen wurde, wird, wenn Sie die Installationsroutine der Bürgerkartenumgebung starten, Ihr Chipkarten Lesegerät automatisch erkannt.

Die Installationsroutine erkennt das angeschlossene Chipkarten Lesegerät und zeigt Ihnen dieses zur Kontrolle an. Erfolgt diese Anzeige nicht, fordern Sie bitte Unterstützung durch den Hersteller Ihres Chipkarten Lesegerätes an.

3.2.1. Installation von itsolution trustDesk basic

Nach dem Starten der Installationsroutine (trustDeskbasic.2-4-3.exe) wird folgender Dialog eingeblendet.:



Sie können die Handbücher lesen und dann mit der Installation fortfahren (Button „Mit Installation fortfahren“).

Danach erkennt die Installationsroutine automatisch, welche Chipkarten Lesegeräte Sie installiert haben. Im nachfolgenden Beispiel wurden zwei Chipkarten Lesegeräte (Reiner SCT und SCM Microsystems) installiert:



Quittieren Sie mit OK.

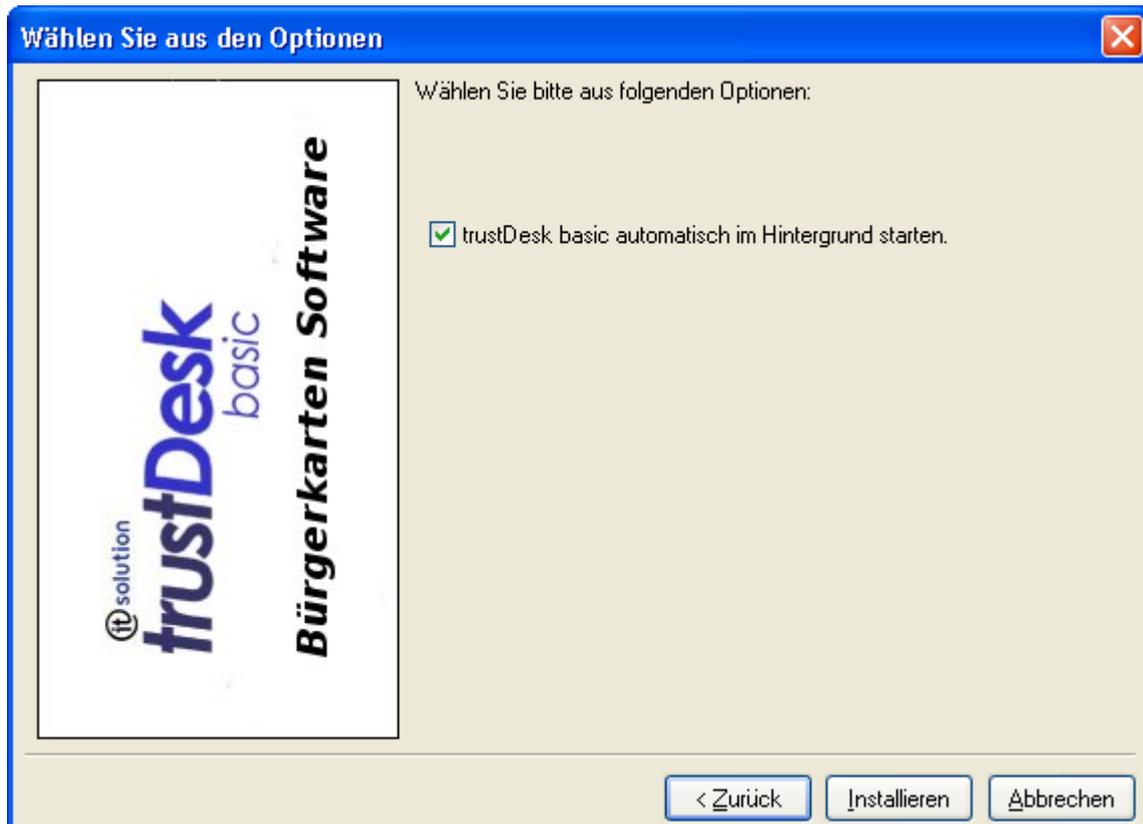
Sie werden gefragt, ob Sie mit der Installation fortfahren möchten:



Bestätigen Sie mit „Ja“.

Bestätigen Sie die folgenden Dialoge mit „Weiter“.

Auf der letzten Dialogseite vor dem Installieren lassen Sie die Checkbox für den automatischen Start am behakt. Dies bewirkt, dass trustDesk basic bei jedem Start Ihres PCs automatisch gestartet wird.



Bestätigen Sie mit "Installieren"

Am Ende bekommen Sie folgende Meldung angezeigt:



Bestätigen Sie mit "OK".

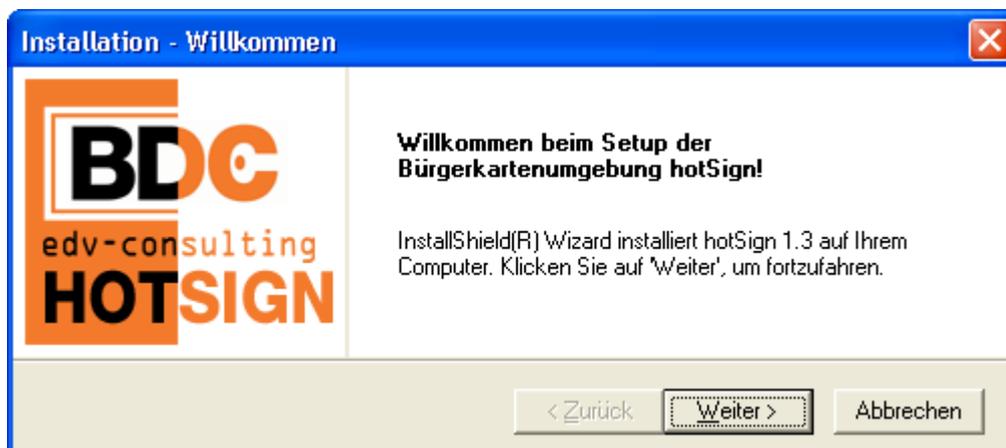
Beim Starten von trustDesk basic wird Ihnen immer ein Kurzhinweis des Tages angezeigt:



Sie können diesen durch Enthaken der Checkbox links unten („Kurzhinweise beim Start anzeigen“) deaktivieren.

3.2.2. Installation von BDC HotSign

Die Installationsroutine beginnt mit folgender Einleitung:



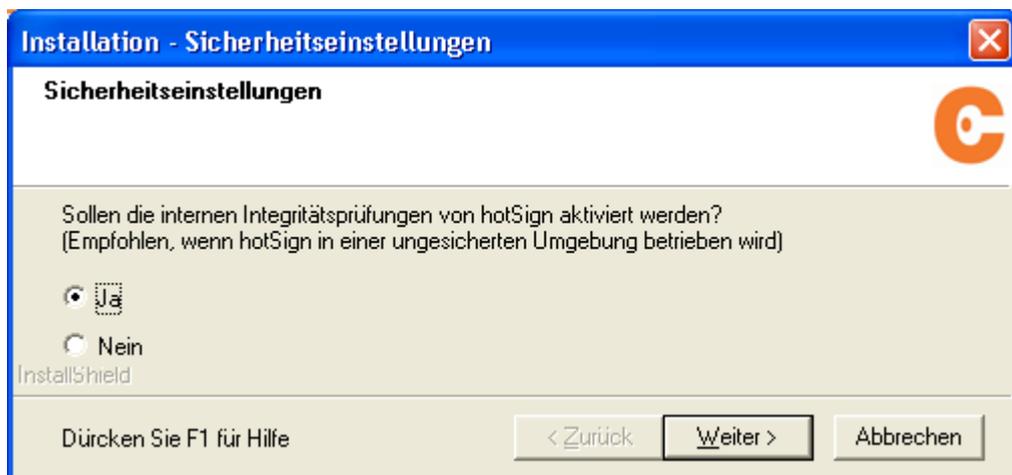
Bestätigen Sie mit “Weiter”.

Wählen Sie den Pfad, in den Sie den BDC HotSign installieren möchten, mit der Funktion „Durchsuchen...“:



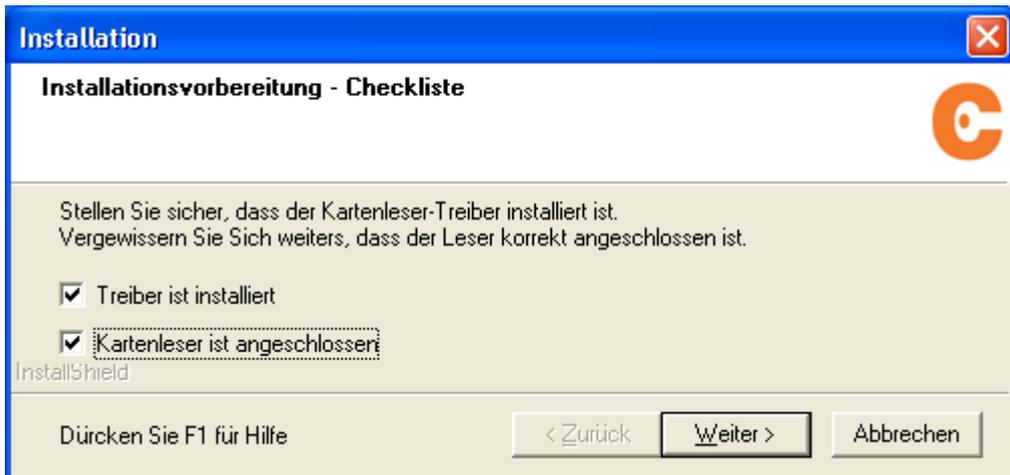
Möchten Sie den Zielordner nicht verändern oder nach Abschluss der Auswahl des Zielordners bestätigen Sie mit "Weiter".

Bei den Sicherheitseinstellungen empfehlen wir die Standardkonfiguration, wobei HotSign interne Integritätsprüfungen aktiviert:



Bestätigen Sie mit "Weiter"

Sie werden von HotSign gefragt, ob Sie sowohl die Treiber installiert als auch den Kartenleser angeschlossen haben. Bitte prüfen Sie beides und behaken Sie die Kontrollkästchen:



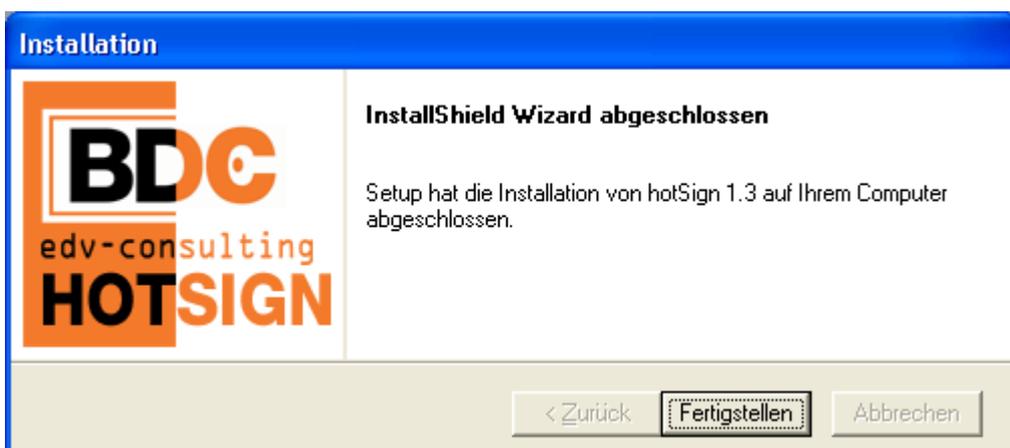
Bestätigen Sie mit "Weiter".

Danach erkennt die Installationsroutine automatisch, welche Chipkarten Leser Sie installiert haben. Im nachfolgenden Beispiel wurde ein Chipkarten Lesegerät (SCM Microsystems) installiert:



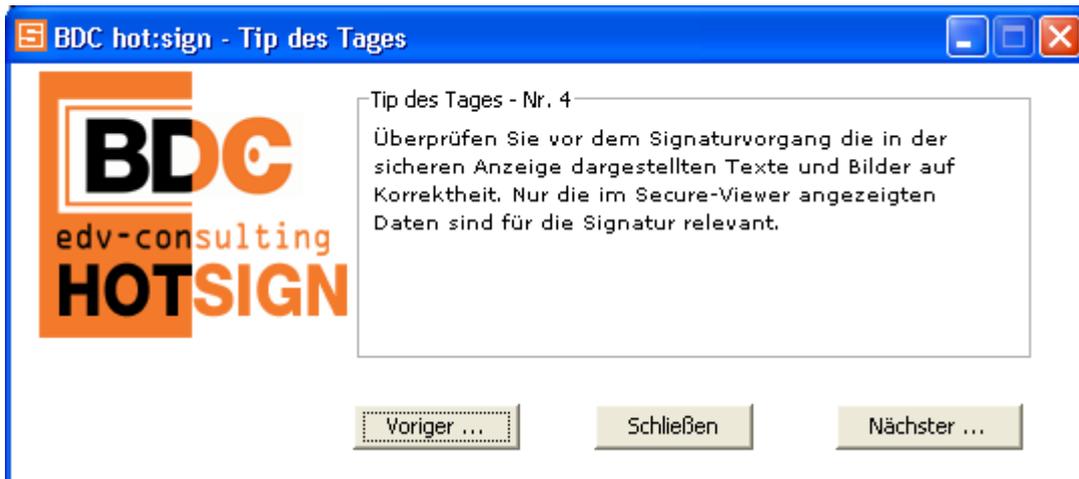
Bestätigen Sie mit "Ja".

Nach dem Abschluss der Installationsroutine erhalten Sie folgende Meldung.



Bestätigen Sie mit „Fertigstellen“.

Beim Starten von BDC HotSign wird Ihnen immer ein Tip des Tages angezeigt:



Den Tip des Tages können Sie wie folgt deaktivieren:

Klicken Sie mit der rechten Maustaste auf das Icon  und wählen Sie Verwaltung -> Tip des Tages. Dadurch wird das Häkchen links davon entfernt und der Tip wird beim nächsten Start nicht mehr eingeblendet.



Anzeige nach Deaktivierung des „Tip des Tages“:



4. Verwendung der Bürgerkartenumgebung in einem Netzwerk

Sowohl itsolution trustdesk als auch hotsign unterstützen die Konfiguration eines Proxy-Servers.

Ein Proxy-Server dient als zentraler Verbindungsserver ins Internet. Jeder PC im Netzwerk muß diesen Proxy-Server bekannt geben, damit die Verbindung ins Internet über diesen Server aufgebaut werden kann.

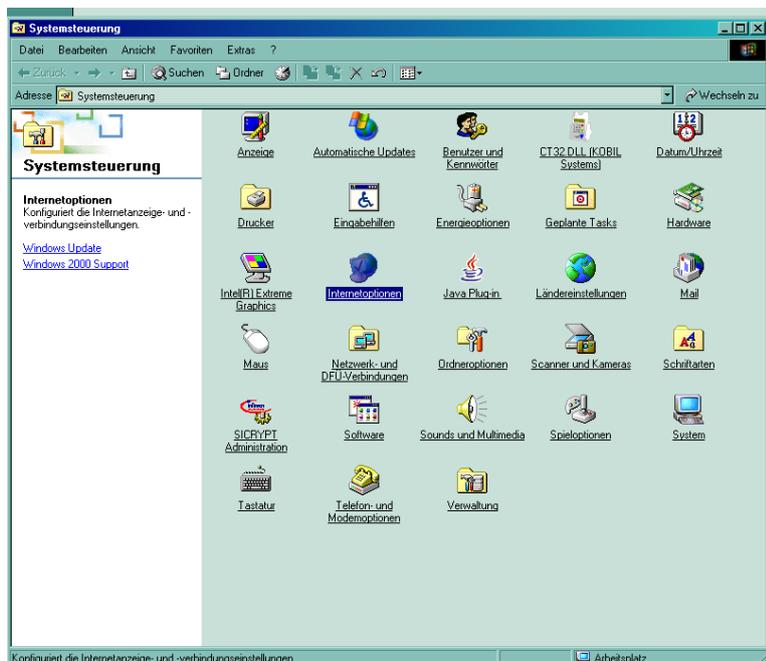
4.1. Ermitteln des Proxy-Servers

Für die Ermittlung des Proxy-Servers gibt es zwei Möglichkeiten:

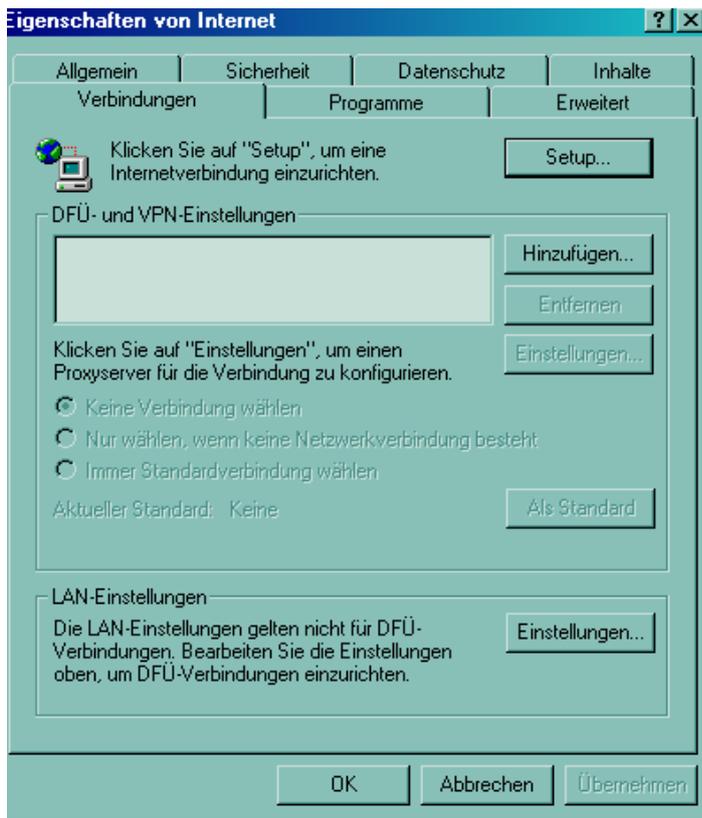
- Sie ermitteln diesen anhand der Einstellungen in Ihrem Browser (nachfolgend dokumentiert für Internet Explorer).
- Wenn dies nicht möglich ist, oder zu keinem Ergebnis führt, dann fragen Sie bitte Ihren Netzwerkbetreuer.

4.1.1. Ermitteln des Proxy-Servers mit MS Internet Explorer

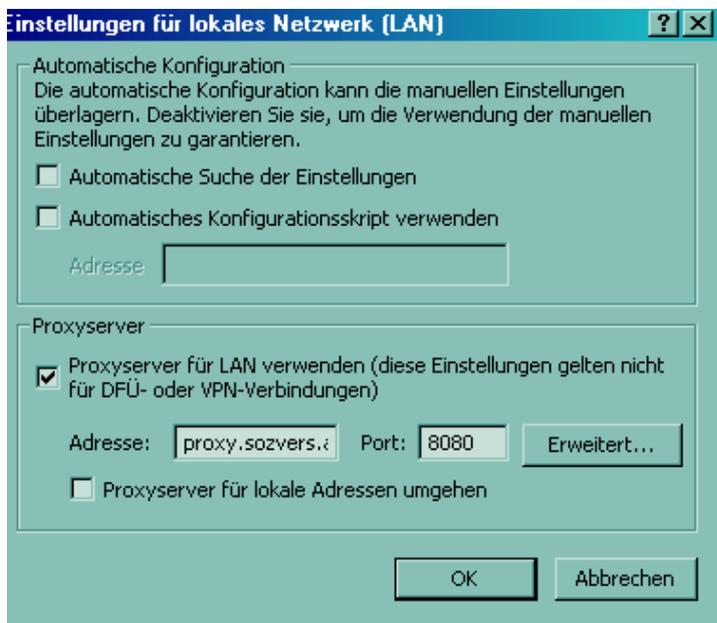
Wählen Sie im Startmenü Einstellungen –> Systemsteuerung aus.



Wählen Sie „Internetoptionen“ und die Registerkarte „Verbindungen“



Wählen Sie „Einstellungen“:



Notieren Sie den bei der Adresse eingegebene Proxy-Server (bzw. kopieren Sie diesen über die Zwischenablage).

4.2. Konfiguration eines Proxy-Servers bei Verwendung des itsolution trustdesk

Stellen Sie sicher, dass der itsolution trustdesk aktiv ist (erkennbar an dem gelben Icon rechts unten in der Taskleiste).

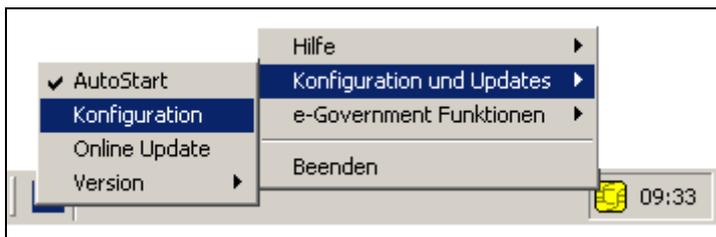


Abbildung 1: Konfigurieren des itsolution trustdesk

Klicken Sie mit der rechten Maustaste auf das gelbe Icon (Chipkarte), und wählen Sie Konfiguration und Updates und dann das Untermenü Konfiguration.

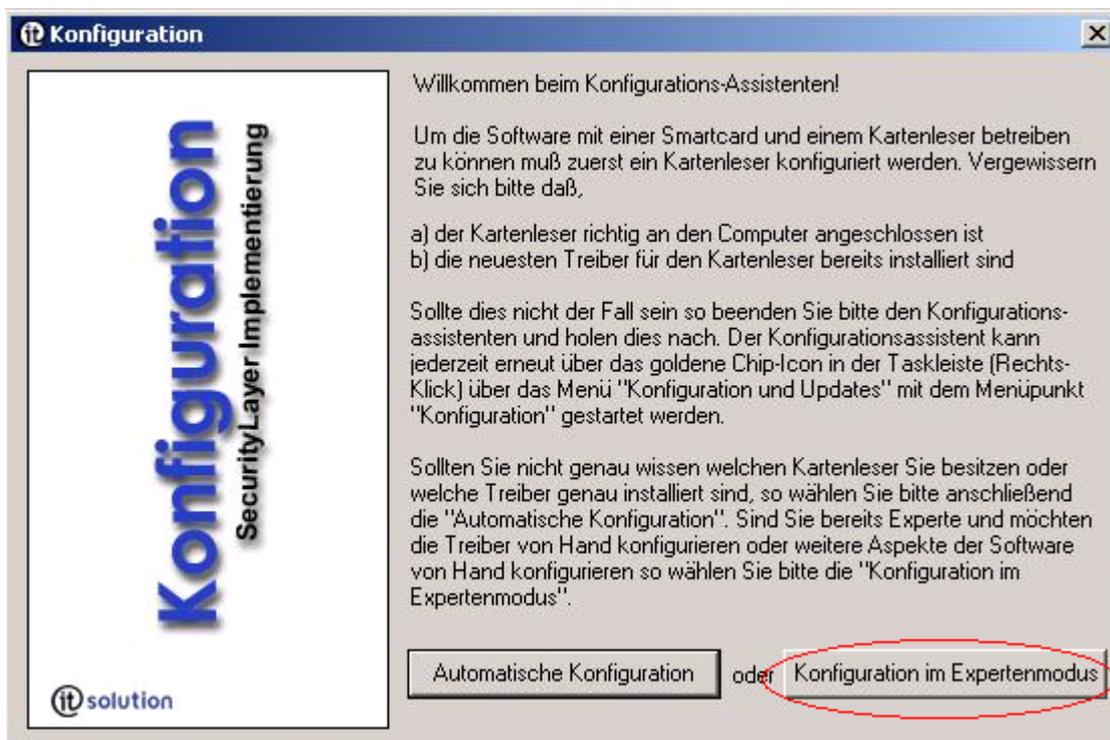


Abbildung 2: Auswahl des Expertenmodus bei itsolution trustdesk

Klicken Sie auf den Button „Konfiguration im Expertenmodus“.

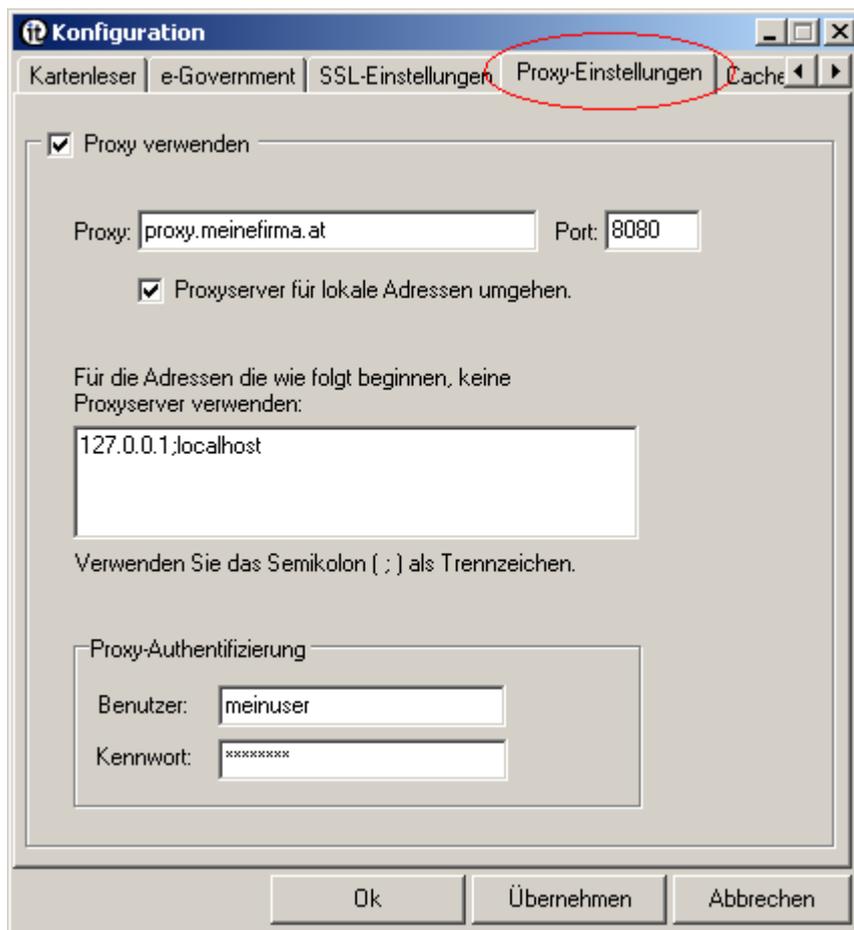


Abbildung 3: Konfiguration der Proxy-Einstellungen bei itsolution trustdesk

Wählen Sie den Reiter „Proxy-Einstellungen“ aus.

Behaken Sie die Option „Proxy verwenden“.

Nun können Sie den Proxy-Server im Feld „Proxy“ eintragen. Sie können diesen auch wie vorher beschrieben aus den Einstellungen des Internet-Explorers über die Zwischenablage übernehmen.

Tragen Sie auch den Port des Proxy-Servers ein (ist auch aus den Einstellungen des Internet-Explorers ablesbar).

Weiters sollten Sie den Proxy-Server für lokale Adressen deaktivieren (da Sie für den Zugriff auf das lokale System nicht den Weg über den Proxy gehen sollten). Tragen Sie dazu die folgenden Adressen ein: „127.0.0.1;localhost“ (siehe oben).

Falls Ihr Proxy eine Authentifizierung verlangt, dann können Sie diese in der Feldgruppe „Proxy-Authentifizierung“ eingeben.

Danach klicken Sie bitte auf Übernehmen und dann auf Ok.

Nun können Sie den itsolution trustdesk mit Proxy-Server verwenden.

4.3. Konfiguration eines Proxy Servers bei Verwendung von BDC HotSign

Beim BDC HotSign-1.3 können Sie einen Proxy Server eintragen. Klicken Sie mit der rechten Maustaste auf das Icon  und wählen Sie „Verwaltung -> Proxy-Einstellungen“.



Danach öffnet sich folgender Dialog:



Hier können Sie die Daten Ihres Proxies eintragen.

Wenn Sie die Checkboxes behaken, können Sie die Proxydaten in die Felder eingeben:



Wir empfehlen, sowohl bei „proxy:port“ als auch „secure proxy:port“ den Proxy einzutragen. Damit wird sowohl für „proxy“ als auch „secure proxy“ der Proxy „proxy.meinefirma.at“ verwendet.

Wenn Ihr Proxy eine Authentifizierung (User / Password) erfordert, dann müssen Sie diese ebenso eintragen. Die Anmeldung beim Proxy Server erfolgt mit dem Benutzer „meinuser“ und dem Kennwort „kennwort“.

Wählen Sie „Speichern“, um Ihre Eingaben zu speichern.

Nach dem Ändern der Konfiguration ist ein Neustart von HotSign erforderlich.

Wählen Sie dazu rechte Maustaste auf das Icon  und wählen „hotsign beenden“. Danach starten Sie den HotSign neu über Start -> Programme -> BDC Consulting EDV GmbH -> Bürgerkartenumgebung hotSign -> hotSign 1.3.

Beim nächsten Signiervorgang erfolgt die Kommunikation mit dem Internet dann über den eingetragenen Proxy Server.

5. Problemlösungen bei speziellen Signaturproblemen

5.1. Probleme mit den Widerrufslisten bei itsolution trustdesk

Es kann vorkommen, dass die Signatur aufgrund von Problemen mit der Widerrufsliste fehlschlägt. Dies erkennen Sie daran, dass die Signatur nach dem Klicken des Buttons „Signieren“ abgebrochen wird.

Ob das Problem mit der Widerrufsliste zusammenhängt, können Sie wie folgt prüfen:

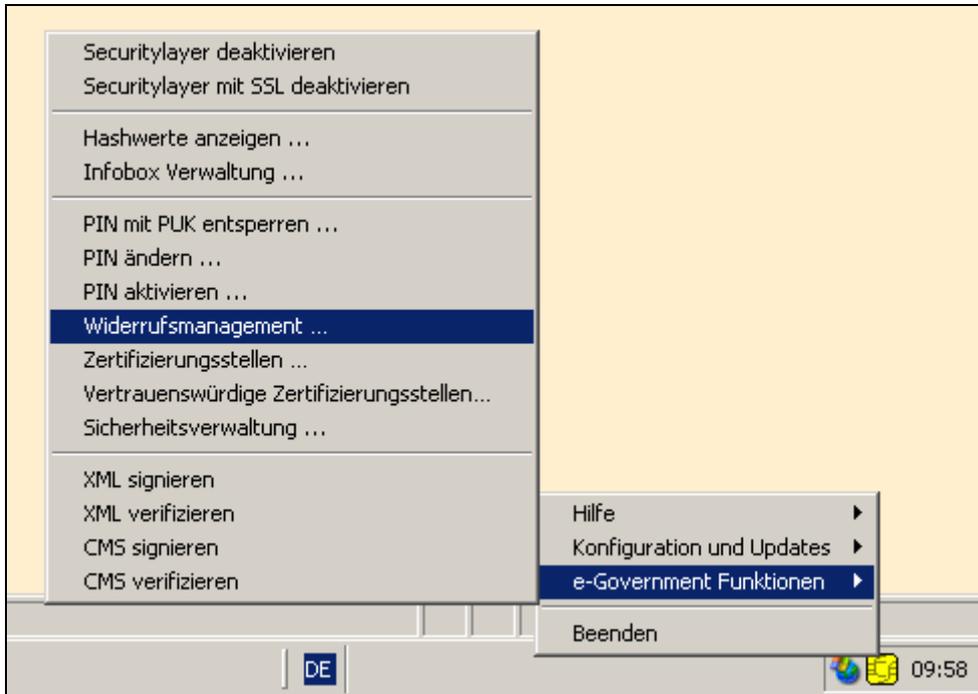


Abbildung 4: Auswählen des Widerrufsmanagements des itsolution trustdesk

Wählen Sie den Reiter „Widerrufslisten Verteilungspunkte“. Dort sind sämtliche Verteilungspunkte von Widerrufslisten angeführt.

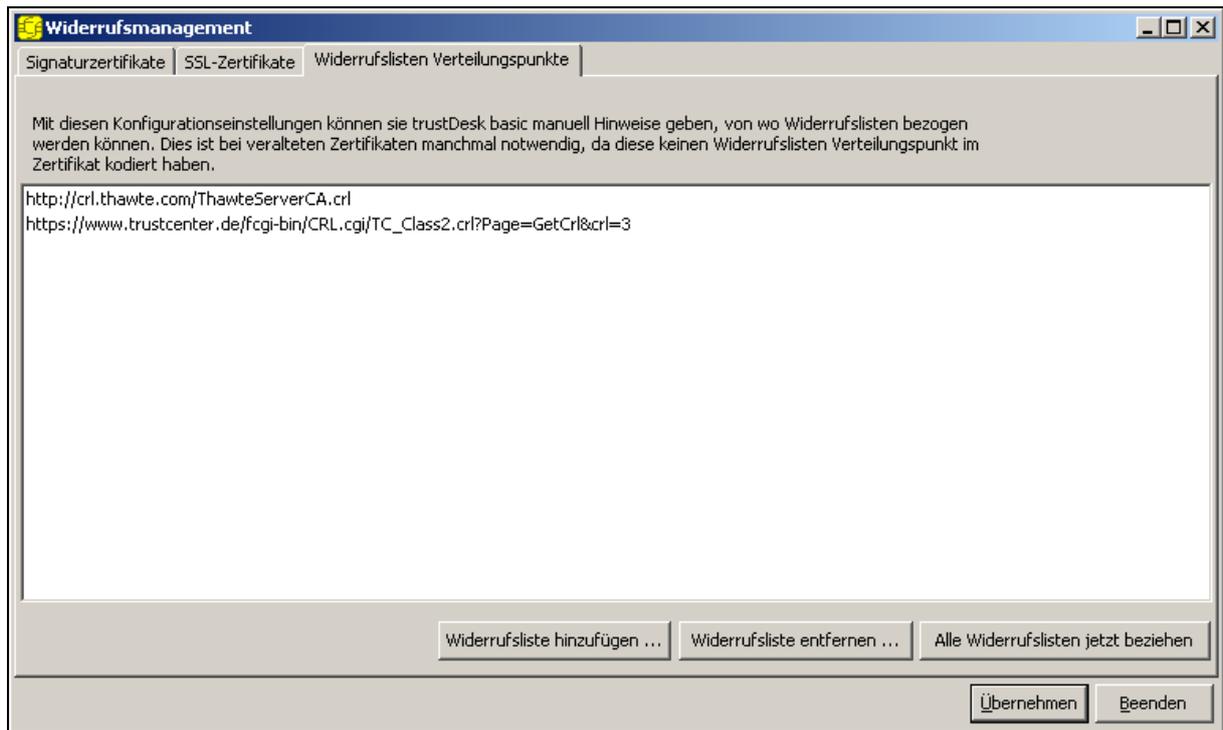


Abbildung 5: Widerrufslisten-Verteilungspunkte

Betätigen Sie den Button „Alle Widerrufslisten jetzt beziehen“, um diese herunterzuladen. Wenn es dabei Probleme gibt, bekommen Sie eine Fehlermeldung angezeigt:



Abbildung 6: Fehlermeldung bei Problemen mit dem Download der Widerrufslisten

Wenn Sie diese Fehlermeldung bekommen, dann sind die Widerrufslisten aktuell nicht abrufbar. In diesem Fall können Sie nur signieren, wenn Sie die Widerrufslistenprüfung vorübergehend deaktivieren.

Dies können Sie wie folgt durchführen:

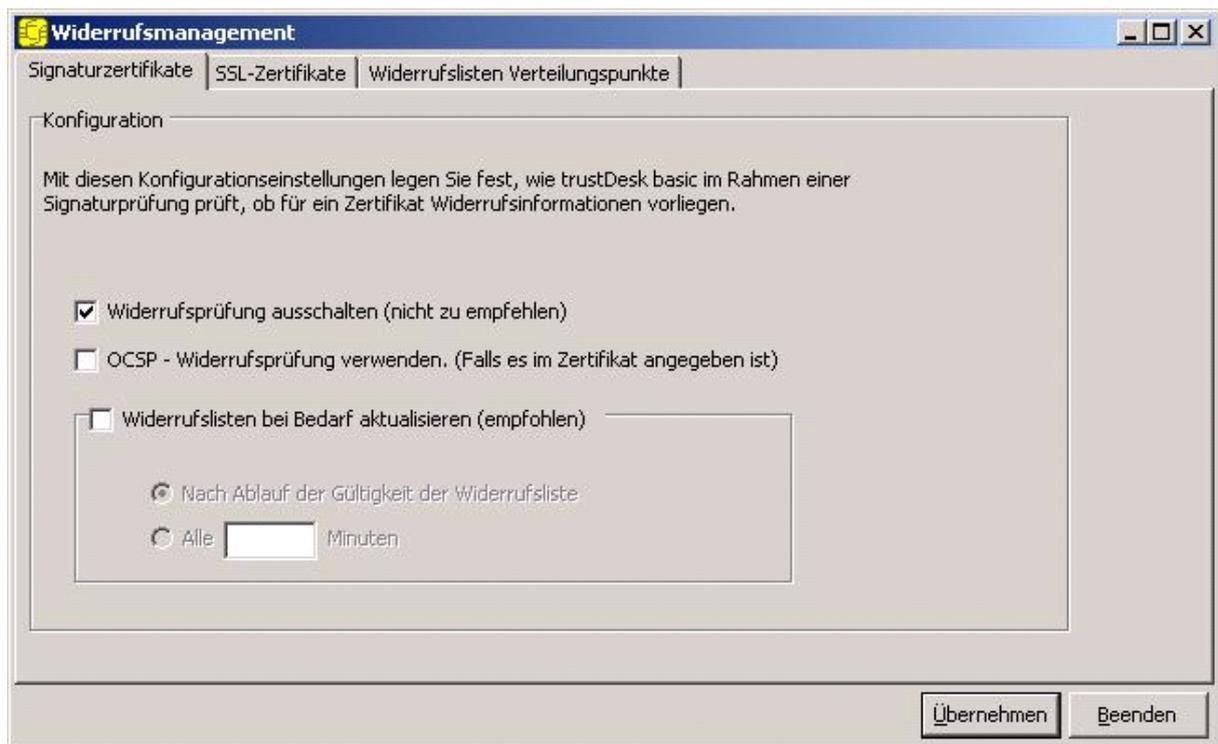


Abbildung 7: Deaktivieren der Widerrufsprüfung bei Signaturzertifikaten

Wählen Sie den Reiter „Signaturzertifikate“ und behaken Sie die Checkbox „Widerrufsprüfung ausschalten“.

Dann klicken Sie auf den Reiter „SSL-Zertifikate“.

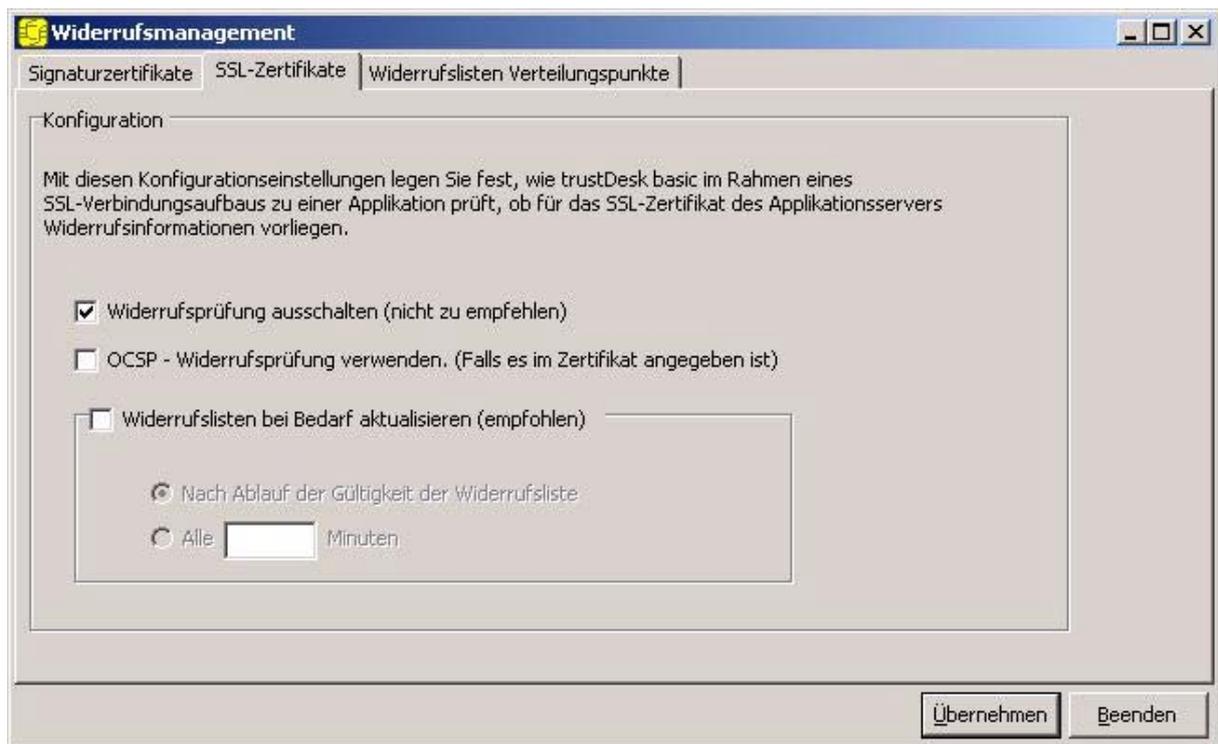


Abbildung 8: Deaktivieren der Widerrufsprüfung bei SSL-Zertifikaten

Wählen Sie den Reiter „SSL-Zertifikate“ und behaken Sie die Checkbox „Widerrufsprüfung ausschalten“.

Danach können Sie wieder normal signieren, auch wenn die Widerrufslisten nicht verfügbar sind. Zu einem späteren Zeitpunkt sollten Sie die Prüfung aber wieder aktivieren.

Signaturwert	3MBWzmNBVzuYY2dshjMaucc6mFWO5zBKho1YqLSux/+d2PgCNW2wp6xH/33kH4C0	
	Signator	C=AT, OU=VSig, O=Hauptverband österr. Sozialvers., CN=Christian Schuller
	Datum	2007-04-03T10:52:14Z
	Aussteller	C=AT,O=Hauptverband österr. Sozialvers.,CN=VSig CA 2
	Seriennummer	17073242825552318146228410362163479320836
Hinweis:	Der Textinhalt dieses Dokumentes wurde ohne Formatsteuerungen elektronisch signiert	
Kennzeichnung	1175597534-19042046@6345-7573-23309-14078-15954')/child::etsi:QualifyingProperties/child::etsi:SignedProperties)	