

a.sign Client Benutzerhandbuch (Programmversion 1.2.x.x)

Inhaltsverzeichnis

1.2	Allgemeines	2
1.2.3	a.sign Client – wozu?	2
1.2.4	Was kann der a.sign Client?	2
1.3	Voraussetzungen	3
1.3.3	Unterstützte Betriebssysteme	3
1.3.4	Empfohlene Kartenlesegeräte	4
1.4	Installation des a.sign Client	5
1.4.3	Voraussetzungen unter Windows 98/98SE/NT/ME	5
1.4.4	Update einer älteren a.sign Client Installation	5
1.4.5	Installation des a.sign Client über den a.sign Installer	8
1.4.6	Manuelle Installation des a.sign Client	8
1.4.7	a.sign Client deinstallieren	14
1.5	Ich habe den a.sign Client installiert – was nun?	14
1.6	Funktionen des a.sign Client Administrationsprogramms	16
1.6.3	Karten aktualisieren	16
1.6.4	Lokale Funktionen	16
1.6.4.4	Kartenverwaltung	17
1.6.4.5	Pin ändern	18
1.6.4.6	Pin entsperren	20
1.6.4.7	Zertifikat anzeigen	22
1.6.4.8	Personenbindung anzeigen	23
1.6.4.9	Pin hinterlegen	25
1.6.4.10	Kartenleser	26
1.6.4.11	Diagnose	28
1.6.4.12	Einstellungen	29
1.6.4.13	Aktualisierung	30
1.6.4.14	Plugins	32
1.6.5	Kundendienste Online	33
1.6.5.4	ZMR – Zentrales Melderegister	34
1.6.5.5	Vertragsdaten ändern	37
1.6.5.6	Verzeichnisdienst Eintrag verwalten	39
1.6.5.7	Verzeichnisdienst Suche	41
1.6.5.8	PUK Dienst	44
1.6.6	a.sign Client beenden	45
1.7	Troubleshooting	45

1.2 Allgemeines

Dieses Benutzerhandbuch beschreibt die Installation und den Betrieb der Software a.sign Client unter Windows Betriebssystemen. Eine Haftung der a.trust für Schäden und Folgen bei Verwendung dieser Software ist ausgeschlossen.

1.2.3 a.sign Client – wozu?

Die Software a.sign Client stellt die Verbindung zwischen Ihrer a.trust Signaturkarte und Standardapplikationsprogrammen her. Der a.sign Client wurde von a.trust für Applikationsprogramme konzipiert, die kryptografische Funktionen wie Signatur und Verschlüsselung entweder über einen sog. „CSP“ (Cryptographic Service Provider) oder über die standardisierte „PKCS#11“ Schnittstelle realisieren. Das sind zum Beispiel:

- Microsoft ® Internet Explorer / Outlook Express ab Version 5.x
- Microsoft ® Outlook 2000, 2002 (XP) und 2003
- Microsoft ® Office XP und 2003
- Netscape ® Navigator / Communicator Version 7.x
- Mozilla Browser / Mail Client ab Version 1.2
- Mozilla Firefox ® / Thunderbird
- Open Office 1.x und 2.x
- Adobe ® Acrobat ab Version 6

Eine Auflistung aller Applikationsprogramme sowie Anleitungen zur Konfiguration finden Sie auf der a.trust Homepage im Support-Bereich (<http://www.a-trust.at> – Privat (bzw. Business) – Support – Zertifikate nutzen – a.sign Client Anleitungen):



1.2.4 Was kann der a.sign Client?

Der a.sign Client kann mit Hilfe der a.trust Signaturkarte und einem angeschlossenen Kartenlesegerät die Basis für Anwendungen bieten, um

- einfache Signaturen mit dem Geheimhaltungsschlüssel / -zertifikat der Karte zu erstellen, beispielsweise in Verbindung mit E-Mails oder Office Dokumenten
- Ver- und Entschlüsselungen durchzuführen, beispielsweise in Verbindung mit E-Mail-Programmen
- sichere Verbindungen im Internet („SSL“) auf Basis des Geheimhaltungszertifikates zu unterstützen

Der a.sign Client kann **keine** sicheren Signaturen nach Signaturgesetz erzeugen. Dazu benötigt man eigene Software mit einem sog. „Secure Viewer“.

Lesen Sie alles Weitere über die Funktionen des a.sign Client im Kapitel 1.13 – Funktionen des a.sign Client Administrationsprogramm

1.3 Voraussetzungen

Bitte beachten Sie, dass eine Installation der Software a.sign Client nur bei angeschlossenem Kartenlesegerät sowie einem korrekt installierten Kartenleser-Treiber möglich ist. Andernfalls bricht die Installation ab (siehe auch 1.8 – Mögliche Fehlermeldungen). Beachten Sie bitte auch die unterstützten Betriebssysteme (1.3) sowie die von a.trust empfohlenen Kartenlesegeräte (siehe 1.4 – Empfohlene Kartenlesegeräte).

1.3.3 Unterstützte Betriebssysteme

Die Installation der Software a.sign Client ist unter folgenden Betriebssystemen möglich:

Windows 98 *

Windows 98 2nd Edition *

Windows NT 4 mit Service Pack 4 oder höher *

Windows Millenium Edition *

Windows 2000 (Service Pack 4 empfohlen)

Windows XP (Service Pack 2 empfohlen)

* Wir bitten Sie um Kenntnisnahme, dass Microsoft für diese Betriebssysteme den Support eingestellt hat. Eine Installation und Benutzung der Software a.sign Client unter diesen Betriebssystemen erfolgt daher auf eigene Gefahr.

1.3.4 Empfohlene Kartenlesegeräte

Anbei eine Auflistung aller von a.trust empfohlenen Kartenlesegeräte (Stand Aug. 2006):

	<p>Cherry Smartboards</p> <p>Empfohlen werden die Modelle G83-6744LUZxx (USB), G83-6700LQZxx/01 (serielle Schnittstelle), G83-6744LBZxx (nicht mehr lieferbar), G81-8015LQZxx/01 (nicht mehr lieferbar), G81-12000LTZxx/01 (nicht mehr lieferbar)</p>
	<p>KOBIL KAA Professional</p> <p>Bitte beachten Sie, dass nur KOBIL KAA Professional der Firmware-Version 2.08 unterstützt werden. Geben Sie daher bei der Bestellung des Gerätes diese Versionsnummer an.</p>
	<p>Reiner SCT cyberJack® pinpad</p> <p>Bitte beachten Sie, dass nur Reiner SCT cyberJack® pinpad der Firmware-Version 2.0 oder 3.0 unterstützt werden. Geben Sie daher bei der Bestellung des Gerätes die Versionsnummer 3.0 an.</p>
	<p>Reiner SCT cyberJack® e-com</p> <p>Bitte beachten Sie, dass nur Reiner SCT cyberJack® e-com der Firmware-Version 2.0 unterstützt werden. Geben Sie daher bei der Bestellung des Gerätes diese Versionsnummer an.</p>
	<p>Towitoko CHIPDRIVE® pinpad / SCM Microsystems SPR532</p> <p>Bitte beachten Sie, dass nur CHIPDRIVE® pinpad der Firmware-Version 4.15 unterstützt werden. Geben Sie daher bei der Bestellung des Gerätes diese Versionsnummer an.</p>
	<p>Omnikey CardMan Trust 3621/3821</p> <p>Bitte beachten Sie, dass nur Omnikey CardMan der Firmware-Version 6.00 unterstützt werden, da nur diese Version für die sichere Signatur zertifiziert ist. Geben Sie daher bei der Bestellung des Gerätes diese Versionsnummer an.</p>

Der a.sign Client unterstützt sowohl Kartenlesegeräte die den CT-API-Standard als auch den PC/SC-Standard verwenden. Damit können praktisch alle gebräuchlichen bzw. handelsüblichen Kartenlesegeräte mit dem a.sign Client verwendet werden.

Beachten Sie bitte nur, dass für die sichere PIN-Eingabe (Eingabe der PIN direkt am Kartenleser) der CT-API-Treiber zu Ihrem Kartenlesegerät installiert sein muss (dieser befindet sich üblicherweise auf der mitgelieferten Hersteller-CD). Wird lediglich der PC/SC-Treiber installiert, erfolgt die PIN-Eingabe über die Tastatur Ihres PCs bzw. Ihres Notebooks.

Beachten Sie bitte auch, dass Sie für die sichere Signatur zwingend ein Kartenlesegerät mit eigenem Pinpad (Tastaturfeld) benötigen.

1.4 Installation des a.sign Client

1.4.3 Voraussetzungen unter Windows 98/98SE/NT/ME

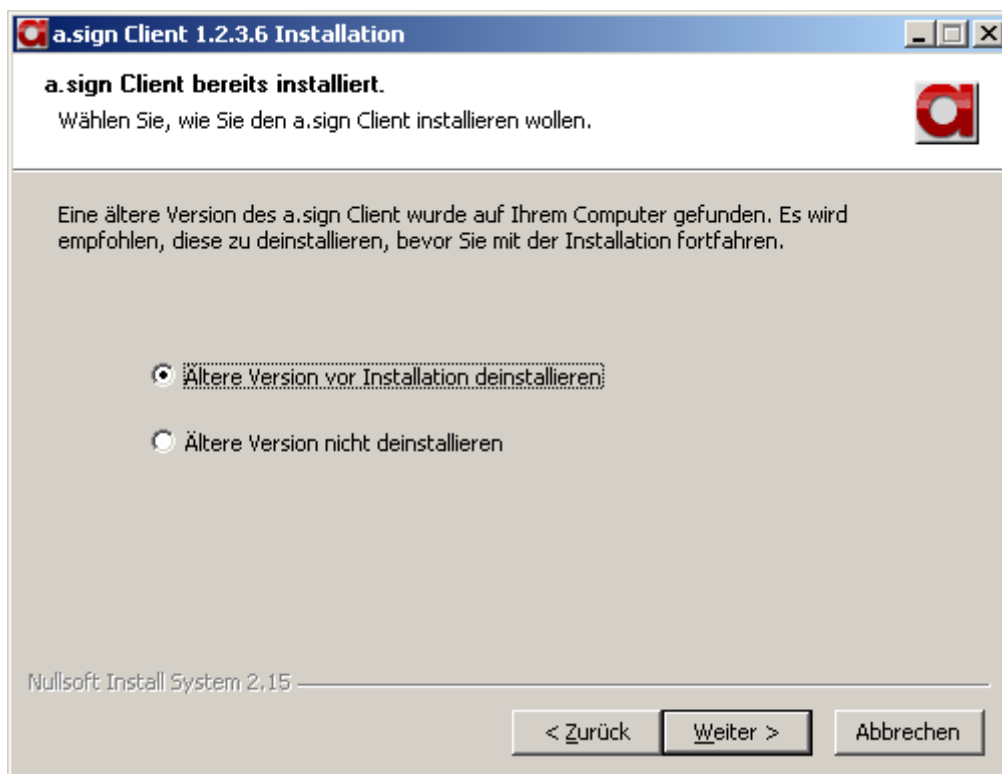
Da die Betriebssysteme Windows 98, Windows 98 2nd Edition, Windows NT 4 sowie Windows Millennium Edition noch nicht über die nötigen Komponenten zum Smartcard-Zugriff verfügen, werden die sog. Microsoft Smart Card Base Components benötigt. Diese können Sie über unsere Homepage beziehen:

<http://www.a-trust.at/downloads/SCBase.zip>

WICHTIG: Die Microsoft Smart Card Base Components müssen vor Installation des a.sign Client auf den genannten Betriebssystemen installiert sein. Auf anderen Betriebssystemen dürfen die Components nicht installiert werden!

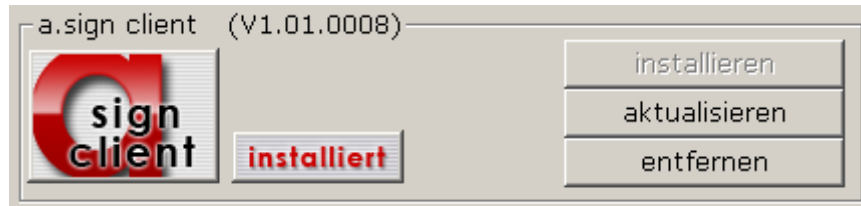
1.4.4 Update einer älteren a.sign Client Installation

Haben Sie eine ältere Version des a.sign Client installiert, so kann diese im Zuge der Installation der neuen Version deinstalliert werden:

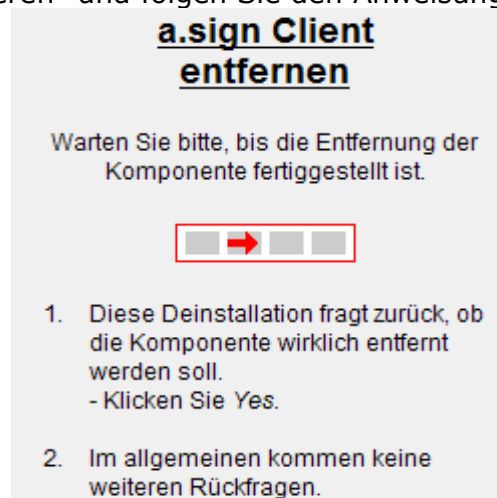


Wenn Sie den a.sign Installer verwenden, wird Ihnen die aktuell installierte Version des a.sign Client angezeigt. Sie haben hier nun die Möglichkeit, diese Version zu deinstallieren

oder auf die online aktuellste Version zu aktualisieren:

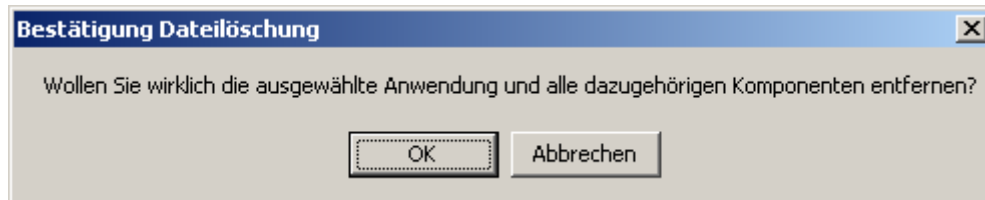


Wählen Sie bitte „aktualisieren“ und folgen Sie den Anweisungen auf Ihrem Bildschirm:



Es startet nun der (De-) Installations-Assistent. Wählen Sie hier bitte „Entfernen“ und klicken Sie auf „Weiter“:

Bestätigen Sie die darauf folgende Meldung mit OK:

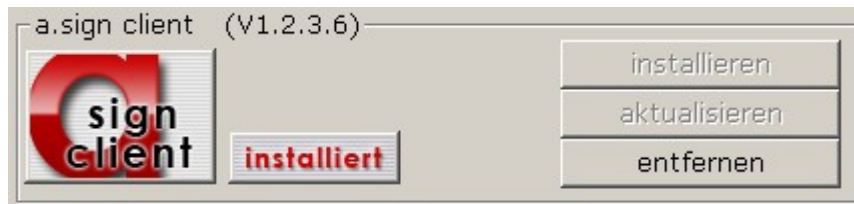


Klicken Sie nun auf „Fertig Stellen“. Es wird nun die aktuellste online verfügbare Version des a.sign Clients heruntergeladen:



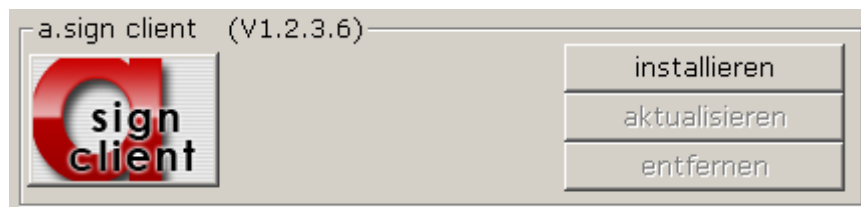
Sobald die Komponente vollständig heruntergeladen wurde, startet der Installations-Assistent automatisch. Bitte folgen Sie hier den Anweisungen auf Ihrem Bildschirm (siehe auch 1.8 – Manuelle Installation des a.sign Client).

Nach Fertigstellung der Installation zeigt Ihnen der a.sign Installer die erfolgreich installierte aktuelle Version des a.sign Client an:



1.4.5 Installation des a.sign Client über den a.sign Installer

Starten Sie den a.sign Installer und wechseln Sie zur Registerkarte „a.sign Client“. Hier wird Ihnen angezeigt, welche Version zur Installation zur Verfügung steht:



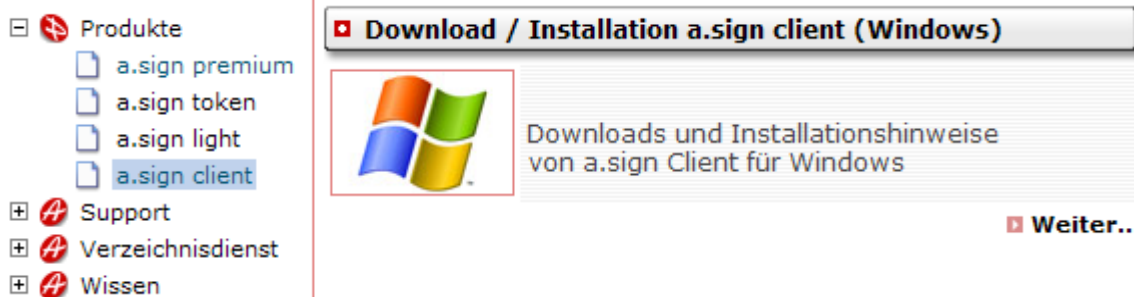
Mit einem Klick auf „installieren“ wird die angezeigte Version heruntergeladen:



Sobald die Komponente vollständig heruntergeladen wurde, startet der Installations-Assistent automatisch. Bitte folgen Sie hier den Anweisungen auf Ihrem Bildschirm (siehe auch 1.8 – Manuelle Installation des a.sign Client).

1.4.6 Manuelle Installation des a.sign Client

Wenn Sie den a.sign Client nicht automatisch über den a.sign Installer installieren wollen, können Sie ihn auch manuell von unserer Homepage herunterladen. Den Download finden Sie im linken Menübereich unter Produkte – a.sign client (egal, ob Sie sich im Privat, Business oder Partner-Bereich befinden):



The screenshot shows a website navigation menu on the left with categories: Produkte (a.sign premium, a.sign token, a.sign light, a.sign client), Support, Verzeichnisdienst, and Wissen. On the right, a button labeled 'Download / Installation a.sign client (Windows)' is highlighted. Below the button is a Windows logo and the text 'Downloads und Installationshinweise von a.sign Client für Windows'. A 'Weiter..' button is located at the bottom right of the highlighted area.

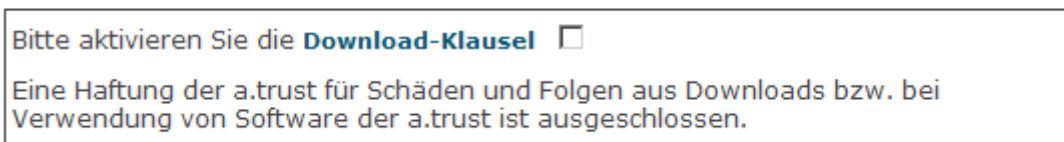
Klicken Sie bitte bei „Download / Installation a.sign Client (Windows) auf „Weiter“



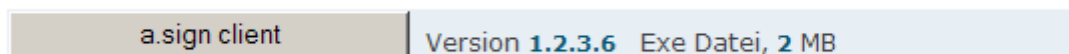
The screenshot shows a page titled '2. Schritt: Installation a.sign client'. The text reads: 'Installieren Sie den **a.sign client**, um Ihr Zertifikat in Standardapplikationen wie Outlook, Internet Explorer und Office nutzen zu können. Bitte beachten Sie, dass diese Standardapplikationen mit Ihrem **Geheimhaltungszertifikat** arbeiten, da nur einfache Signaturen erstellt werden.' Below this is a link: 'Installation der Software a.sign client'.

Klicken Sie nun auf „Installation der Software a.sign Client“

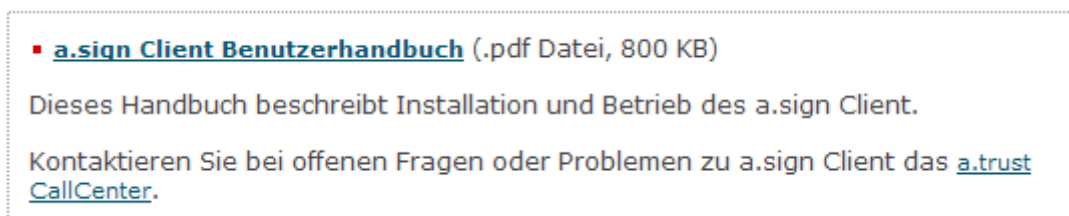
a sign Client - Download



The screenshot shows a section with the text: 'Bitte aktivieren Sie die **Download-Klausel** Eine Haftung der a.trust für Schäden und Folgen aus Downloads bzw. bei Verwendung von Software der a.trust ist ausgeschlossen.'



The screenshot shows a button labeled 'a.sign client' and the text 'Version 1.2.3.6 Exe Datei, 2 MB'.

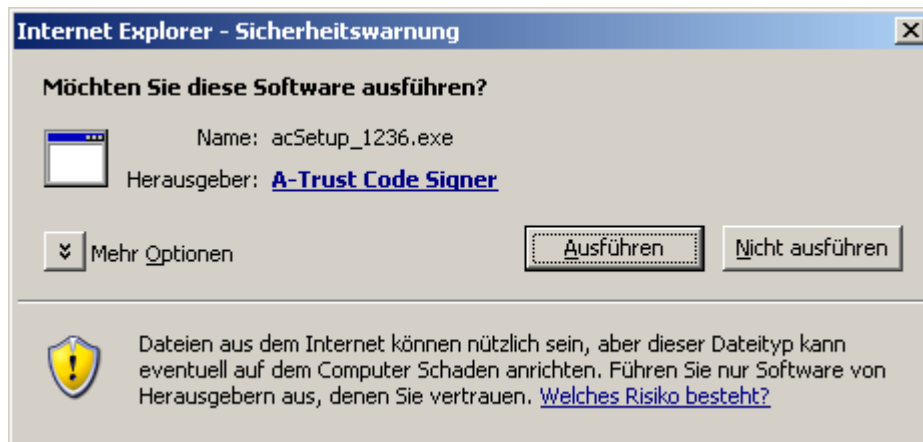


The screenshot shows a link: 'a.sign Client Benutzerhandbuch (.pdf Datei, 800 KB)'. Below it is the text: 'Dieses Handbuch beschreibt Installation und Betrieb des a.sign Client. Kontaktieren Sie bei offenen Fragen oder Problemen zu a.sign Client das [a.trust CallCenter](#).'

Aktivieren Sie hier die Download-Klausel und klicken Sie auf den Button „a.sign client“, um den Download zu starten.



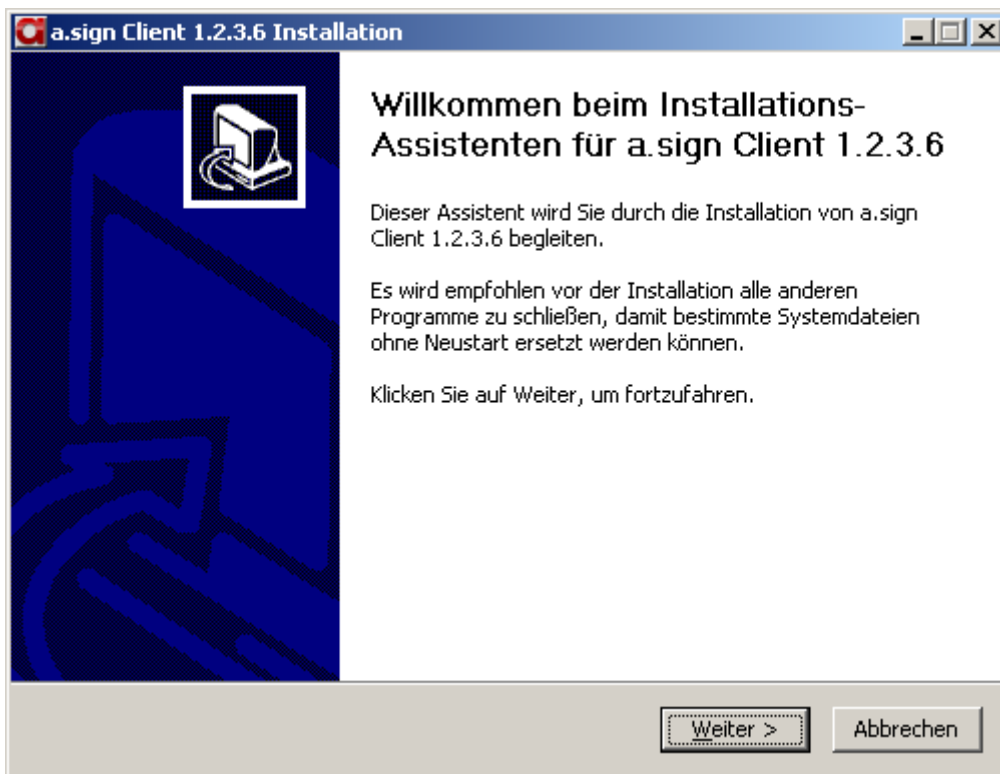
Wählen Sie „Ausführen“, um die Installation automatisch nach Beendigung des Downloads zu starten, oder „Speichern“, um die heruntergeladene Datei manuell zu starten.



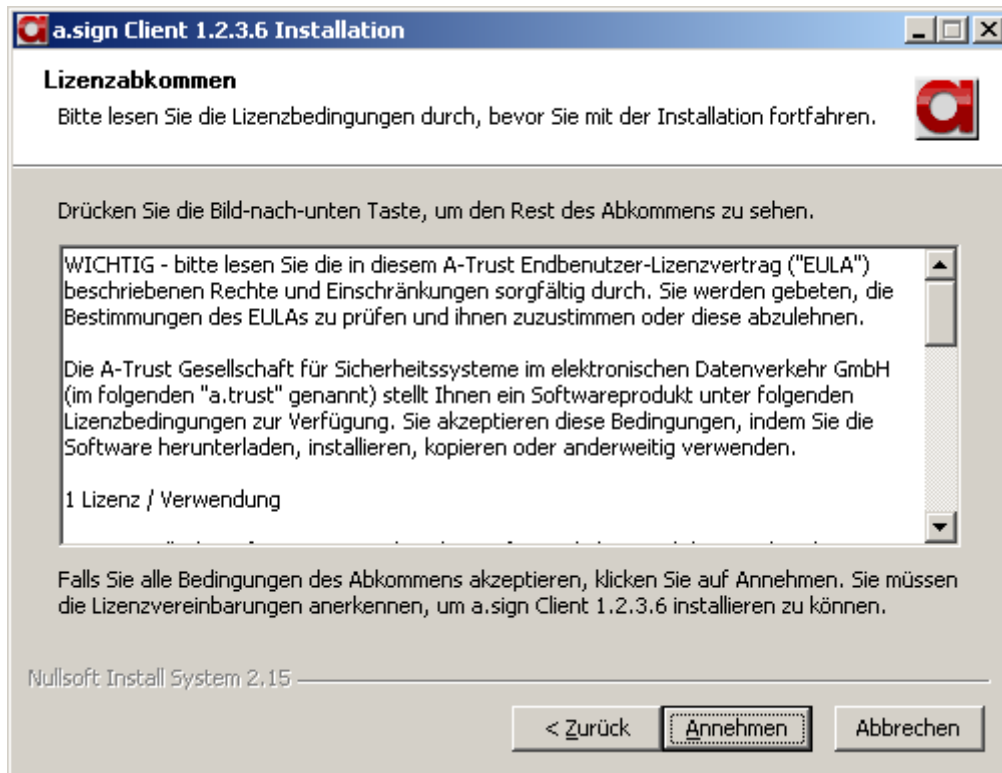
Bitte bestätigen Sie diese Sicherheitswarnung durch einen Klick auf „Ausführen“ (bzw. überprüfen Sie den Herausgeber durch einen Klick auf „A-Trust Code Signer“).



Wählen Sie die Installationssprache und bestätigen Sie mit "OK". Es startet nun der Installations-Assistent.



Klicken Sie hier bitte auf „Weiter“.



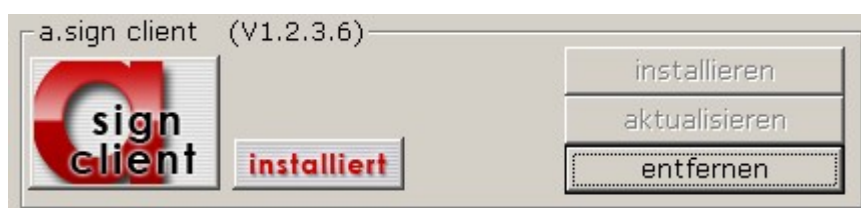
Akzeptieren Sie bitte das Lizenzabkommen durch einen Klick auf „Annehmen“:



Beenden Sie die Installation durch „Fertig stellen“

1.4.7 a.sign Client deinstallieren

Sie können den a.sign Client über „Start – Programme (bzw. Alle Programme) – A-Trust GmbH – a.sign Client – Uninstall“ deinstallieren. Oder Sie starten den a.sign Installer und klicken im a.sign Client Reiter auf „entfernen“:



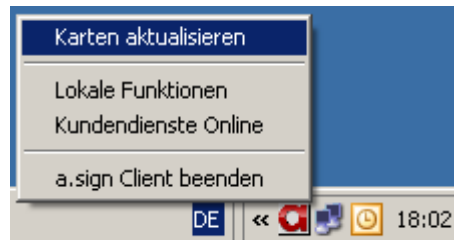
1.5 Ich habe den a.sign Client installiert – was nun?

Der a.sign Client macht sich durch ein rotes a-Logo in der Taskleiste bemerkbar:



Der a.sign Client ermöglicht den Applikationsprogrammen den Zugriff auf Ihre a.trust Signaturkarte und das darauf befindliche Geheimhaltungszertifikat.

Nach erfolgreicher Installation sollte sich Ihr Geheimhaltungszertifikat im Windows Zertifikatsspeicher befinden. Dies können Sie überprüfen, indem Sie im Internet Explorer unter „Extras – Internetoptionen – Inhalte – Zertifikate“ einsteigen. Unter „Eigene Zertifikate“ sollte Ihr Geheimhaltungszertifikat aufscheinen. Wenn nicht, führen Sie bitte einmal die Funktion „Karten aktualisieren“ bei eingelegter Karte durch:



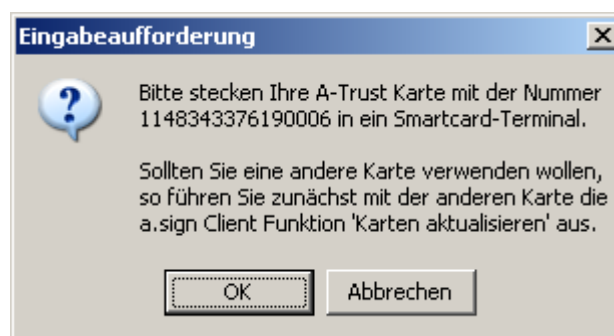
Für die Dauer des Aktualisierungsvorganges wird statt dem a-Logo eine drehende Smartcard angezeigt:



Sobald das a-Logo wieder sichtbar ist, überprüfen Sie bitte erneut im Windows Zertifikatsspeicher, ob nun Ihr Geheimhaltungszertifikat aufscheint.

Hinweis: Das Zertifikat verbleibt auch dann im Windows Zertifikatsspeicher, wenn die Karte aus dem Kartenlesegerät entfernt wird.

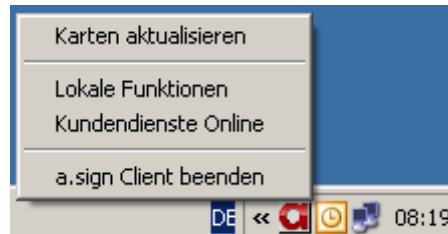
Wenn ein Applikationsprogramm auf das Zertifikat zugreifen will, während sich keine oder eine andere a.trust Signaturkarte im Kartenlesegerät befindet, zeigt der a.sign Client eine Aufforderung zum Einlegen der zuletzt aktualisierten Karte an:



Wählen Sie in diesem Fall „Abbrechen“, führen Sie die Funktion „Karten aktualisieren“ durch und starten Sie den Versuch erneut.

1.6 Funktionen des a.sign Client Administrationsprogramms

Die Funktionen des a.sign Client Administrationsprogramms werden durch einen **Rechtsklick** auf das a-Logo abgerufen:



Hinweis: Greift eine Applikation auf den a.sign Client bzw. den Kartenleser zu, wird das a-Logo grau dargestellt:

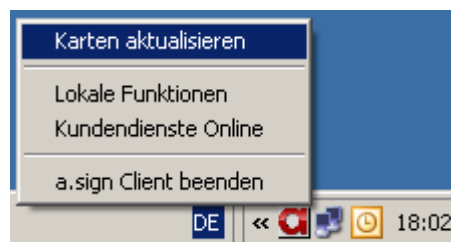


Währenddessen ist ein Anwählen der Funktionen nicht möglich.

1.6.3 Karten aktualisieren

Siehe auch 1.12 – Ich habe den a.sign Client installiert – was nun?

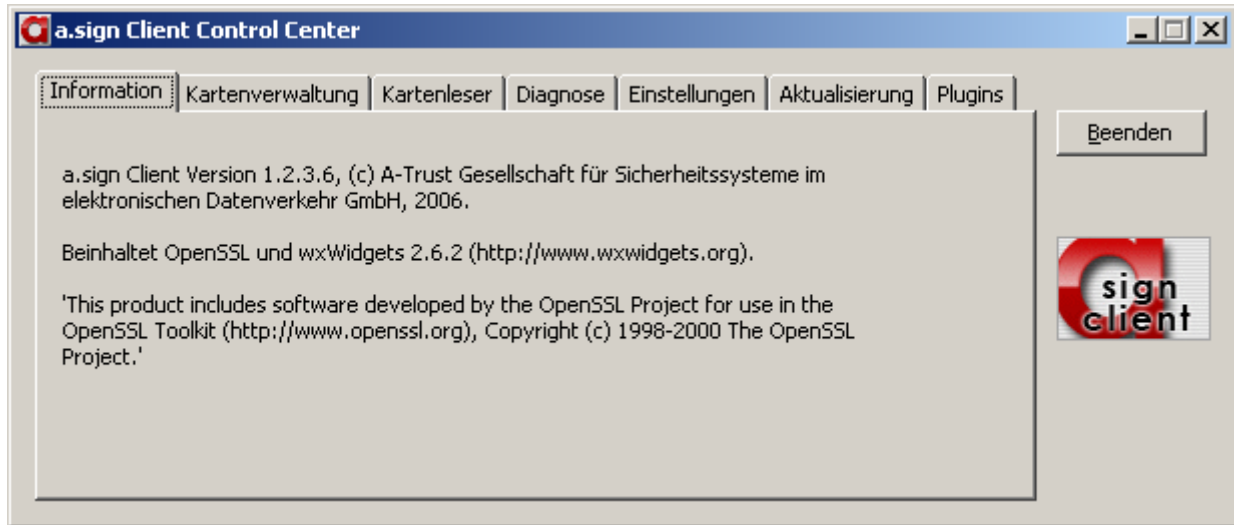
Führen Sie die Funktion „Karten aktualisieren“ aus, um Ihr Geheimhaltungszertifikat auf der a.trust Signaturkarte in den Windows Zertifikatsspeicher zu transportieren. Den gleichen Effekt erzielen Sie übrigens auch, wenn Sie den a.sign Client mit der linken Maustaste doppelklicken.



Wenn Sie mehrere Karten auf einem System verwenden, führen Sie bitte jedes Mal diese Funktion aus, sobald Sie die eingelegte Signaturkarte durch eine andere ersetzen.

1.6.4 Lokale Funktionen

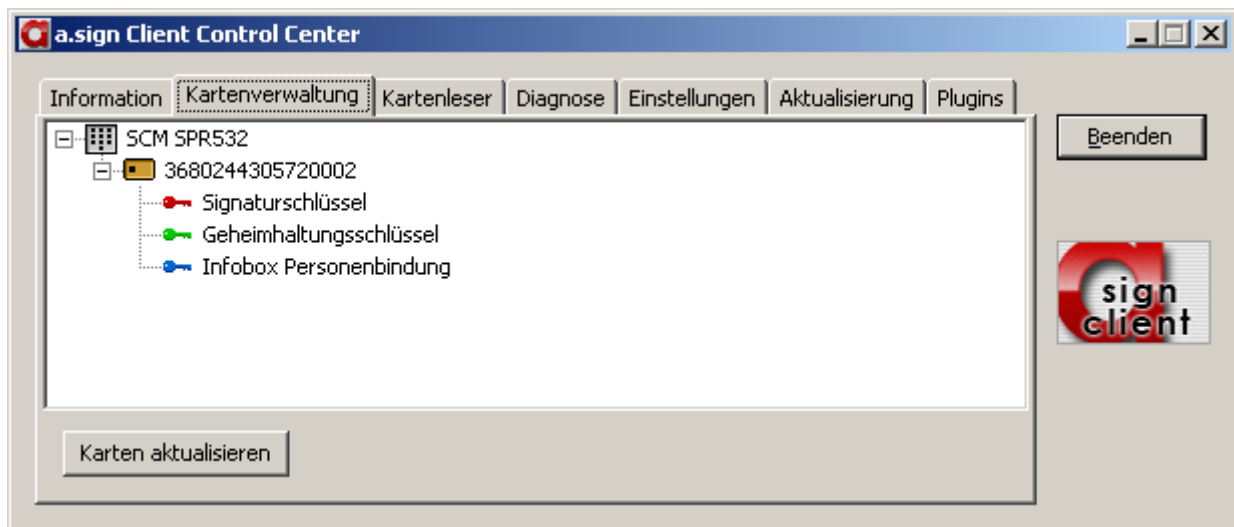
Die Lokalen Funktionen sind das Herzstück des a.sign Client Administrationsprogramms. Die Funktionen gliedern sich in 7 Registerkarten auf:



Über den Button „Beenden“ können Sie das a.sign Client Control Center schließen.

1.6.4.4 Kartenverwaltung

In der Kartenverwaltung wird Ihnen – sofern Ihr Kartenlesegerät korrekt angeschlossen, der Treiber installiert und die a.trust Signaturkarte eingelegt ist – folgender Inhalt angezeigt:



In der obersten Zeile wird Ihr Kartenlesegerät angezeigt – in diesem Fall ein SCM SPR532 (Chipdrive Pinpad pro).

In der zweiten Zeile wird Ihre a.trust Signaturkarte in Form der 16-stelligen Signaturvertragsnummer (auch als CIN – Cardholder Identification Number – bekannt) angezeigt.

In den weiteren Zeilen werden die wichtigsten auf der Karte befindlichen Daten angezeigt

(diese können je nach Produkt variieren):

- Signaturschlüssel
- Geheimhaltungsschlüssel
- Infobox Personenbindung

Die Infobox Personenbindung befindet sich auf Signaturkarten, auf denen ein **a.sign premium** Zertifikat aktiviert wurde – z.B. a.sign premium Bestellkarte, maestro-Karte (Bankomatkarte) oder Mastercard.

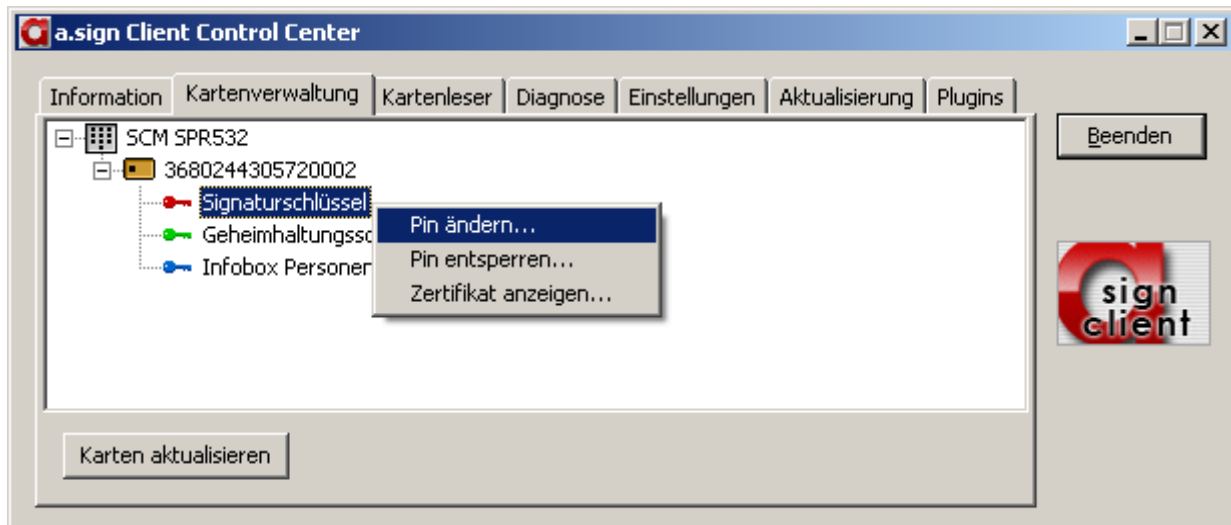
Mit einem Rechtsklick auf eine der 3 Elemente können die dazugehörigen Funktionen aktiviert werden:

- Pin ändern
- Pin entsperren
- Zertifikat anzeigen
- Personenbindung anzeigen
- Pin hinterlegen

Hinweis: Zertifikate (Geheimhaltungs- bzw. Signaturschlüssel) oder Personenbindung lassen sich auch durch einen Doppelklick anzeigen.

1.6.4.5 Pin ändern

Diese Funktion kann durch einen Rechtsklick auf den entsprechenden Schlüssel bzw. auf die Infobox Personenbindung angewählt werden:



Hinweis: Bei bestimmten Karten (z.B. a.sign token) kann die Pin zu Ihrem Geheimhaltungsschlüssel nicht geändert werden. Sie erkennen dies daran, dass die Funktion „Pin ändern“ nicht zur Verfügung steht.

Nachdem Sie die Funktion angewählt haben, erscheint je nachdem, ob der Leser eine sichere Pin-Eingabe unterstützt (Typ CT-API) oder nicht (Typ PC/SC), die Aufforderung zur Änderung der Pin direkt am Pinpad des Kartenlesegeräts oder am Bildschirm (in diesem Fall muss die Pin über Ihre PC-/Notebook-Tastatur eingegeben werden).

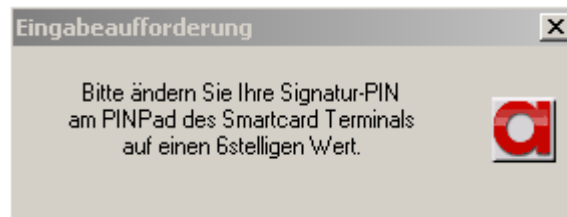
Während diesem Vorgang werden Sie zunächst nach der aktuellen, „alten“ Pin gefragt. Anschließend müssen Sie 2 Mal Ihre neue gewünschte Pin eingeben. 2 Mal deswegen, um die unbeabsichtigte Änderung auf einen ungewollten Wert zu vermeiden.

Eingabeaufforderung des a.sign Client bei Verwendung eines Kartenlesegeräts vom Typ PC/SC bzw. bei verwendetem PC/SC-Treiber:



Eingabeaufforderung des a.sign Client bei Verwendung eines Kartenlesegeräts vom Typ

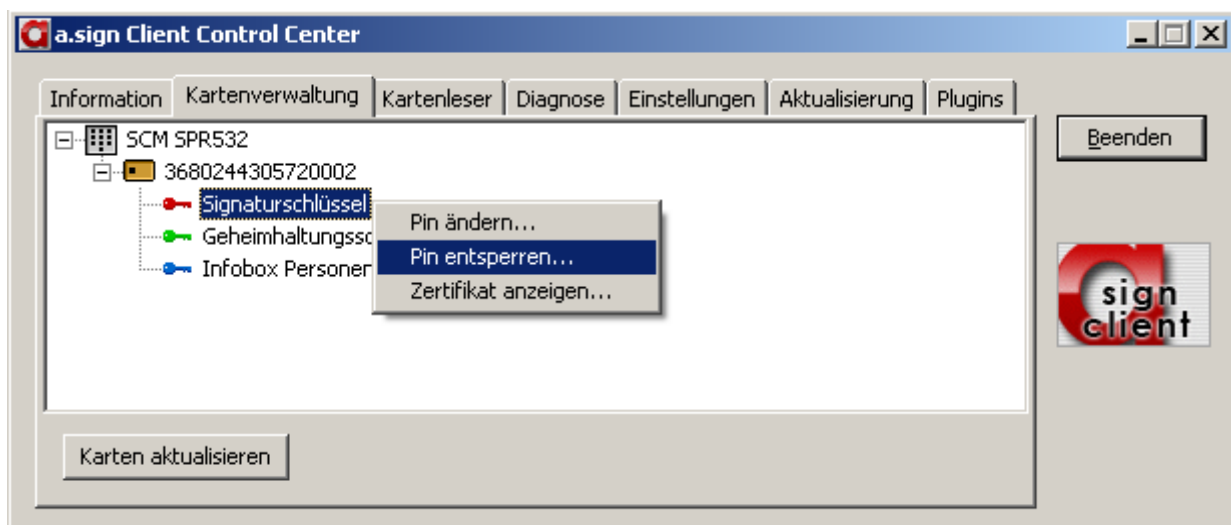
CT-API mit eigenem Pinpad:



Hinweis: Die Geheimhaltungs-Pin sowie die Infobox-Pin können jeweils nur auf einen 4-stelligen Wert geändert werden, die Signatur-Pin nur auf einen 6-stelligen Wert.

1.6.4.6 Pin entsperren

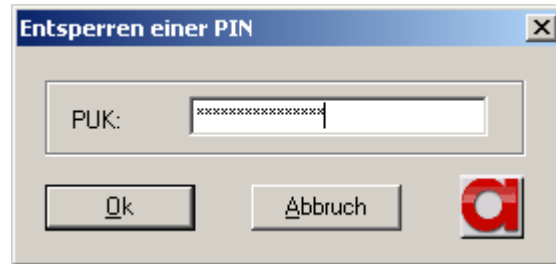
Ist eine Pin gesperrt (durch zu viele aufeinanderfolgende Fehleingaben) können Sie diese mittels PUK (Personal Unblocking Key) entsperren. Diese Funktion kann durch einen Rechtsklick auf den entsprechenden Schlüssel bzw. auf die Infobox-Personenbindung angewählt werden:



Hinweis: Bei bestimmten Karten (z.B. a.sign premium 3 Jahre) kann die Pin zu Ihrem Signaturschlüssel nicht entsperret werden. Sie erkennen dies daran, dass die Funktion „Pin entsperren“ nicht zur Verfügung steht.

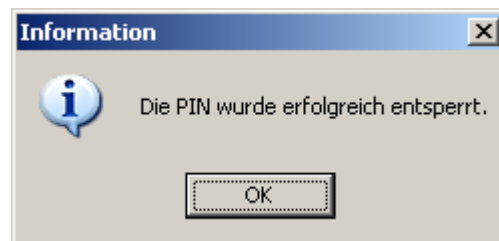
Um eine Pin entsperren zu können, benötigen Sie den dazugehörigen PUK (das heißt: Zur 4-stelligen Geheimhaltungs-Pin gehört der 16-stellige Geheimhaltungs-PUK etc.). Diesen können Sie über die a.sign Client Funktion „Kundendienste Online“ bestellen (siehe auch ...).

Sie erhalten nun die Eingabeaufforderung des jeweiligen PUK vom a.sign Client:



Bitte geben Sie den 16-stelligen PUK über die Tastatur Ihres Pcs/Laptops ein und bestätigen Sie anschließend mit „Ok“.

Sie erhalten nun eine positive Rückmeldung:



Bei manchen Karten (z.B. a.sign premium 3 Jahre) bekommen Sie beim Entsperren der Geheimhaltungs-Pin folgende Eingabemaske:



In diesem Fall müssen Sie nicht nur den 16-stelligen Geheimhaltungs-PUK eingeben, sondern können auch gleich über die Eingabefelder „PIN“ und „Bestätigen der PIN“ eine neue Geheimhaltungs-PIN vergeben.

Hinweis: Je nach Karte wird eine Pin nach 3 (z.B. bei a.sign premium 3 Jahre, a.sign to-

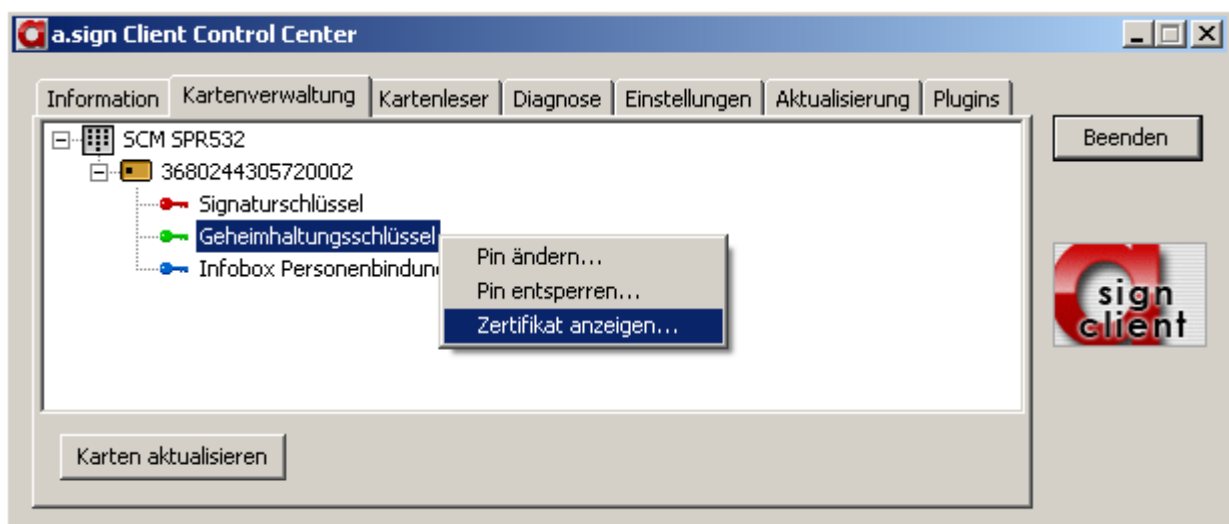
ken)) bzw. 10 (a.sign premium 5 Jahre bzw. a.sign premium auf maestro- oder Mastercard) aufeinander folgenden Fehleingaben gesperrt.

Beachten Sie bitte auch, dass ein PUK nicht beliebig oft verwendet werden kann. In Folge darf die Deblockierung mittels PUK nur 3 Mal durchgeführt werden. Erfolgt nach 3-maligem Deblockieren keine korrekt PIN-Eingabe, ist die Karte für immer blockiert.

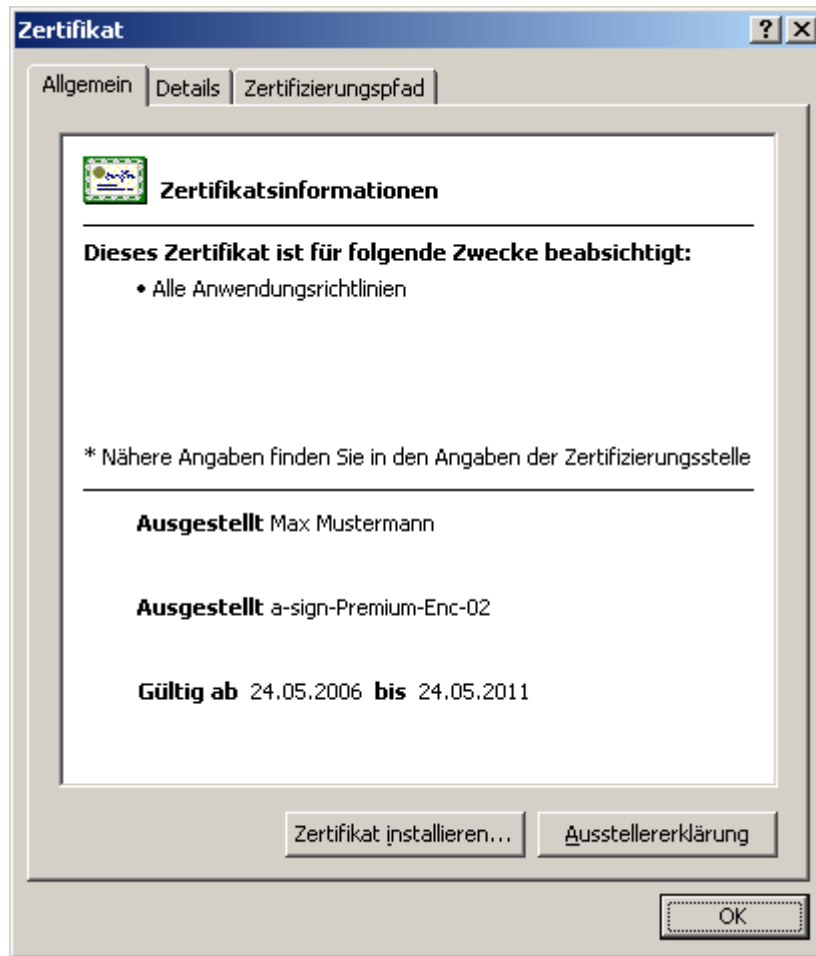
Sie können die PUKs über die a.sign Client Zusatzfunktion „**Kundendienste Online**“ ordern (siehe 1.6.5.8 – PUK Dienst)

1.6.4.7 Zertifikat anzeigen

Diese Funktion kann durch einen Rechtsklick auf den entsprechenden Schlüssel angewählt werden:



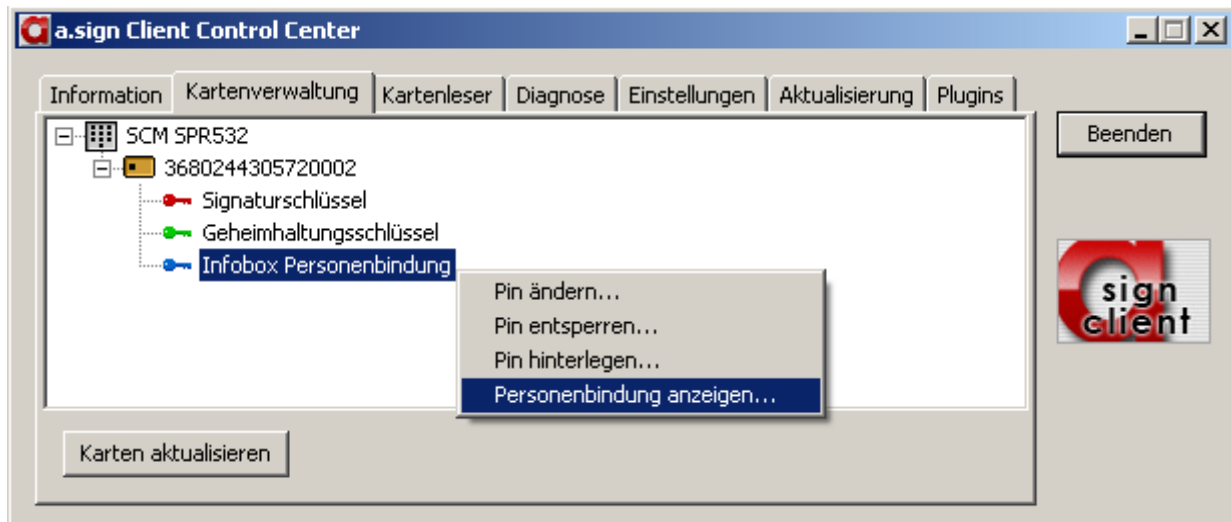
Nach Anwahl dieser Funktion wird das Zertifikat im Windows-eigenen Zertifikats-Viewer dargestellt:



Hinweis: Auf diese Art und Weise können Sie die Gültigkeit sowie den Inhalt Ihrer Zertifikate überprüfen. Sind zum Beispiel die a.trust Stammzertifikate nicht installiert oder ist Ihr Zertifikat abgelaufen, so wird in dieser Maske ein Warnhinweis angezeigt.

1.6.4.8 Personenbindung anzeigen

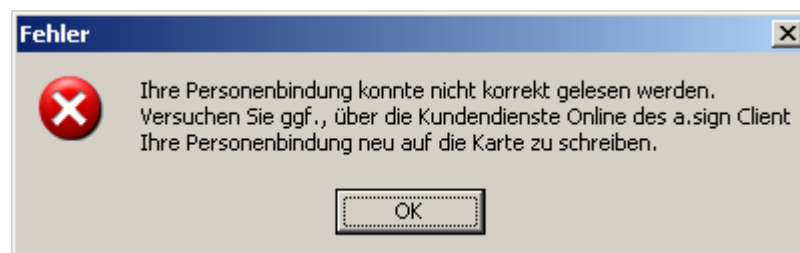
Diese Funktion kann durch einen Rechtsklick auf die Infobox Personenbindung angewählt werden:



Wenn Sie die Personenbindung bereits erfolgreich auf die Karte geschrieben (siehe auch ...) haben, werden Ihnen Vorname, Nachname, Geburtsdatum sowie Stammzahl (geschützt) angezeigt:



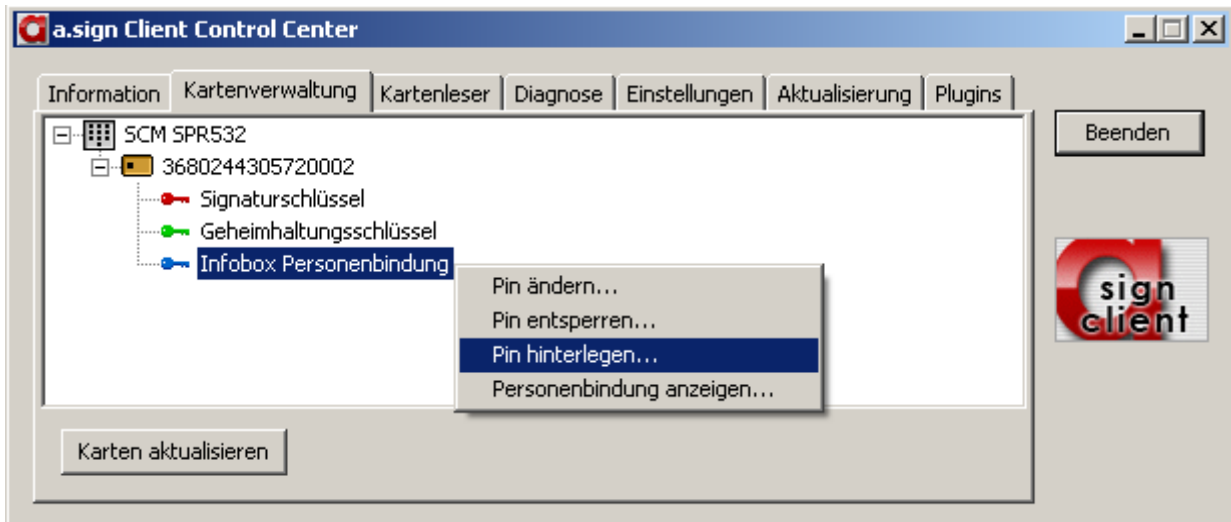
Sollte sich Ihre Personenbindung noch nicht auf Ihrer a.trust Signaturkarte befinden, erhalten Sie folgende Rückmeldung:



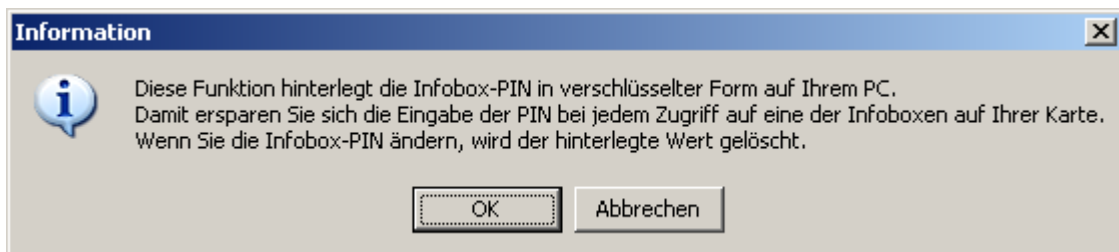
In diesem Fall starten Sie bitte über die a.sign Client Funktion „Kundendienste Online“ das ZMR-Service (siehe auch ...)

1.6.4.9 Pin hinterlegen

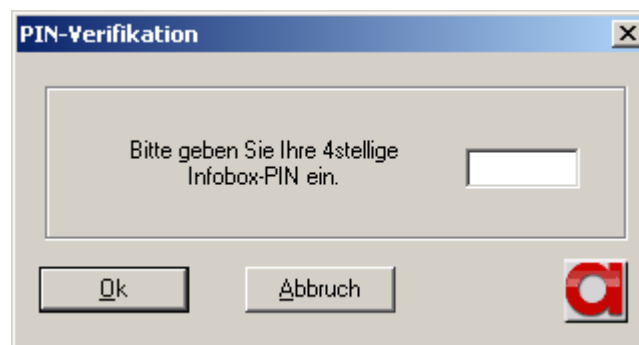
Diese Funktion steht Ihnen nur bei der Infobox-Pin zur Verfügung und kann durch einen Rechtsklick auf die Infobox Personenbindung angewählt werden:



Sie erhalten zuerst folgende Information:



Bestätigen Sie mit OK. Sie erhalten nun eine Eingabemaske – geben Sie hier bitte Ihre Infobox-PIN (0000 - sofern Sie nicht geändert wurde) über die Tastatur Ihres Pcs/Laptops ein und bestätigen Sie mit „Ok“:



Sie erhalten nun die Rückmeldung:



Diese Funktion dient dazu, Ihre Infobox-Pin in verschlüsselter Form in Ihrem System zu hinterlegen. Das ist dann sinnvoll, wenn Sie Ihre Infobox-Pin von Ihrem Standard-Wert (0000) geändert haben. In diesem Fall wird für jeden Zugriff auf die Infobox (auch zum Feststellen, ob sich überhaupt ein Infobox auf der Karte befindet) die Infobox-Pin verlangt. Um die regelmäßigen Pin-Eingaben zu vermeiden, können Sie Ihre Pin am PC hinterlegen.

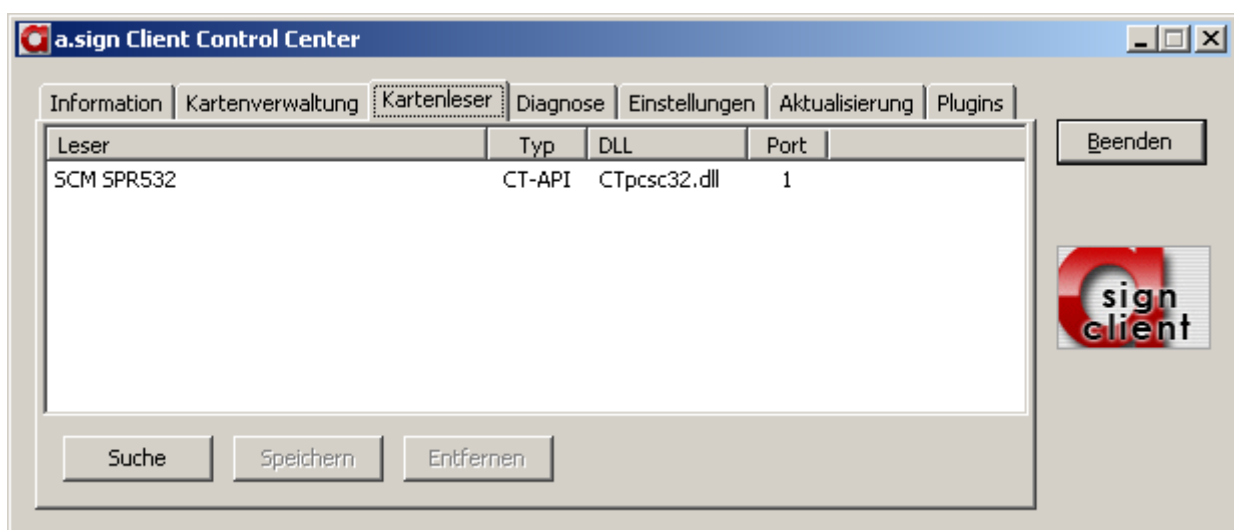
Sie können die hinterlegte Infobox-Pin jederzeit wieder löschen, indem Sie Ihre Infobox-Pin ändern.

Hinweis: Die Funktion „Pin hinterlegen“ bei Ihrer Infobox Personenbindung steht Ihnen nur dann zur Verfügung, wenn Ihre Karte über eine Personenbindung und eine eigene Infobox-Pin verfügt. Dies ist bei allen a.sign premium Karten (nzw. Bei a.sign premium auf der maestro- oder Mastercard) gegeben.

1.6.4.10 Kartenleser

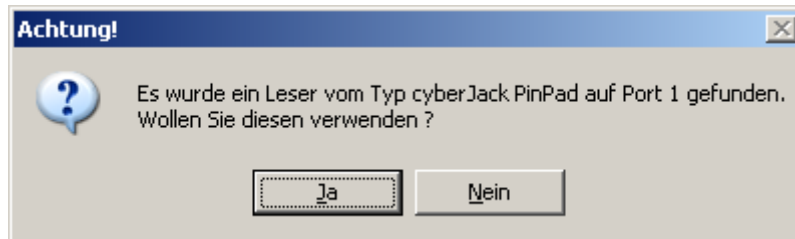
Hier werden Ihnen alle Kartenlesegeräte angezeigt, die während der a.sign Client Installation an Ihrem PC/Laptop angeschlossen und korrekt installiert waren.

Hinweis: Der a.sign Client unterstützt bis zu 8 angeschlossene Kartenlesegeräte vom Typ CT-API und PC/SC.

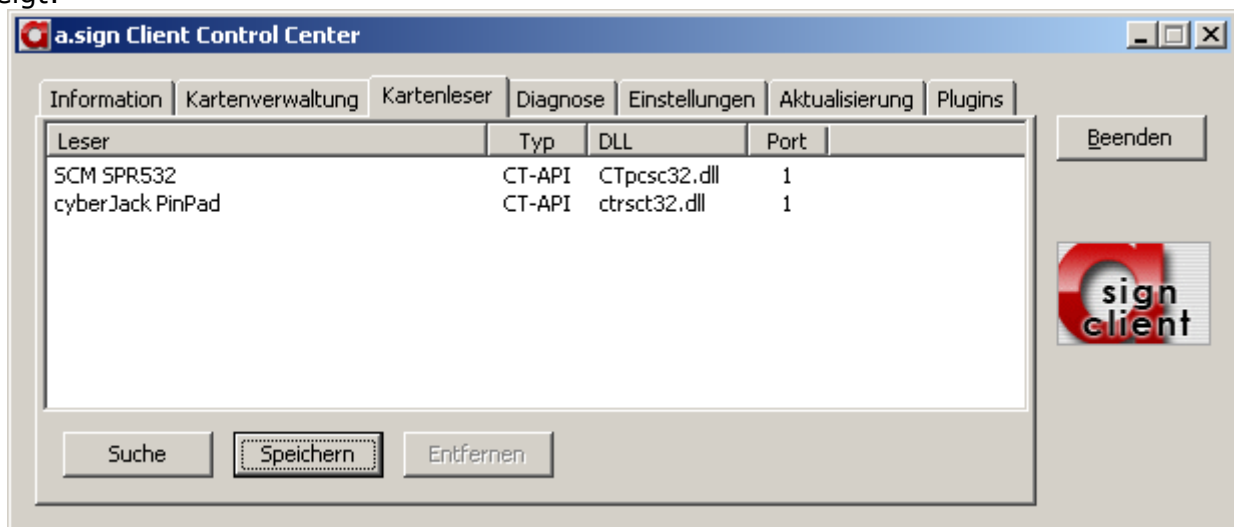


In diesem Fall ist ein SCM SPR532 (Chipdrive Pinpad pro) vom Typ CT-API installiert.

Sollten Sie nach Installation des a.sign Client einen neuen Treiber bzw. ein neues Kartenlesegerät angeschlossen und installiert haben, können Sie dieses über den „Suche“-Button hinzufügen:



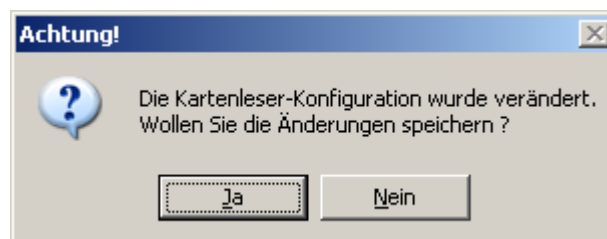
In diesem Fall wurde zusätzlich ein Reiner SCT PinPad angeschlossen und installiert. Bestätigen Sie diese Meldung mit „Ja“. Es wird nun zusätzlich der Reiner SCT PinPad angezeigt:



Klicken Sie abschließend auf „Speichern“, um die neue Konfiguration zu übernehmen.

Sie können natürlich auch ein Kartenlesegerät aus der a.sign Client Konfiguration entfernen. Markieren Sie einfach das gewünschte Gerät und klicken Sie auf „Entfernen“. Speichern Sie die neue Konfiguration abschließend bitte wieder ab.

Sollten Sie ohne zu speichern in eine andere Registerkarte des a.sign Client wechseln oder den a.sign Client beenden wollen, erhalten Sie folgenden Hinweis:



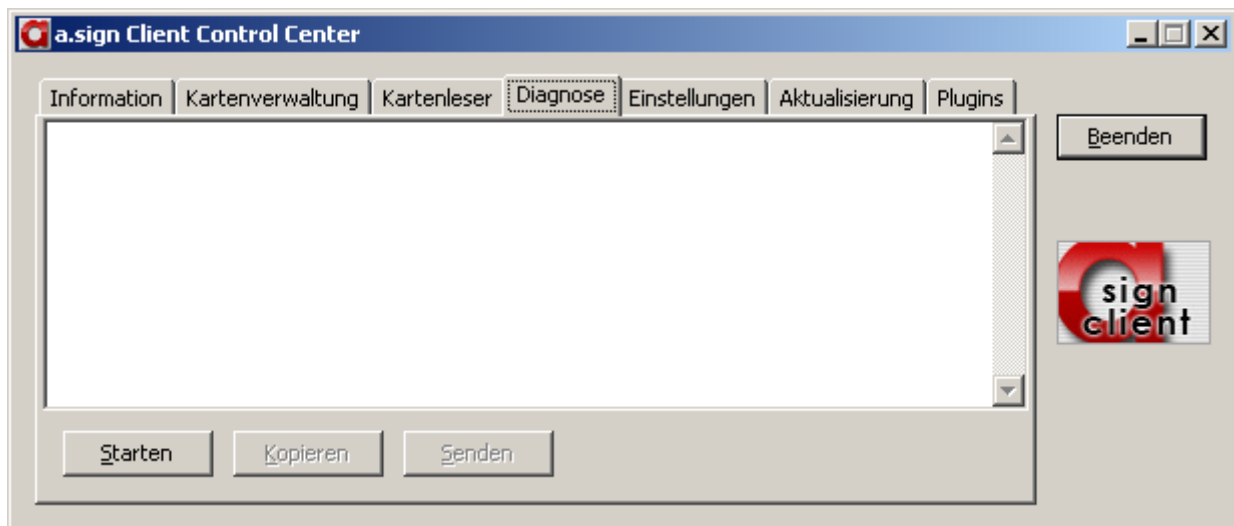
Wenn Sie mit „Ja“ bestätigen, wird die zuletzt angezeigte Konfiguration gespeichert. Wenn Sie „Nein“ wählen, bleibt die zuletzt gespeicherte Konfiguration erhalten.

1.6.4.11 Diagnose

Das Diagnose-Tool entspricht dem Client Check auf der a.trust Homepage (<http://www.a-trust.at> – Privat (oder Business) – Support – Tools/Downloads – Clientstatus überprüfen).

Bei Problemen rund um Ihre Signaturkarte bzw. den Signaturanwendungen können Sie die mittels der Diagnose erstellten Informationen an a.trust senden.

Hinweis: Es werden keine vertraulichen Informationen Ihres Pcs/Laptops an a.trust gesendet. Es wird lediglich die Client-Installation überprüft und von der a.trust Technik auf etwaige Fehler überprüft.

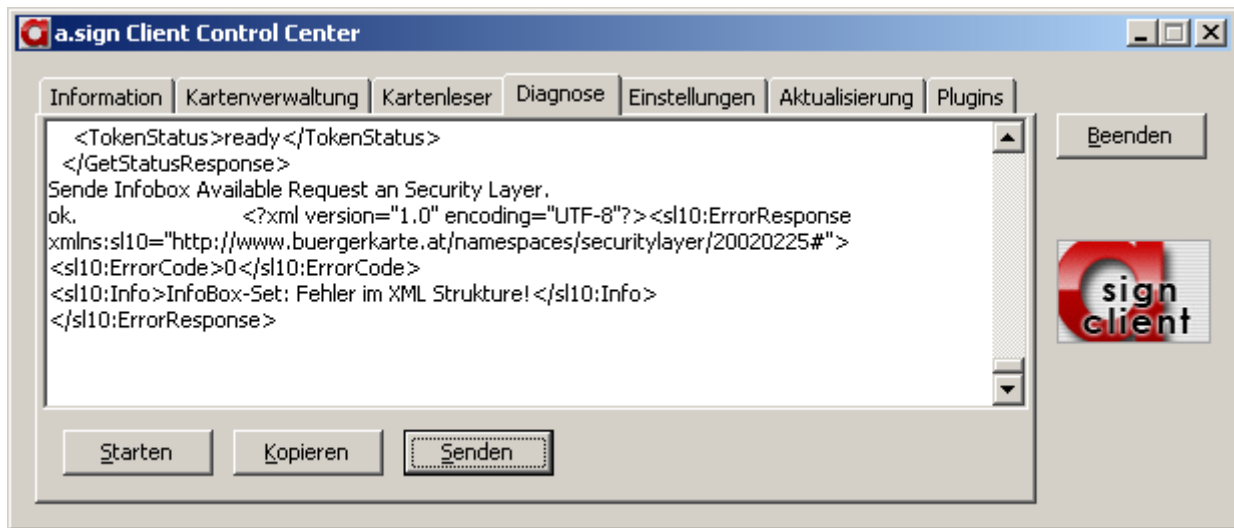


Klicken Sie auf „Starten“, um das Diagnose-Tool zu starten. Sie erhalten noch folgenden Hinweis:



Sobald Sie mit „OK“ bestätigt haben, startet die Diagnose.

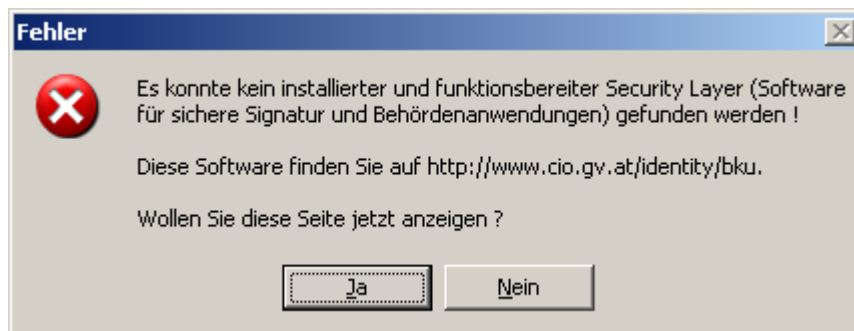
Bitte warten Sie das Ende der Diagnose ab – anschließend haben Sie die Möglichkeit, über den „Kopieren“-Button und anschließend über den „Senden“-Button die Diagnose an a.trust zu senden:



Sobald Sie auf Senden klicken, öffnet sich Ihr Mail-Programm mit einem neuen Mail. Empfänger sowie Betreff sind bereits vorausgefüllt, Sie müssen nur noch die kopierte Diagnose im Text-Bereich einfügen.

Hinweis: Während die Diagnose läuft kann kein anderes Programm auf den Kartenleser und auf die a.trust Signaturkarte zugreifen.

Sollten Sie keinen Security Layer (=Bürgerkartenumgebung) installiert bzw. gestartet haben, wird Ihnen am Ende der Diagnose ein Fehler gemeldet:



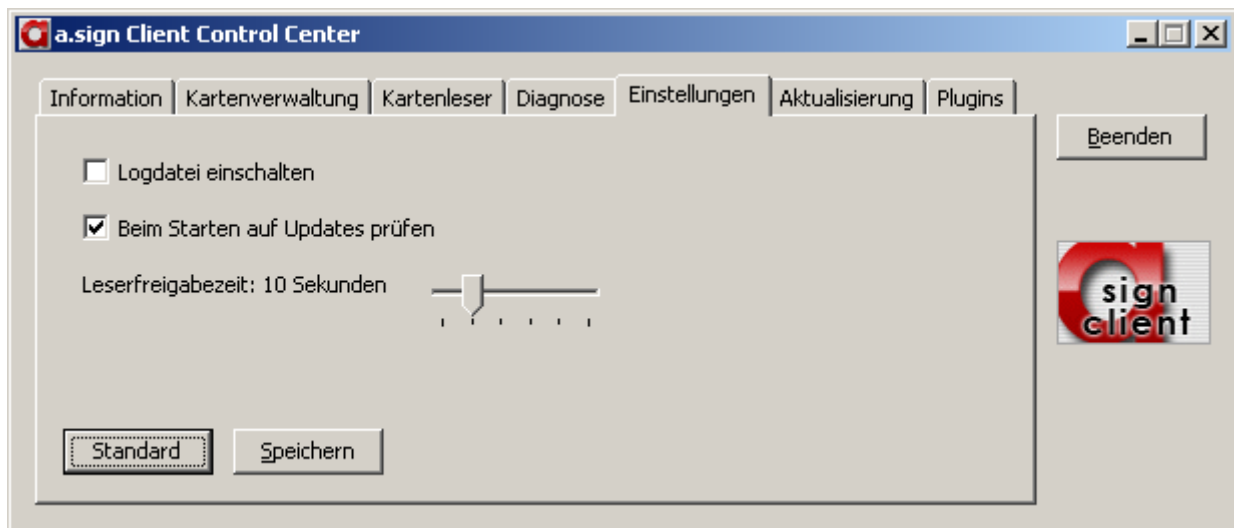
Mit einem Klick auf „Ja“ gelangen Sie auf die Hoempage des Bundeskanzleramtes, wo Sie die aktuellste Version der Bürgerkartenumgebung herunterladen können. Bei „Nein“ bleiben Sie auf der Diagnose-Maske und können diese wie beschrieben an a.trust senden.

1.6.4.12 Einstellungen

In den Einstellungen haben Sie folgende Möglichkeiten:

- Logdatei einschalten
- Beim Start auf Updates prüfen
- Leserfreigabezeit

In der Standardeinstellungen ist die Updatefunktion aktiviert und die Leserfreigabezeit auf 10 Sekunden gestellt:



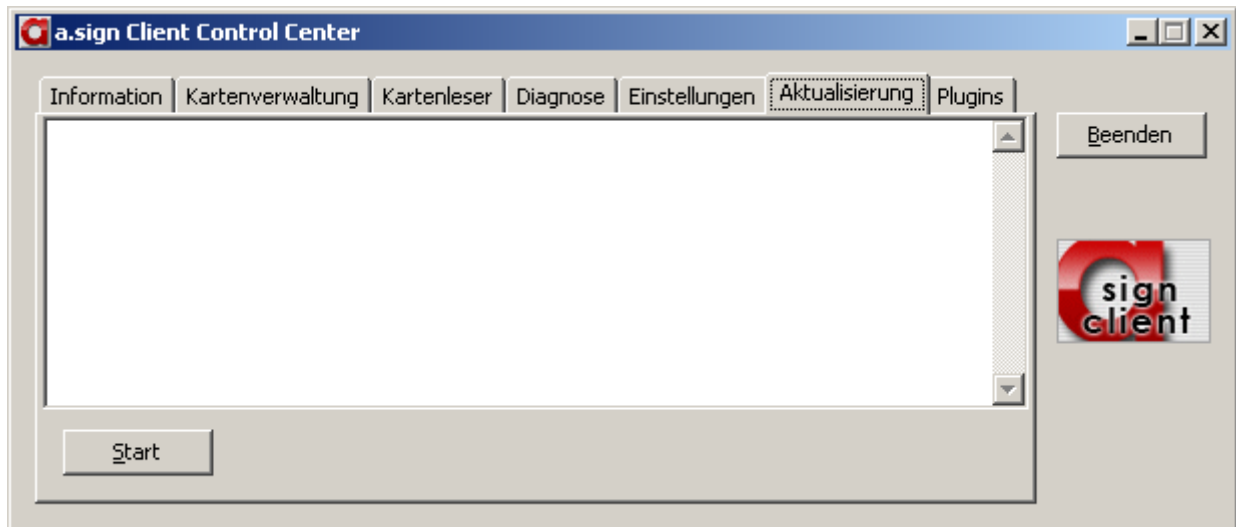
Wenn Sie die Logdatei aktivieren, wird im Verzeichnis C: Ihrer Festplatte die Datei „asi-gngna.log“ erstellt und bei jedem Zugriff auf den a.sign Client bzw. der a.trust Signaturkarte Log-Daten in dieses File geschrieben. Dieses File kann für die a.trust Technik nützlich beim Erkennen von Problemen sein.

Wenn Sie bei jedem Start des a.sign Client wünschen, dass dieser nach der aktuellsten online verfügbaren a.sign Client Version sowie nach neuen a.trust Stammzertifikaten sucht, aktivieren Sie „Beim Start auf Updates prüfen“. Ist ein Update verfügbar, werden Sie beim nach dem Windows-Start darauf aufmerksam gemacht.

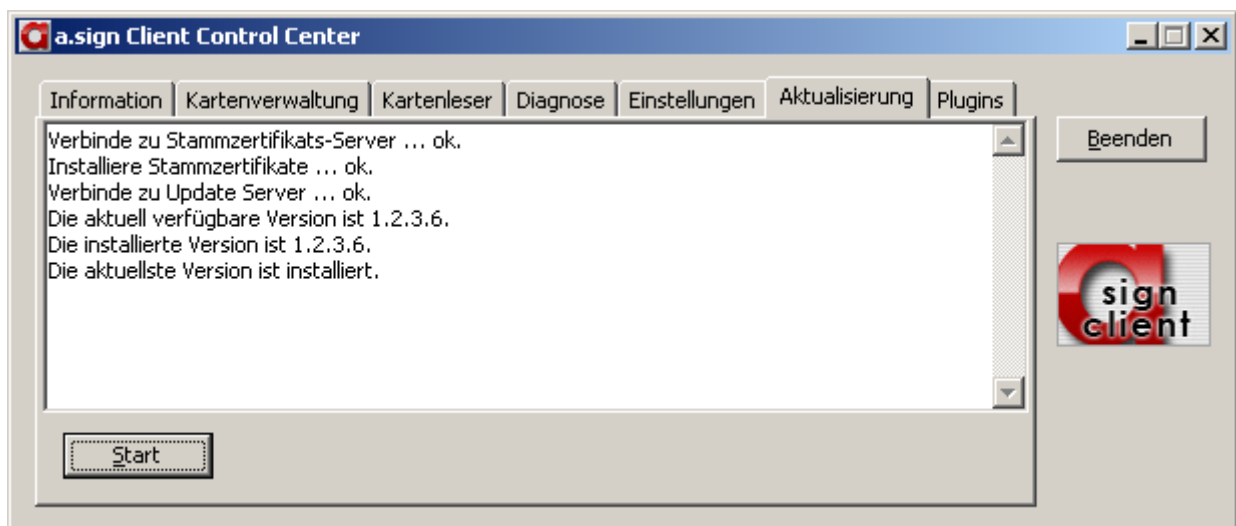
Bei der Leserfreigabezeit handelt es sich um die maximale Zeit, die ein Programm (z.B. Mozilla, Firefox) beim Zugriff auf den a.sign Client veranschlagen kann. Bei der Standardeinstellung von 10 Sekunden wird der Kartenleser nach spätestens 10 Sekunden vom Programm freigegeben und kann somit wieder angesprochen werden.

1.6.4.13 Aktualisierung

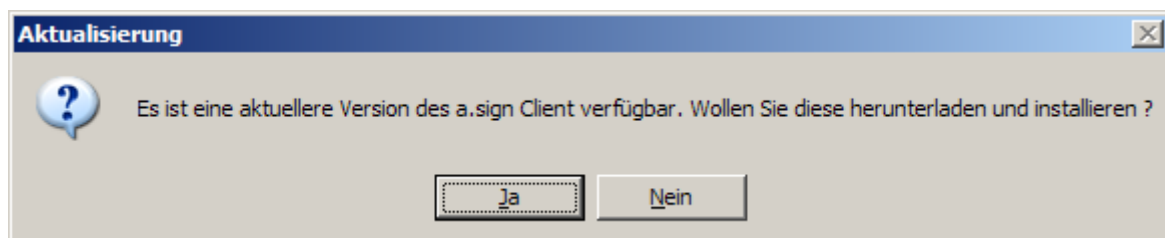
Hier können Sie sofort nach der aktuell verfügbaren a.sign Client Version bzw. nach neuen a.trust Stammzertifikaten suchen:



Klicken Sie auf „Start“, um die Verbindung zum a.trust Update-Server herzustellen:



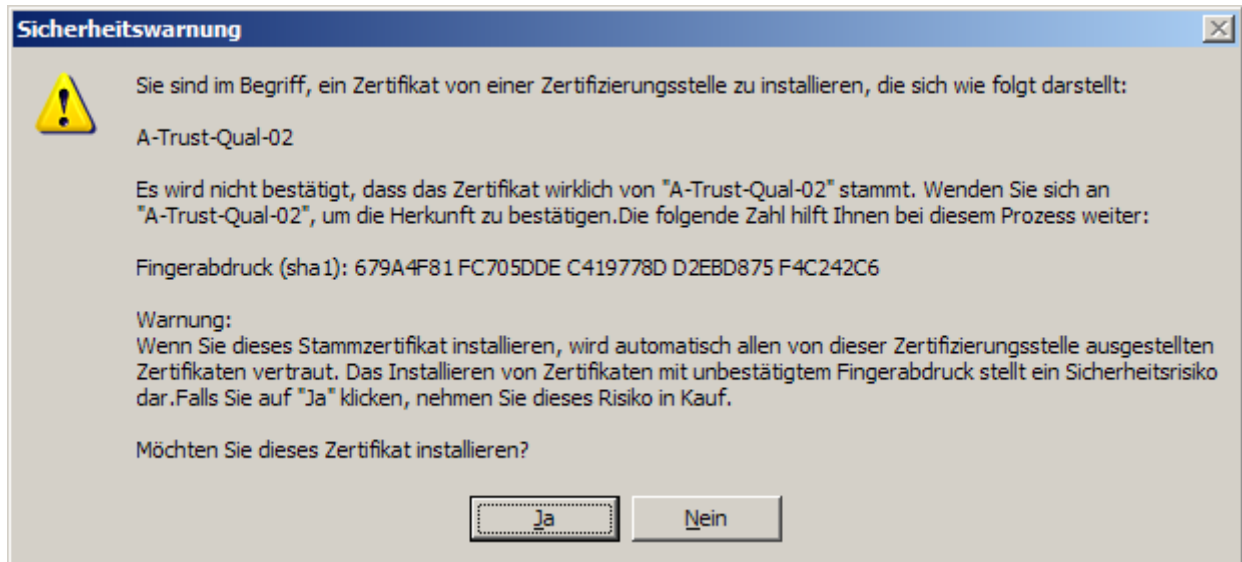
Steht eine aktuellere Version des a.sign Client zur Verfügung, wird Ihnen dies mitgeteilt:



Bestätigen Sie mit „Ja“, um die neue Version herunterzuladen und die Installation zu star-

ten.

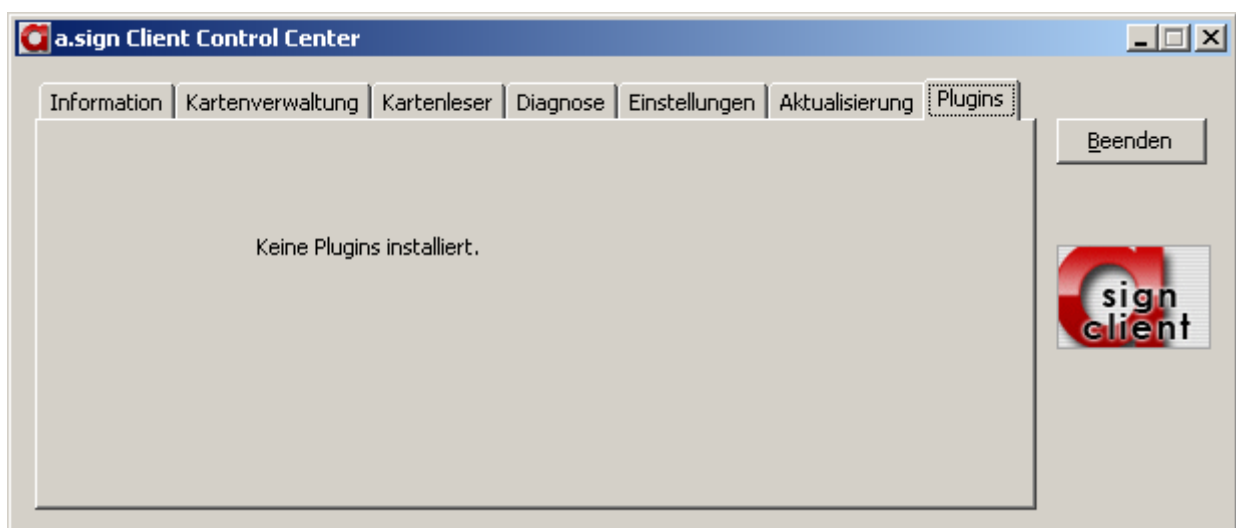
Fehlt Ihnen ein Stammzertifikat, wird Ihnen dieses zur Installation vorgeschlagen:



Bestätigen Sie mit „Ja“, damit das Stammzertifikat in den Windows Zertifikatsspeicher aufgenommen werden kann. Wenn Sie die Installation der a.trust Stammzertifikate ablehnen, kann dies zu Problemen mit Signaturanwendungen führen, die auf den Windows Zertifikatsspeicher zugreifen.

1.6.4.14 Plugins

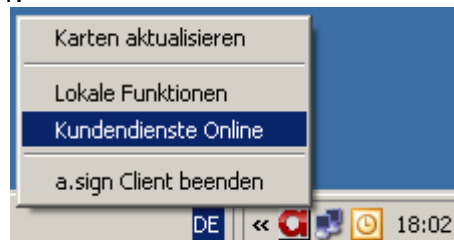
Hier werden installierte Zusatzprogramme des a.sign Client, zum Beispiel **a.sign Login**, angezeigt:



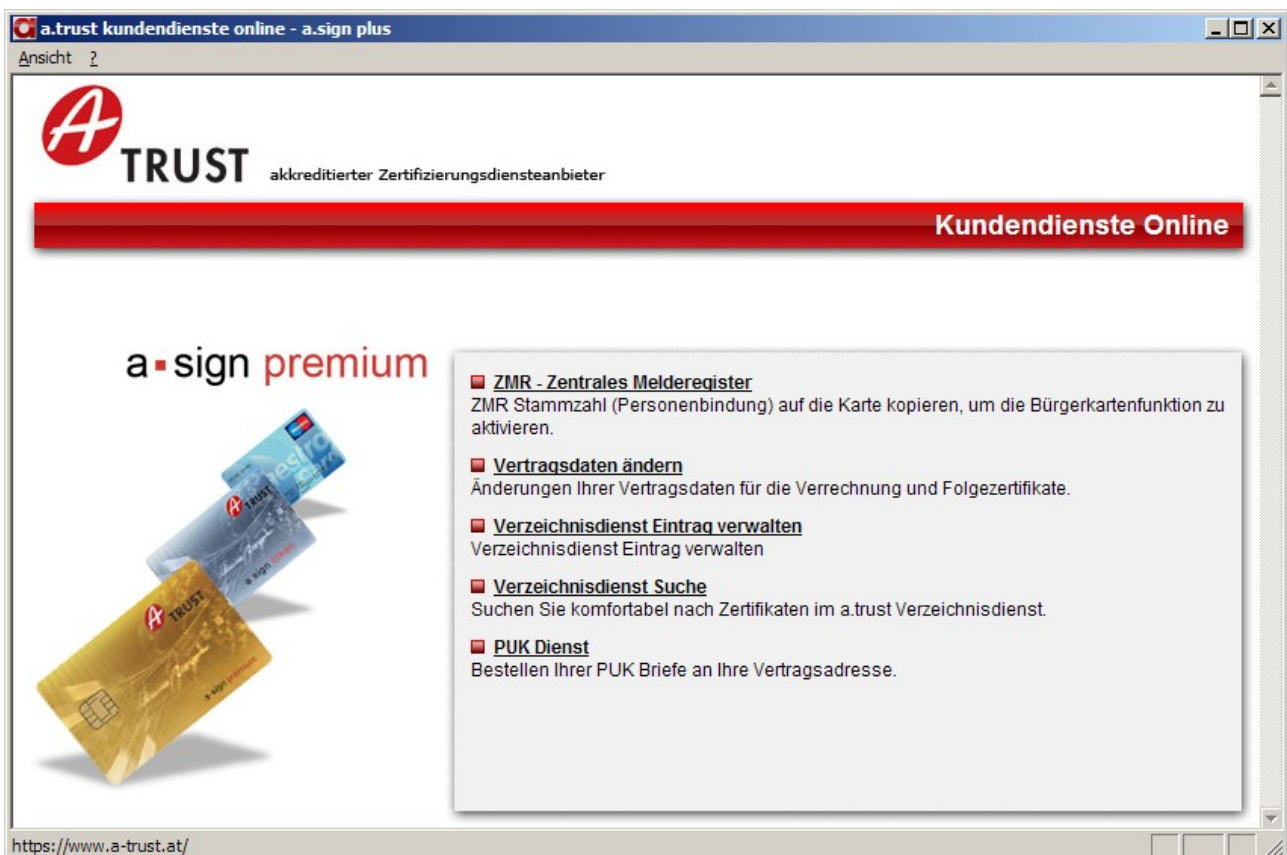
Standardmäßig wird der a.sign Client ohne Plugin installiert. Alle Informationen zum a.sign Login finden Sie auf der a.trust Homepage (<http://www.a-trust.at>).

1.6.5 Kundendienste Online

Über die a.sign Client Funktion „Kundendienste Online“ haben Sie die Möglichkeit, Ihre Personenbindung auf die Karte zu schreiben, Ihre Vertragsdaten zu ändern, Ihren Verzeichnisdienst Eintrag zu verwalten, im Verzeichnisdienst nach anderen a.trust Kunden zu suchen sowie unser PUK-Service zu nutzen. Durch einen Rechtsklick auf das a-Logo gelangen Sie zu dieser Funktion:



Sie gelangen nun auf die Startseite der Kundendienste Online. Wählen Sie hier das gewünschte Service:




1.6.5.4 ZMR – Zentrales Melderegister

Mit diesem Service haben Sie die Möglichkeit, Ihre ZMR-Bindung (=Personenbindung) auf Ihre a.trust Signaturkarte zu laden. Die Personenbindung ist vor allem dann notwendig, wenn Sie ein e-Government Service nutzen wollen.

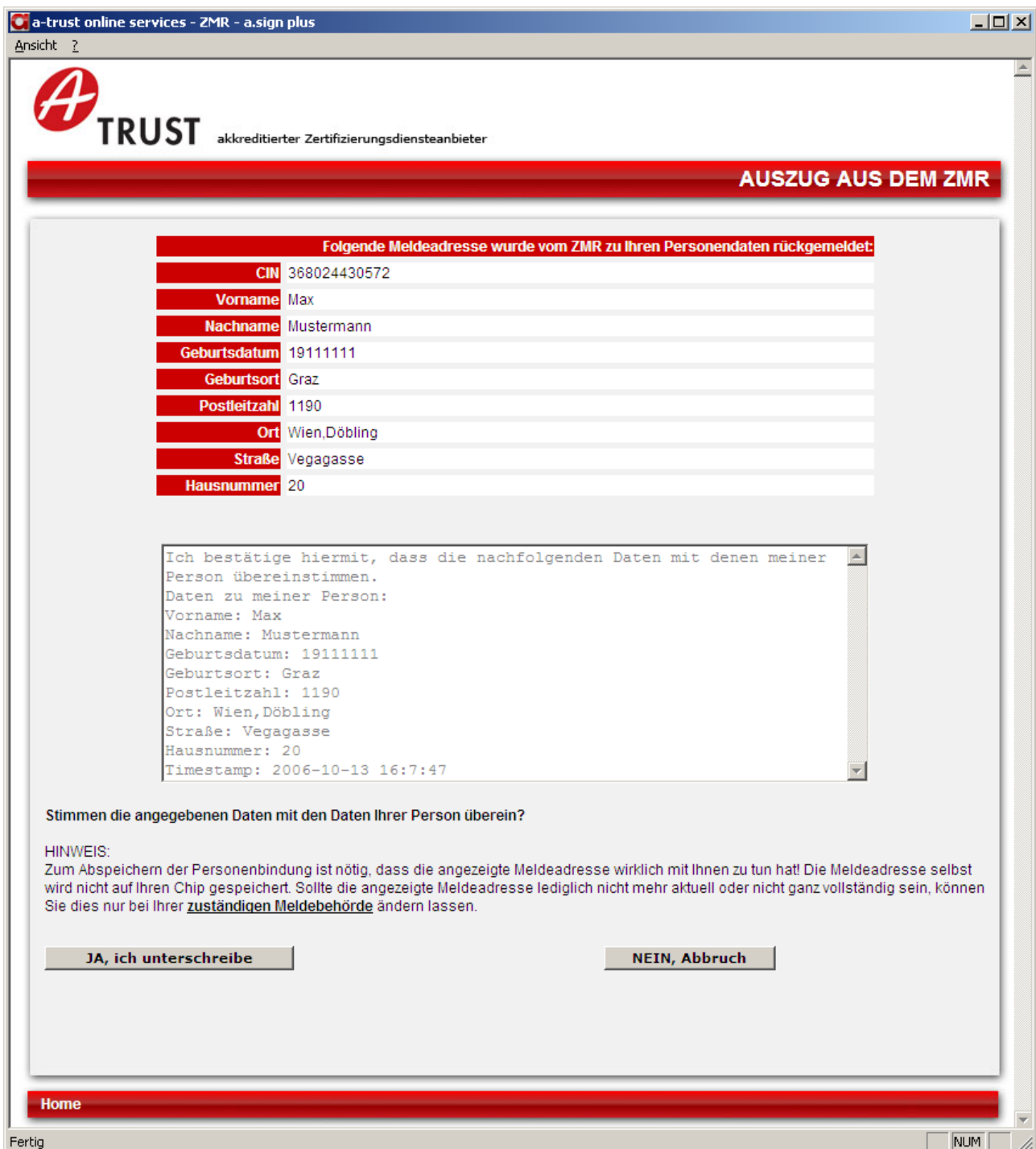
Bitte halten Sie die **Geheimhaltungs-PIN** parat – Sie werden während diesem Vorgang 3 Mal danach gefragt.

Klicken Sie auf „ZMR – Zentrales Melderegister“, um den Vorgang zu starten:



Überprüfen Sie hier bitte, ob das angegebene Zertifikat auch Ihres ist bzw. der eingelegten Signaturkarte entspricht. Wird hier kein Zertifikat angezeigt, führen Sie bitte die Funktion „Karten aktualisieren“ durch (siehe auch Punkt 1.6.3).

Klicken Sie auf „ZMR Abfrage starten“ - Sie werden nun das erste Mal nach der 4-stelligen Geheimhaltungs-PIN gefragt und erhalten anschließend folgende Maske:



The screenshot shows a web browser window titled "a-trust online services - ZMR - a.sign plus". The page header includes the A-TRUST logo and the text "akkreditierter Zertifizierungsdiensteanbieter". A red banner at the top right reads "AUSZUG AUS DEM ZMR".

The main content area features a red header: "Folgende Meldeadresse wurde vom ZMR zu Ihren Personendaten rückgemeldet:". Below this is a table of personal data:

CIN	368024430572
Vorname	Max
Nachname	Mustermann
Geburtsdatum	19111111
Geburtsort	Graz
Postleitzahl	1190
Ort	Wien,Döbling
Straße	Vegagasse
Hausnummer	20

Below the table is a text area containing a confirmation message:

```
Ich bestätige hiermit, dass die nachfolgenden Daten mit denen meiner Person übereinstimmen.  
Daten zu meiner Person:  
Vorname: Max  
Nachname: Mustermann  
Geburtsdatum: 19111111  
Geburtsort: Graz  
Postleitzahl: 1190  
Ort: Wien,Döbling  
Straße: Vegagasse  
Hausnummer: 20  
Timestamp: 2006-10-13 16:7:47
```

Below the text area is the question: "Stimmen die angegebenen Daten mit den Daten Ihrer Person überein?".

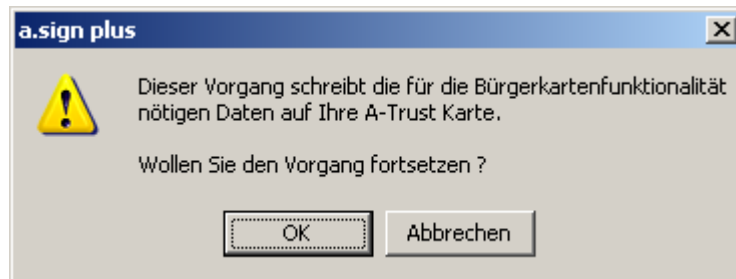
A "HINWEIS:" section follows, stating: "Zum Abspeichern der Personenbindung ist nötig, dass die angezeigte Meldeadresse wirklich mit Ihnen zu tun hat! Die Meldeadresse selbst wird nicht auf Ihren Chip gespeichert. Sollte die angezeigte Meldeadresse lediglich nicht mehr aktuell oder nicht ganz vollständig sein, können Sie dies nur bei Ihrer zuständigen Meldebehörde ändern lassen."

At the bottom of the form are two buttons: "JA, ich unterschreibe" and "NEIN, Abbruch".

A red "Home" button is located at the bottom left of the page content. The browser status bar at the bottom shows "Fertig" and "NUM".

Wählen Sie bitte nur **„NEIN, Abbruch“**, wenn die angegebenen Daten in keiner Weise mit Ihrer Person zu tun hat. Sie gelangen anschließend auf eine Informationsseite.

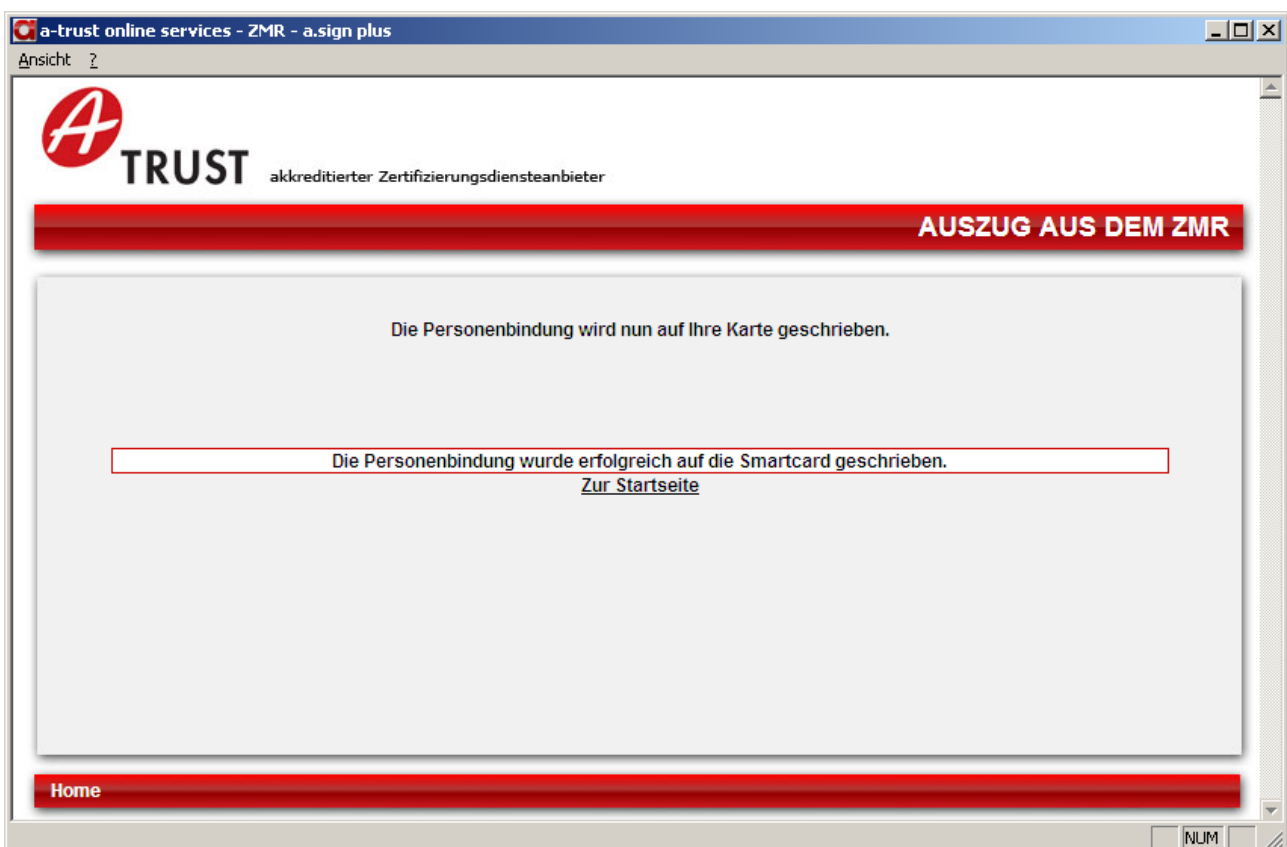
Um den Vorgang fortzusetzen, wählen Sie bitte **„JA, ich unterschreibe“**. Sie werden erneut nach der 4-stelligen Geheimhaltungs-PIN gefragt.



Bestätigen Sie bitte mit „OK“, um die Personenbindung auf die Karte zu schreiben. Allenfalls wird der Vorgang abgebrochen.

Sie werden nun ein letztes Mal nach der 4-stelligen Geheimhaltungs-PIN gefragt.

Abschließend sollten Sie folgende Rückmeldung erhalten:

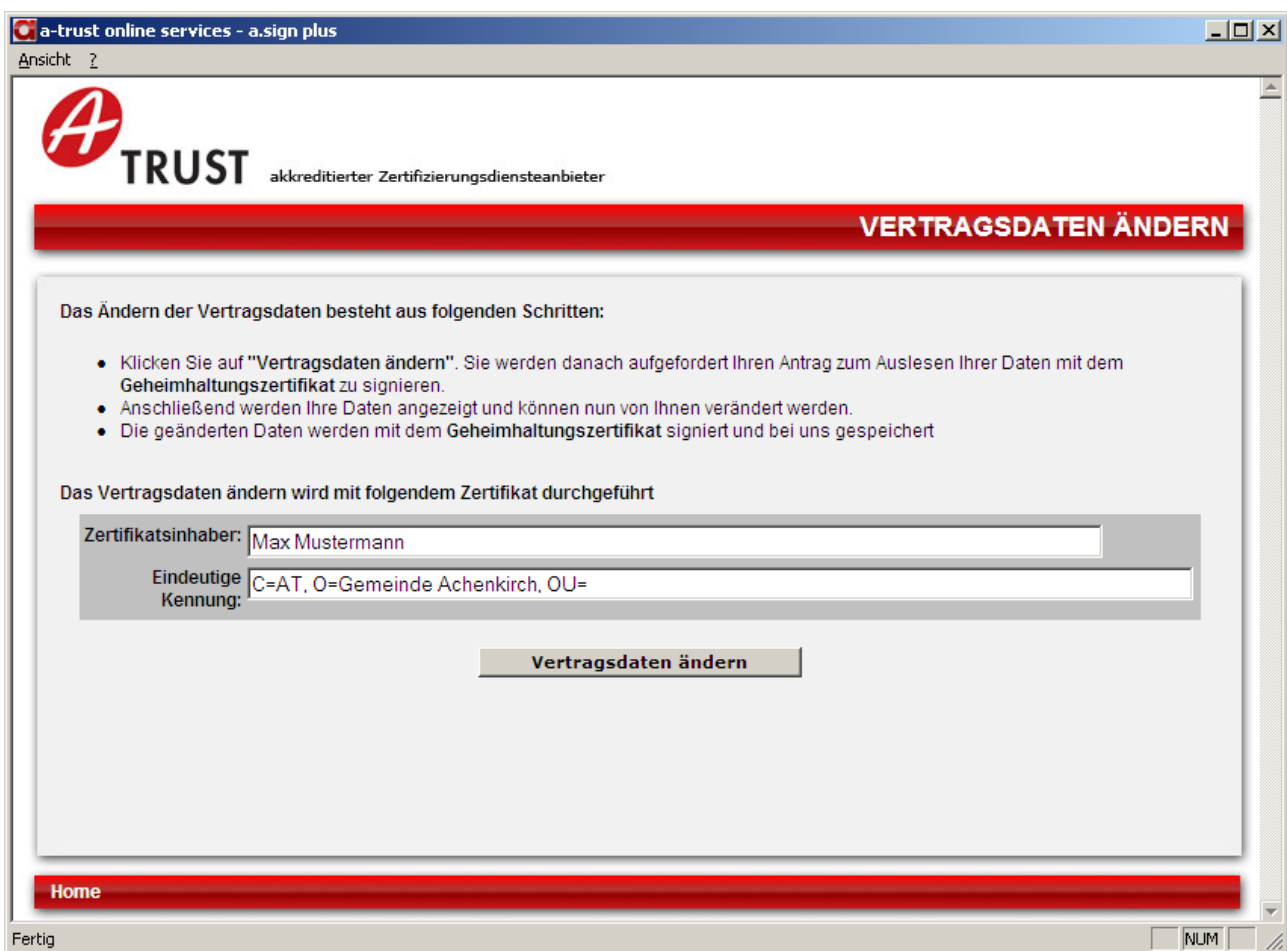


Die Personenbindung befindet sich nun auf der Smartcard, einer erfolgreichen Anmeldung an e-Government-Services steht somit nichts mehr im Wege.

Wie Sie überprüfen können, ob sich die Personenbindung tatsächlich auf der Karte befindet, können Sie unter 1.6.4.8 nachlesen.

1.6.5.5 Vertragsdaten ändern

Hier haben Sie die Möglichkeiten, Daten rund um Ihren Signaturvertrag einzusehen und zu ändern (sofern möglich).



a-trust online services - a.sign plus

Ansicht ?

 **TRUST** akkreditierter Zertifizierungsdiensteanbieter

VERTRAGSDATEN ÄNDERN

Das Ändern der Vertragsdaten besteht aus folgenden Schritten:

- Klicken Sie auf "Vertragsdaten ändern". Sie werden danach aufgefordert Ihren Antrag zum Auslesen Ihrer Daten mit dem Geheimhaltungszertifikat zu signieren.
- Anschließend werden Ihre Daten angezeigt und können nun von Ihnen verändert werden.
- Die geänderten Daten werden mit dem Geheimhaltungszertifikat signiert und bei uns gespeichert

Das Vertragsdaten ändern wird mit folgendem Zertifikat durchgeführt

Zertifikatsinhaber:

Eindeutige Kennung:

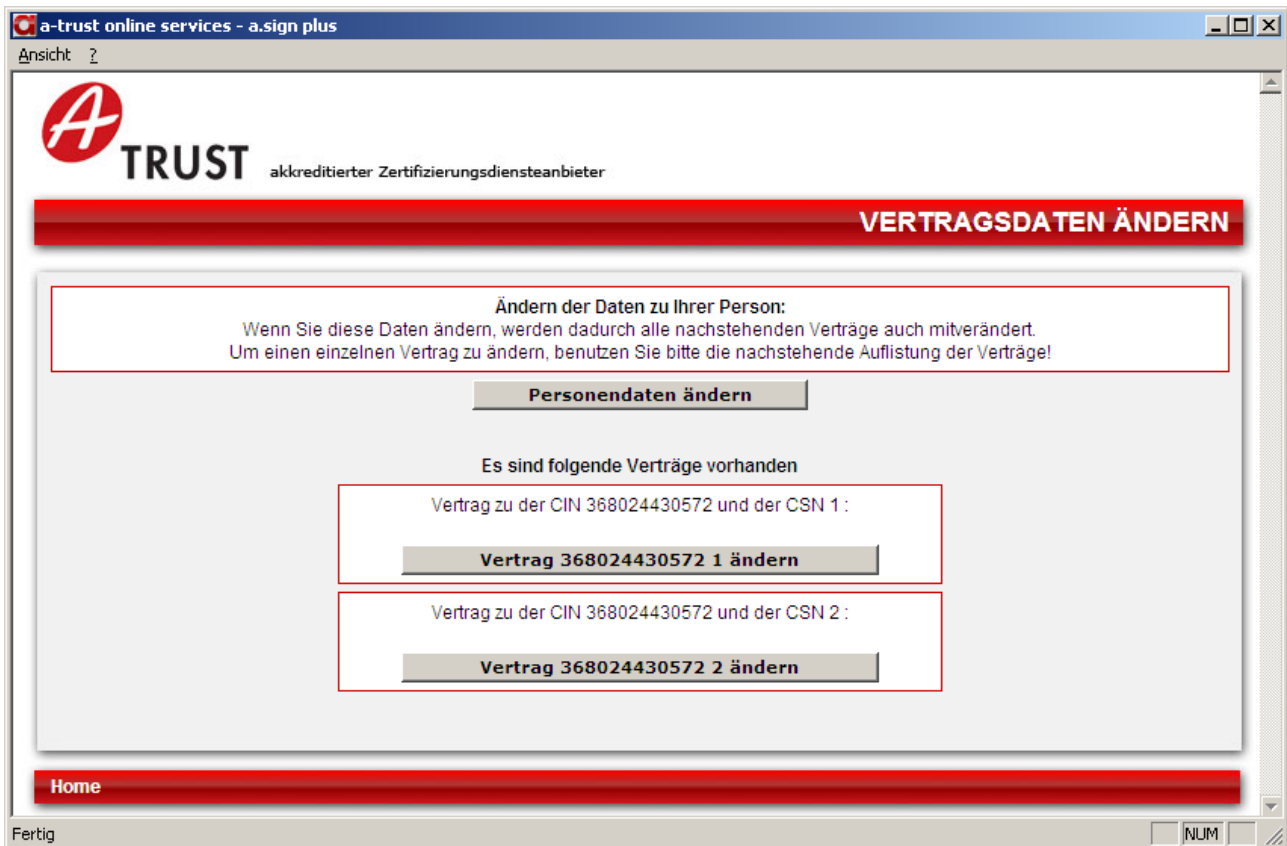
Home

Fertig

Klicken Sie auf „**Vertragsdaten ändern**“, um den Vorgang zu starten.



Klicken Sie auf „**Antrag signieren**“ - Sie werden nun nach der 4-stelligen Geheimhaltungs-PIN gefragt.



In unserem Fall gibt es 2 Verträge – je nachdem, wieviele Zertifikate unter der angegebenen Signaturvertragsnummer bereits ausgestellt wurden, werden hier ein oder mehrere Verträge angezeigt.

Unter „**Personendaten bearbeiten**“ finden Sie alle bei a.trust abgelegten Kontaktdaten, das sind Adresse, Widerrufspasswort (wird benötigt, wenn Sie Ihr Zertifikat sperren oder widerrufen möchten), Kontakt-E-Mail-Adresse sowie Telefonnummer. Klicken Sie auf „Ändern“, um die von Ihnen vorgenommenen Änderungen abzuspeichern. Sie erhalten anschließend die positive Rückmeldung „Ihre Daten wurden erfolgreich geändert“ und eine Bestätigungs-E-Mail.

Unter „**Vertragsdaten ändern**“ haben Sie die Möglichkeit, Ihre Ausweisdaten, Ihre Bankverbindung sowie die E-Mail-Adresse im Zertifikat zu ändern. Beachten Sie bitte, dass sich diese Änderungen erst bei der Ausstellung eines neuen Zertifikates auswirken. Klicken Sie auf „Ändern“, um die von Ihnen vorgenommenen Änderungen abzuspeichern. Sie erhalten anschließend die positive Rückmeldung „Ihre Daten wurden erfolgreich geändert“ und eine Bestätigungs-E-Mail.

1.6.5.6 Verzeichnisdienst Eintrag verwalten

Hier haben Sie die Möglichkeit zu bestimmen, ob Ihre Zertifikate im öffentlichen a.trust Verzeichnis aufscheinen sollen oder nicht.



The screenshot shows a web browser window titled "a-trust online services - a.sign plus". The page header includes the a-trust logo and the text "akkreditierter Zertifizierungsdiensteanbieter". A prominent red banner at the top right reads "VERZEICHNISDIENST".

The main content area is titled "Verzeichnisdienst Eintrag verwalten:" and contains the following text: "Hier können Sie die Einträge zu Ihren Zertifikaten aus dem a.trust Verzeichnis löschen bzw. hinzufügen. Falls Sie mehrere Zertifikate besitzen, müssen Sie diesen Vorgang für jedes Zertifikat seperat durchführen. Es kann nur jeweils der Eintrag zu dem Zertifikat geändert werden, mit welchem Sie sich hier anmelden."

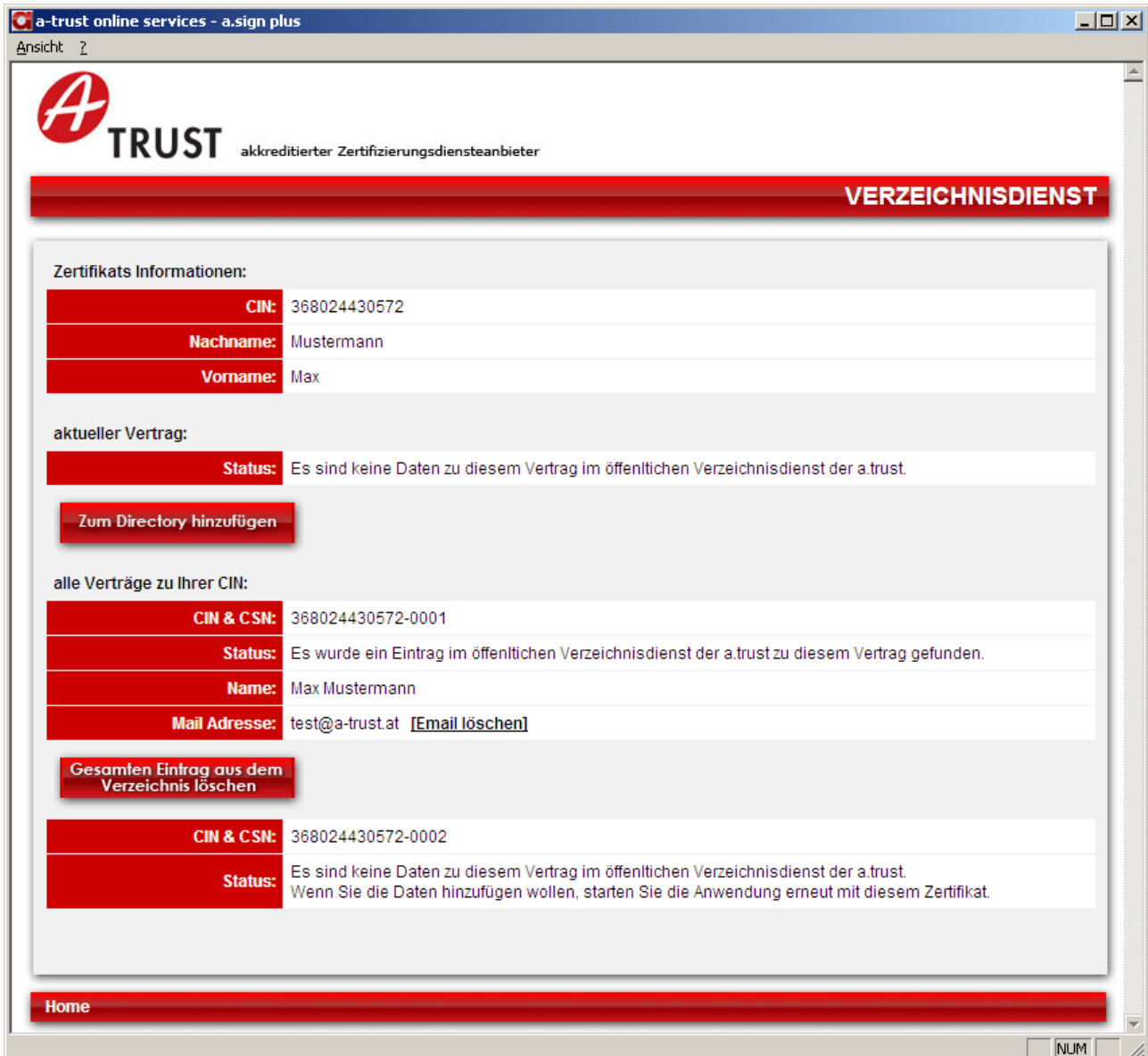
Below the text is a form with three input fields:

Zertifikatsinhaber:	Max Mustermann
Eindeutige Kennung:	C=AT, O=Gemeinde Achenkirch, OU=
Aussteller:	a-sign-Premium-Enc-02

At the bottom of the form area is a button labeled "Verzeichnisdienst Eintrag verwalten".

A red banner at the bottom left of the page contains the word "Home". The browser status bar at the bottom shows "Fertig" and "NUM".

Klicken Sie „**Verzeichnisdienst Eintrag verwalten**“, um den Vorgang fortzusetzen.



The screenshot shows a web browser window titled 'a-trust online services - a.sign plus'. The page header includes the 'a.trust' logo and the text 'akkreditierter Zertifizierungsdiensteanbieter'. A prominent red banner at the top right reads 'VERZEICHNISDIENST'.

Zertifikats Informationen:

CIN:	368024430572
Nachname:	Mustermann
Vorname:	Max

aktueller Vertrag:

Status:	Es sind keine Daten zu diesem Vertrag im öffentlichen Verzeichnisdienst der a.trust.
----------------	--

[Zum Directory hinzufügen](#)

alle Verträge zu Ihrer CIN:

CIN & CSN:	368024430572-0001
Status:	Es wurde ein Eintrag im öffentlichen Verzeichnisdienst der a.trust zu diesem Vertrag gefunden.
Name:	Max Mustermann
Mail Adresse:	test@a-trust.at [Email löschen]

[Gesamten Eintrag aus dem Verzeichnis löschen](#)

CIN & CSN:	368024430572-0002
Status:	Es sind keine Daten zu diesem Vertrag im öffentlichen Verzeichnisdienst der a.trust. Wenn Sie die Daten hinzufügen wollen, starten Sie die Anwendung erneut mit diesem Zertifikat.

At the bottom left, there is a 'Home' link. At the bottom right, there is a 'NUM' button.

Je nachdem, ob Ihre Zertifikate zum aktuellen Zeitpunkt im Verzeichnisdienst veröffentlicht ist oder nicht, bekommen Sie „Zum Directory hinzufügen“ (damit wird Ihr Zertifikat dem Verzeichnisdienst hinzugefügt) oder „Gesamten Eintrag aus dem Verzeichnis löschen“ zur Auswahl.

Ihre Zertifikate dem Verzeichnis hinzuzufügen macht vor allem dann Sinn, wenn Sie zum Beispiel Geschäftspartner haben, die Ihren öffentlichen Schlüssel zum Versand verschlüsselter Nachrichten benötigen.

1.6.5.7 Verzeichnisdienst Suche

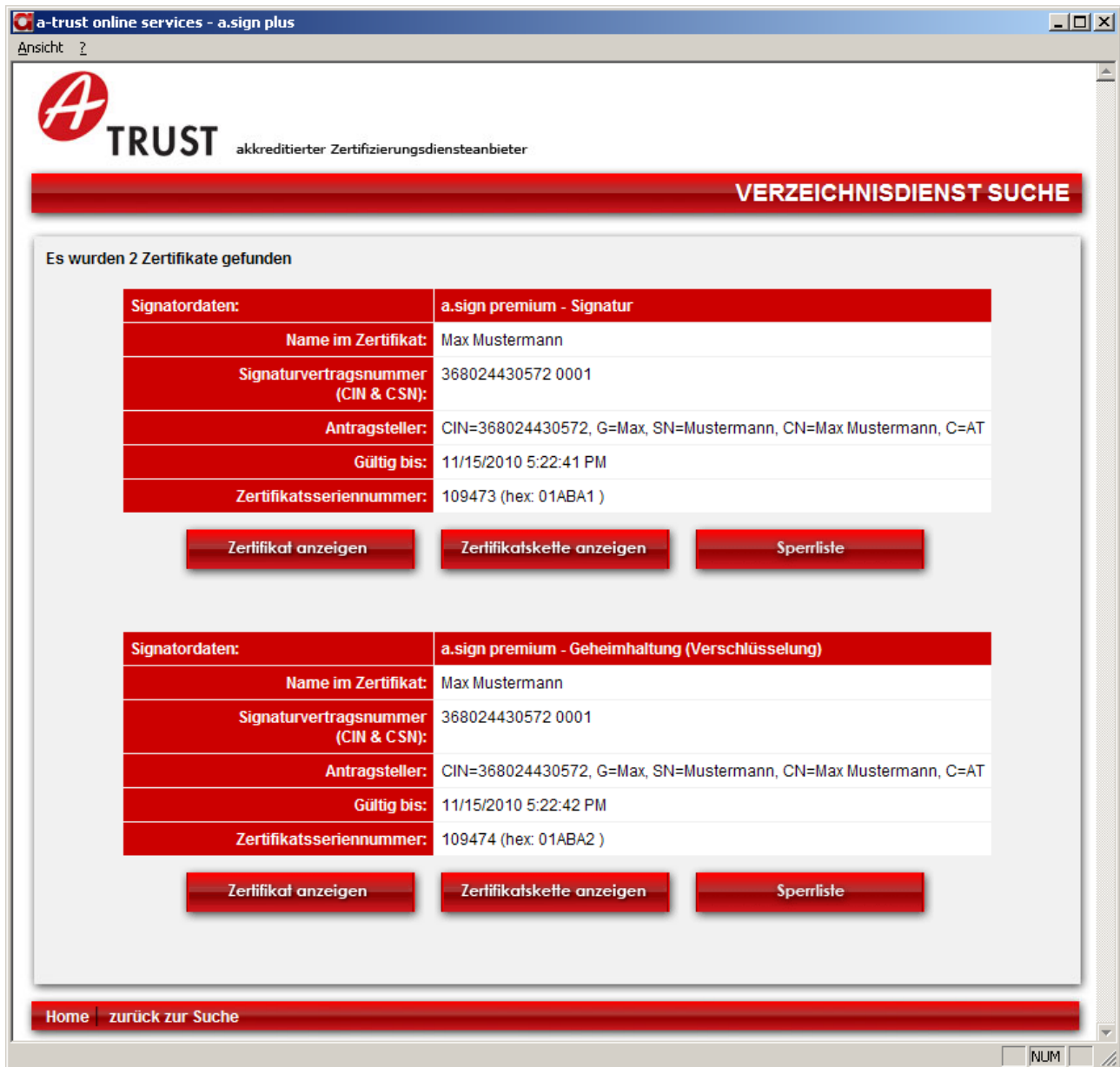
Hier haben Sie die Möglichkeit, nach einem bestimmten a.trust Zertifikat zu suchen, falls dieses im a.trust Verzeichnisdienst veröffentlicht wurde:



Geben Sie hier CIN (Signaturvertragsnummer), Vorname, Nachname oder Pseudonym ein und klicken Sie auf „**Suchen**“. Eine Selektierung nach Produkten (z.B. a.sign premium) ist ebenfalls möglich.

Im Falle eines Kartenproduktes werden 2 Zertifikate angezeigt, da sich auf Ihrer Karte der **Geheimhaltungsschlüssel** sowie der **Signaturschlüssel** befindet. Sollten Sie bei der Suche mehrere Zertifikate finden, berücksichtigen Sie bitte auch, dass auch abgelaufene oder widerrufen Produkte weiterhin im Verzeichnisdienst aufscheinen, sofern Sie nicht vom Besitzer gelöscht wurden (siehe 1.6.5.6). Achten Sie daher immer darauf, ob es sich um das aktuelle Zertifikat handelt.

Bei den (im folgenden Fenster angezeigten) Zertifikaten handelt sich ausschließlich um die **öffentlichen Schlüssel** der Zertifikate. Die privaten Schlüssel Ihrer Zertifikate verlassen natürlich niemals den geschützten Bereich Ihrer Signaturkarte.



The screenshot shows a web browser window titled "a-trust online services - a.sign plus". The page header includes the "A TRUST" logo and the text "akkreditierter Zertifizierungsdiensteanbieter". A red banner at the top reads "VERZEICHNISDIENST SUCHE". Below this, a message states "Es wurden 2 Zertifikate gefunden".

The first certificate entry is for "a.sign premium - Signatur". Its details are as follows:

Signatordaten:	a.sign premium - Signatur
Name im Zertifikat:	Max Mustermann
Signaturvertragsnummer (CIN & CSN):	368024430572 0001
Antragsteller:	CIN=368024430572, G=Max, SN=Mustermann, CN=Max Mustermann, C=AT
Gültig bis:	11/15/2010 5:22:41 PM
Zertifikatsseriennummer:	109473 (hex: 01ABA1)

Below the table are three buttons: "Zertifikat anzeigen", "Zertifikatskette anzeigen", and "Sperrliste".

The second certificate entry is for "a.sign premium - Geheimhaltung (Verschlüsselung)". Its details are as follows:

Signatordaten:	a.sign premium - Geheimhaltung (Verschlüsselung)
Name im Zertifikat:	Max Mustermann
Signaturvertragsnummer (CIN & CSN):	368024430572 0001
Antragsteller:	CIN=368024430572, G=Max, SN=Mustermann, CN=Max Mustermann, C=AT
Gültig bis:	11/15/2010 5:22:42 PM
Zertifikatsseriennummer:	109474 (hex: 01ABA2)

Below the table are three buttons: "Zertifikat anzeigen", "Zertifikatskette anzeigen", and "Sperrliste".

At the bottom of the page, there is a red bar with "Home" and "zurück zur Suche" links, and a "NUM" button in the bottom right corner.

Hier werden die Zertifikatsinhalte vom Namen bis hin zur Zertifikats-Seriennummer angezeigt. Die Seriennummer ist vor allem dann interessant, wenn Sie z.B. Ihre Signaturkarte bei Ihrer Bank für Online Banking mit Digitaler Signatur freischalten lassen wollen (Ihr Bankbetreuer benötigt die hier ausgegebenen Details).

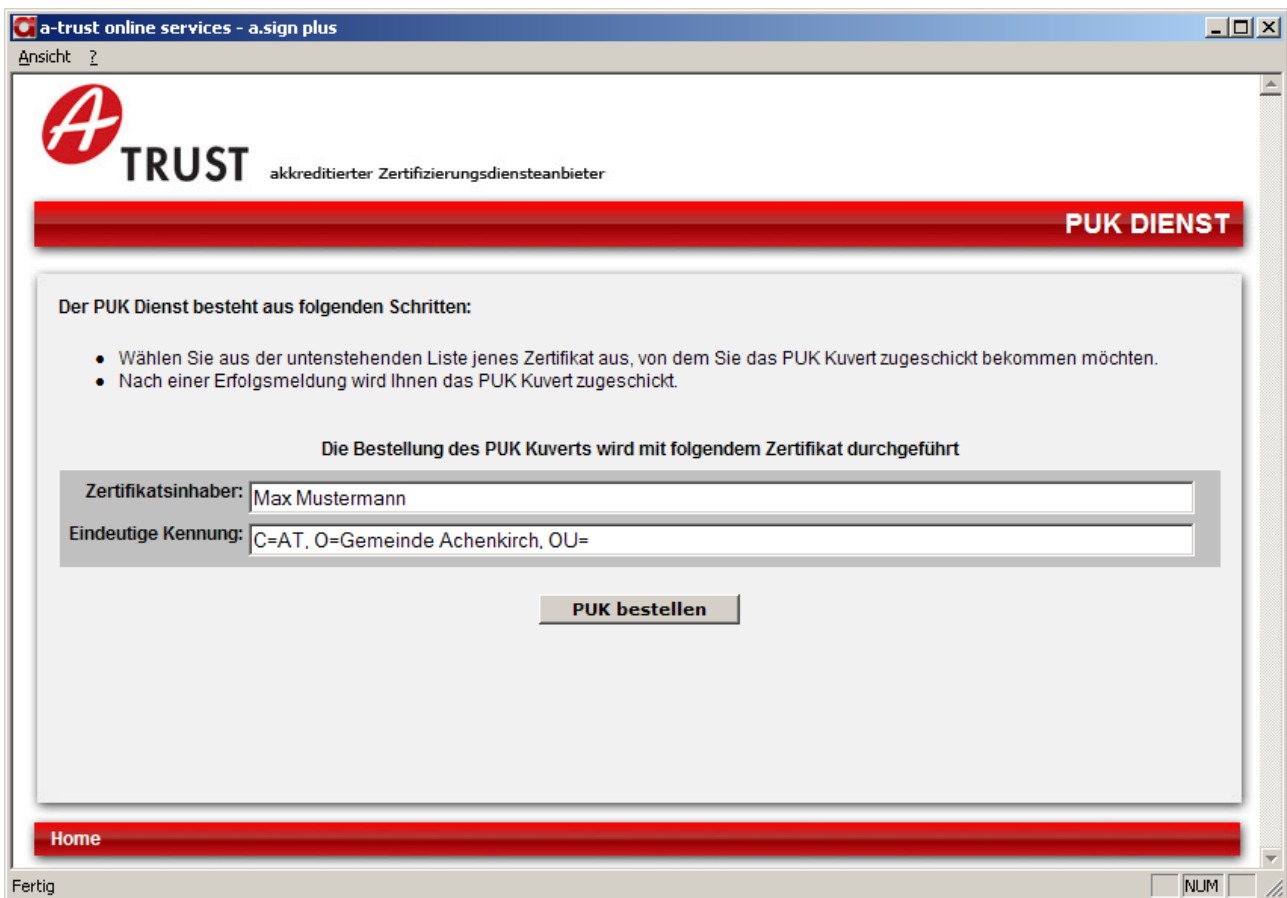
Außerdem können Sie sich das „Zertifikat anzeigen“ lassen bzw. über diesen Befehl das Zertifikat abspeichern, oder auch die komplette Zertifikatskette (samt Zwischeninstanz- und Stammzertifikaten) anzeigen lassen oder herunterladen.

Ebenfalls ist es hier möglich, sich die aktuelle Sperrliste zu dem angezeigten Produkt (z.B. a.sign premium) herunterzuladen.

1.6.5.8 PUK Dienst

Hier haben Sie die Möglichkeit, PUKs zu Ihrem Geheimhaltungs-, Signaturschlüssel sowie der Infobox Personenbindung zu ordern. Einen PUK benötigen Sie dann, wenn einer Ihrer PINs durch zu viele aufeinander folgende Fehlversuche gesperrt wurde.

Bitte beachten Sie, dass Sie mit einer PUK lediglich die Fehlversuche auf 0 zurücksetzen können (siehe auch 1.6.4.6). Sie können jede PUK 3 Mal zum Entsperren der PIN verwenden, danach ist auch die PUK aufgebraucht und kann nicht mehr benutzt werden.



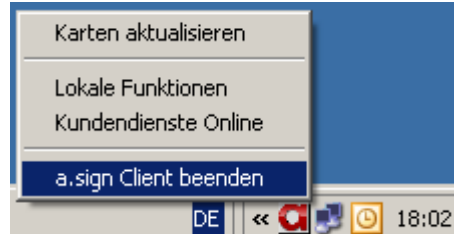
The screenshot shows a web browser window titled "a-trust online services - a.sign plus". The page header includes the "A TRUST" logo and the text "akkreditierter Zertifizierungsdiensteanbieter". A prominent red banner at the top right reads "PUK DIENST". Below this, the text "Der PUK Dienst besteht aus folgenden Schritten:" is followed by a bulleted list: "Wählen Sie aus der untenstehenden Liste jenes Zertifikat aus, von dem Sie das PUK Kuvert zugeschickt bekommen möchten." and "Nach einer Erfolgsmeldung wird Ihnen das PUK Kuvert zugeschickt." A sub-section titled "Die Bestellung des PUK Kuverts wird mit folgendem Zertifikat durchgeführt" contains two input fields: "Zertifikatsinhaber:" with the value "Max Mustermann" and "Eindeutige Kennung:" with the value "C=AT, O=Gemeinde Achenkirch, OU=". A "PUK bestellen" button is centered below the fields. At the bottom left, there is a "Home" link, and at the bottom right, a "NUM" button. The status bar at the very bottom shows "Fertig" and a progress indicator.

Klicken Sie auf „PUK bestellen“. Sie erhalten nun folgende Rückmeldung:

Ihr Antrag wurde erfolgreich durchgeführt!
In den nächsten Tagen wird Ihnen das PUK Kuvert per Post zugeschickt!
[Zur Startseite](#)

1.6.6 a.sign Client beenden

Sie können das a.sign Administrationsprogramm beenden, indem Sie die Funktion „a.sign Client beenden“ ausführen:

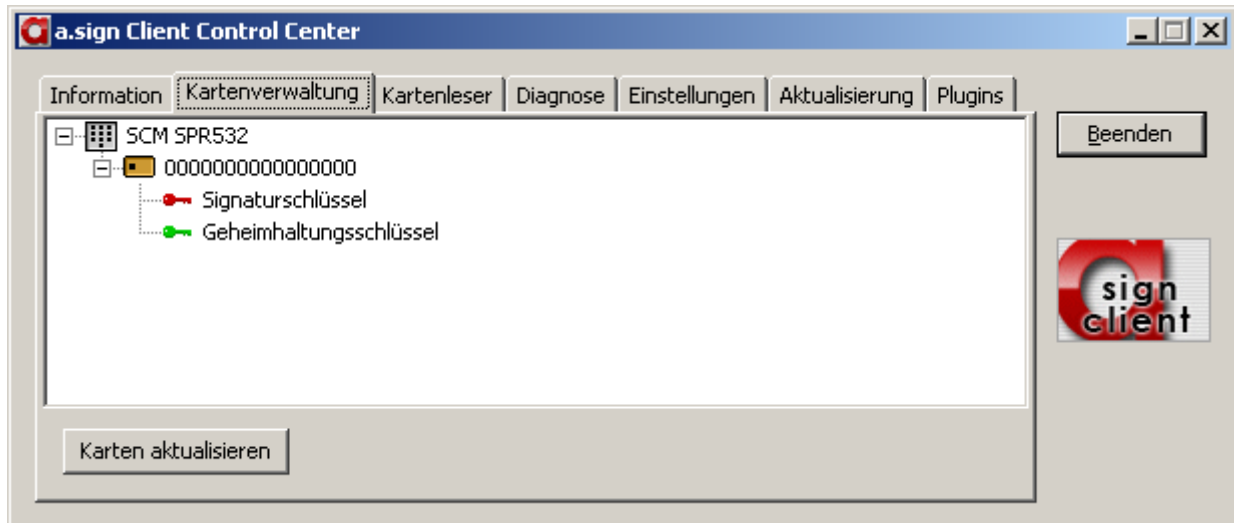


Hinweis: Damit wird lediglich das Administrationsprogramm beendet. Auch ohne aktivem a.sign Client Programm ist es Ihnen möglich, z.B. Mails oder Dateien zu signieren. Der a.-sign Client wird automatisch aktiv, wenn ein Programm darauf zugreift.

1.7 Troubleshooting

Anbei finden Sie uns bekannte Problemfälle und deren Ursache sowie Problemlösung:

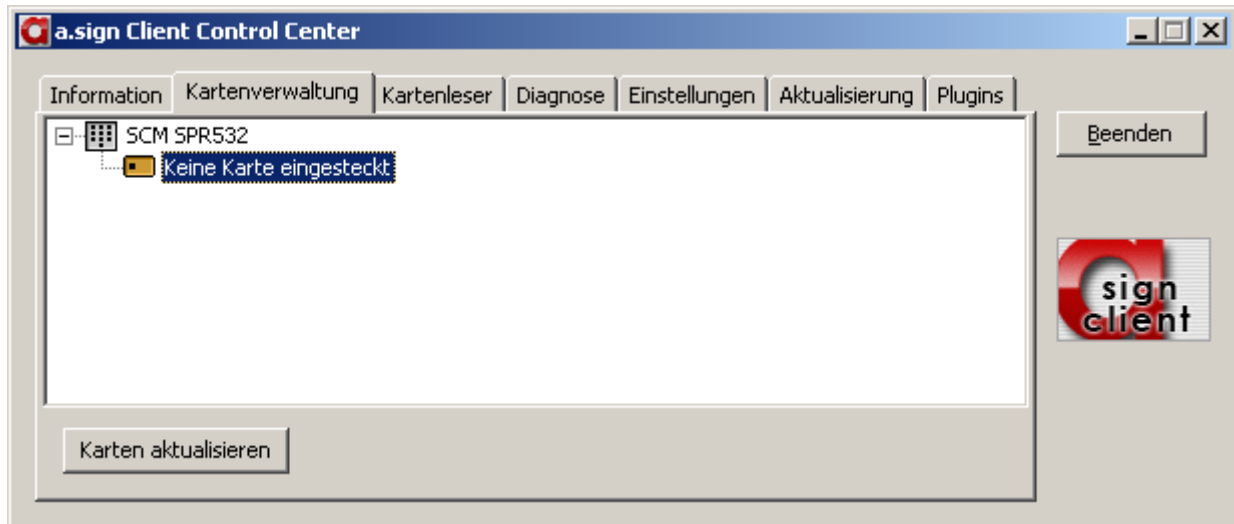
- Die Signaturkarte wird in der Kartenverwaltung nicht korrekt angezeigt



Wie hier zu erkennen ist, werden anstatt der Signaturvertragsnummer nur Nullen angezeigt. Das bedeutet, dass die eingelegte Karte zwar für die Digitale Signatur geeignet und vorbereitet ist, jedoch noch keine Zertifikate darauf aktiviert wurden.

Lösung: Suchen Sie eine nächstgelegene Registrierungsstelle auf und lassen Sie sich a.-sign premium auf Ihrer maestro- oder Mastercard aktivieren. Eine Liste aller Registrierungsstellen finden Sie unter <http://www.a-trust.at/registrierung>.

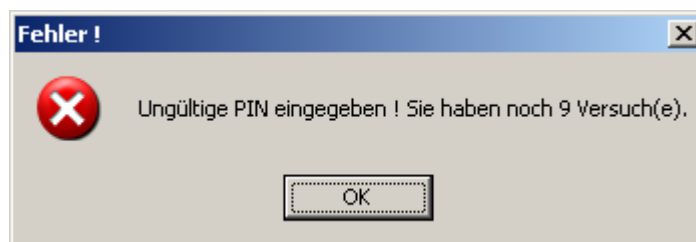
- Meldung „Keine Karte eingesteckt“



Die Signaturkarte befindet sich nicht (korrekt) im Kartenlesegerät oder kann nicht gelesen werden. Ebenfalls kann es sich auch um eine Fremdkarte handeln (z.B. die e-card), die nicht für a.sign premium geeignet ist.

Lösung: Beachten Sie bitte: Beim Einlegen der Signaturkarte in das Kartenlesegerät muss bei dieser der Chip zu Ihnen schauen und im Kartenleser verschwinden. Wird der Karteninhalt dennoch nicht angezeigt und handelt es sich um eine aktivierte a.trust Signaturkarte, testen Sie eine andere a.trust Signaturkarte an diesem Kartenlesegerät bzw. testen Sie Ihre Karte an einem anderen Kartenlesegerät.

- Ungültige Pin-Eingabe



Diese Meldung erscheint, wenn Sie eine nicht korrekt Pin eingegeben haben (z.B. beim Signieren von Mails oder beim Ändern einer Pin).

Lösung: Kontrollieren Sie die eingegebene Pin mit den Pin-Informationen, die Sie von a.trust erhalten haben. Achten Sie auch immer darauf, welche Pin (Geheimhaltung, Si-

gnatur, Infobox) verlangt wird.

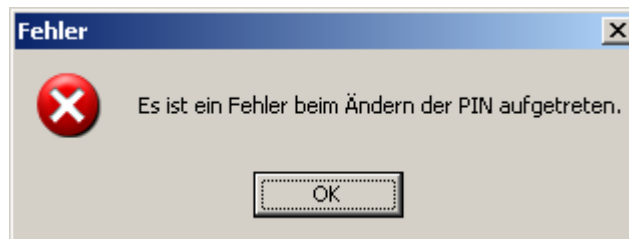
- Eingabe für neue Pin nicht identisch



Dieser Fehler erscheint, wenn bei einer Pin-Änderung die neue Pin bzw. die wiederholte Eingabe der neuen Pin nicht übereinstimmen.

Lösung: Versuchen Sie es erneut und achten Sie dabei auf die Reihenfolge: Alte Pin – neue Pin – neue Pin wiederholen

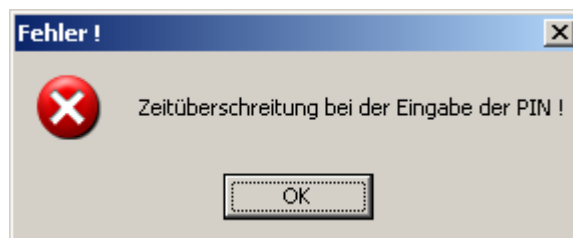
- Fehler beim Ändern der Pin



Diese Meldung kommt abschließend, wenn die neue Pin sowie die Wiederholung der neuen Pin nicht übereinstimmen.

Lösung: Siehe auch „Eingabe für neue Pin nicht identisch“

- Zeitüberschreitung bei der Eingabe der Pin

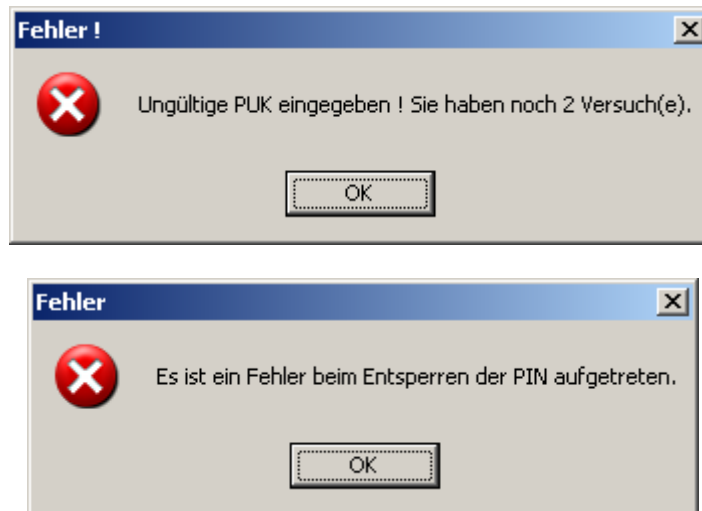


Diese Meldung erscheint, wenn eine Pin wurde nicht in der angegebenen Zeit eingegeben

wurde.

Lösung: In der Regel haben Sie für die erste Stelle der Pin 60 Sekunden, für jede weitere Stelle 5 Sekunden Zeit, um diese einzugeben. Achten Sie daher auf die verbleibende Zeit. Eine Zeitüberschreitung zählt aber nicht als Fehlversuch.

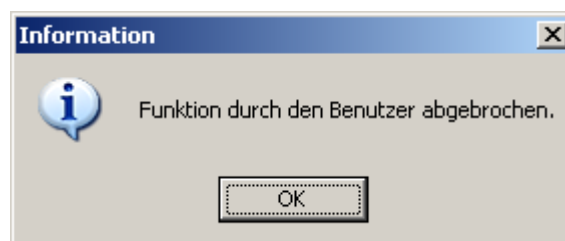
- Ungültige PUK-Eingabe bzw. Fehler beim Entsperren der Pin



Diese Meldungen erscheinen, wenn Sie beim Entsperren einer Pin einen falschen PUK verwendet haben.

Lösung: Kontrollieren Sie den PUK mit den PUK-Informationen, die Ihnen a.trust zugesandt hat (siehe auch ...). Achten Sie bitte auch darauf, für das Entsperren einer Pin den richtigen PUK zu verwenden (zum Beispiel wird für das Entsperren der Geheimhaltungs-Pin der Geheimhaltungs-PUK benötigt).

- Funktion durch Benutzer abgebrochen

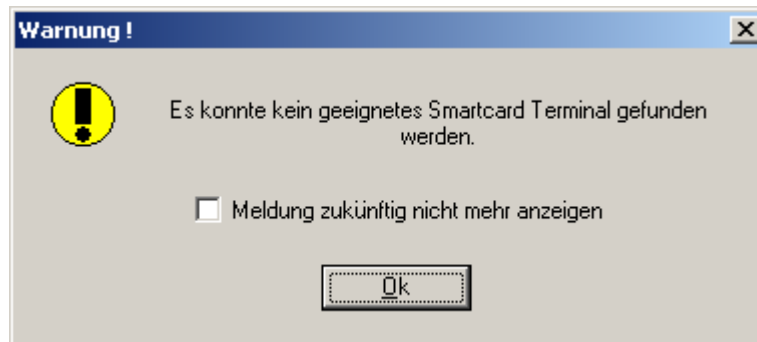


In diesem Falle wurde der Abbruch durch den Benutzer verursacht, z.B. durch das Drücken der „Abbrechen“-Taste auf dem Kartenlesegerät oder bei einem Abbruch beim

Entsperren oder Hinterlegen einer Pin.

Lösung: Wählen Sie die Abbrechen-Funktion nur, wenn Sie den Verdacht haben, eine Pin-Stelle falsch eingegeben zu haben. Dadurch wird ein Fehlversuch vermieden.

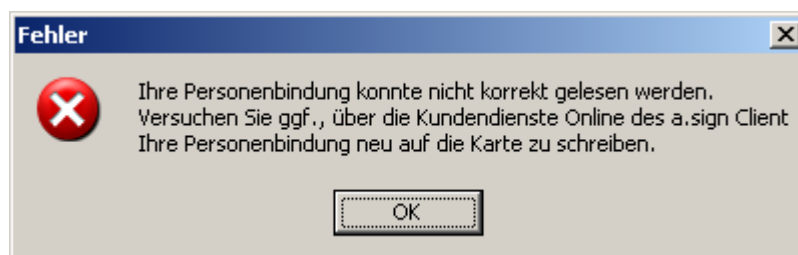
- Es konnte kein geeignetes Smartcard Terminal gefunden werden



Diese Meldung erscheint, wenn Sie keinen funktionsfähigen Kartenleser an Ihrem PC/Laptop angeschlossen haben.

Lösung: Überprüfen Sie, ob Ihr Kartenlesegerät korrekt an Ihrem PC/Laptop angeschlossen ist. Installieren Sie ggfls. Den Kartenleser-Treiber neu.

- Personenbindung konnte nicht korrekt gelesen werden



Diese Meldung kommt, wenn sich auf Ihrer a.trust Signaturkarte keine bzw. eine fehlerhafte Personenbindung befindet.

Lösung: Schreiben Sie über die Funktion „Kundendienste Online“ des a.sign Client Ihre Personenbindung neu auf die Karte.