A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH
A-1030 Wien, Landstraßer Hauptstraße 5 www.a-trust.at
DVR-Nummer: 1065181 - FN: 195738 a
akkreditierter Zertifizierungsdienstanbieter

Registrierungshandbuch
für Registration Officers
zum qualifizierten Zertifikat

trust|sign

a.sign premium

Version 2.1

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

INHALT DES REGISTRIERUNGSHANDBUCHS:

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

Ablauf der Registrierung laut Checkliste für den Zertifikatswerber

Schritt	Vorgang
A	Gültiger amtlicher Lichtbildausweis und Antragstellerformular vorhanden? Wissen Sie Ihre PINs? (Vorbereitung der Registrierung)
B	Identifikation des Zertifikatswerbers – Ausweisprüfung
C	Kontrolle des Antrags
D	Kontrolle des Signaturvertrags und der kommerziellen Vereinbarungen
E	Belehrung im Sinne des Signaturgesetzes
F	Unterzeichnen des Antrags und des Signaturvertrags
G	Archivierung der Dokumente und Ausstellung der Zertifikate
H	Aktivierung der Karte durch Eingabe der SignaturPIN des RO
I	Erstellen der SignaturPIN mit Hilfe der InitialPIN

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

Die Registrierung mit dem RA-Client (RA-Setup 1.1)

A) Vorbereitung der Registrierung

Frage nach den notwendigen Unterlagen:

- Gültiger amtlicher Lichtbildausweis:
  - Internationaler Reisepass
  - Österreichischer Führerschein
  - Österreichischer Personalausweis
  - Österreichische Identitätskarte
- Kenntnis der beiden PINs
- Antragstellerformular

Sollte keiner dieser gültigen (!) amtlichen Lichtbildausweise vorhanden sein, und/oder der Signator seine PINs nicht kennen, muss ein neuer Registrierungstermin vereinbart werden.

Karte aus dem Tresor holen:

Name und Kartennummer ist dem Antragstellerformular und dem PIN- oder PUK-Kuvert zu entnehmen
Eintragen der Kartenentnahme in die Lagerliste (Produktionsprotokoll)
Erst dann darf die sichere Verbindung mit dem RA-Client aufgebaut werden (Karte des RO nicht unbeaufsichtigt lassen!).

Hat der Signator sein Antragstellerformular nicht mit, so müssen die Daten des Signators direkt im RA-Client korrigiert werden.
Sollte die Karte noch nicht eingetroffen sein: Status der Karte im RA-Client prüfen (Tabelle II) und entsprechenden neuen Termin zur Abholung vereinbaren (Empfehlung: nach mind. 5 Werktagen).

B) Identifikation des Zertifikatswerbers

Qualifizierte Zertifikate dürfen laut österreichischem Signaturgesetz ausschließlich für natürliche Personen ausgestellt und die Karte mit den Signaturerstellungsdaten nur dem Signator persönlich übergeben werden. Die Identifikation des Zertifikatswerbers ist deshalb neben der Belehrung wesentliches Qualitätskriterium des trust|sign bzw a.sign premium Registrierungsvorgangs.

Kriterien zur Ausweiskontrolle:

- Ausweis ist in der Liste der von a.trust akzeptierten Dokumente
- Lichtbild stimmt mit Ausweisinhaber überein
- Ausweis ist für den RO lesbar (Sprache Deutsch oder Englisch, Vergilbung und Verschmutzung?)
- Gültigkeitsdatum ist nicht abgelaufen (Auch bei Reisepass!)
- Sensibilität gegenüber den Sicherheitsmerkmalen von Ausweisen (Gesamteindruck)

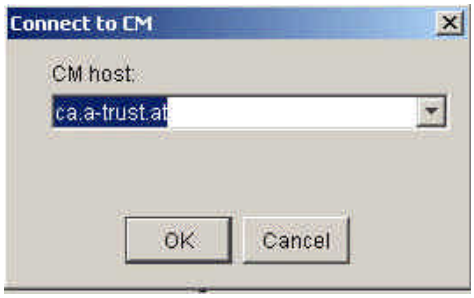
Bei Bedenken hinsichtlich mindestens eines Kriteriums: Vorlage eines anderen Ausweises aus der Liste der von a.trust akzeptierten Dokumente verlangen! (§§ 7 u. 8 SigG)

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

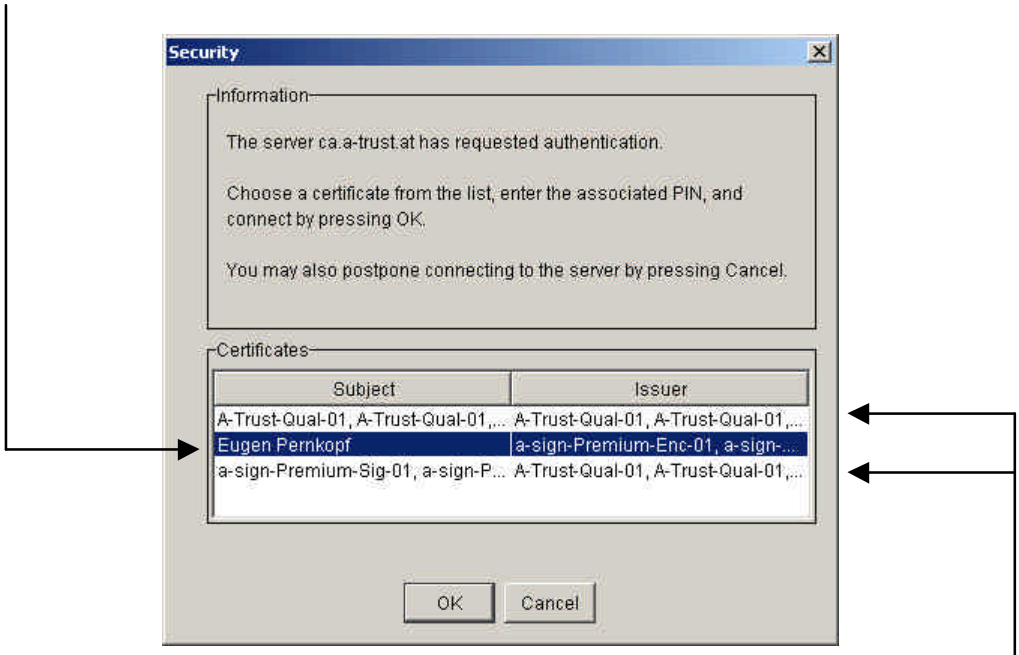
Aufbau der sicheren Verbindung:

Vor dem Starten des RA-Client die RO-Karte in den RO-Kartenleser stecken. – Die Karte ist nach ca. zehn Sekunden betriebsbereit, weil die Zertifikate aus dem Chip gelesen werden.

Adresse der ECHT-CA: **ca.a-trust.at (Verbindung nur mit Echtkarten)**
(Adresse der TRAININGS-CA: ca-train.a-trust.at (Verbindung nur mit Trainingskarten))



Die Zeile, die das Zertifikat des RO anzeigt, muss blau hinterlegt sein, dann „OK“.



(Wenn die RO-Karte eine a.sign premium ist, dann werden hier auch die Stammzertifikate angezeigt. Bei trust|sign ist dies nicht der Fall!)

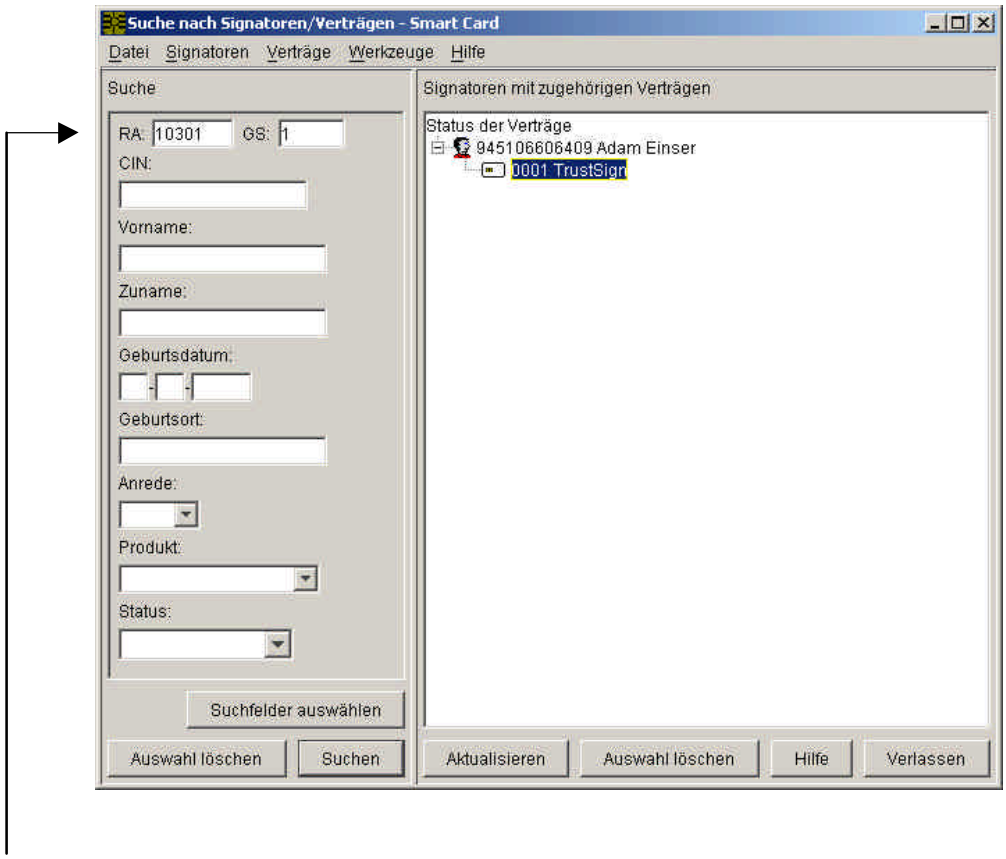
Jetzt den Kartenleser beachten und **GeheimhaltungsPIN (!!!) eingeben**

Die RO Karte muss während des gesamten Aktivierungsvorganges im Kartenleser bleiben, sonst wird die Verbindung/der Vorgang sofort unterbrochen!
Wenn der Verbindungsaufbau nicht möglich ist, muss der RO sich mit dem zRO oder seiner eigenen HOTLINE in Verbindung setzen. → Das Call Center der a.trust ist *für Kunden/Signatoren* zuständig.

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

Suche nach Signatoren/Verträgen:

Der RA-Client springt in den Screen „Suche nach Signatoren/Verträgen“:

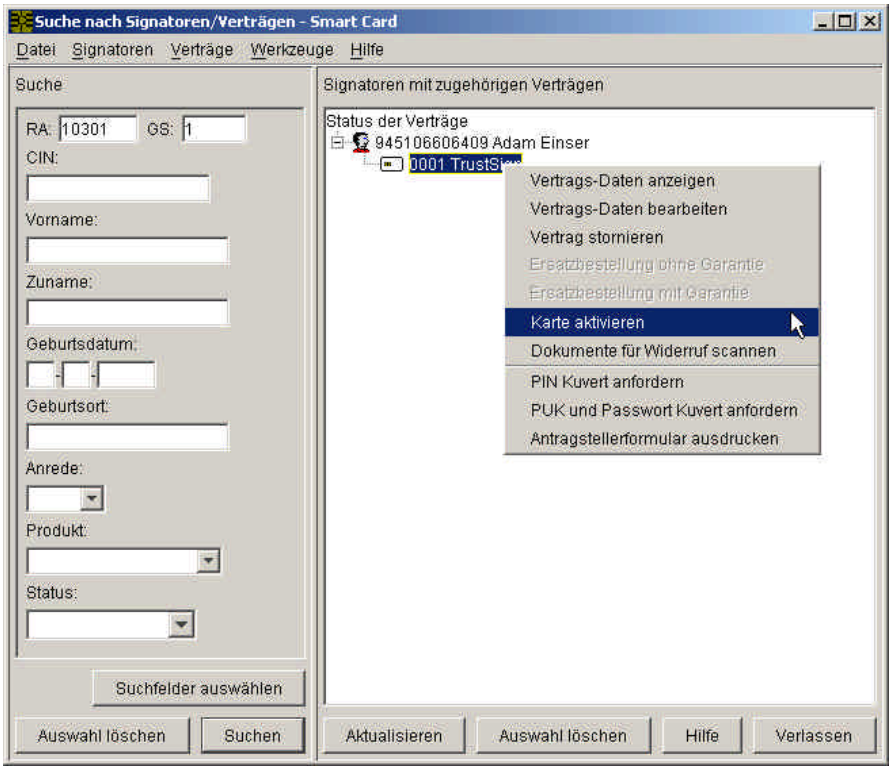


Falls eine Karte gesucht wird, die in einer anderen Filiale ausgestellt wurde, ist es notwendig, den Inhalt der Felder „RA“ und „GS“ vor dem Beginn der Suche zu löschen.

Zwei Möglichkeiten, einen Signator und seine(n) Verträge/Karte(n) zu finden:

- Die Signatorkarte in den Kunden-Kartenleser stecken: Damit liest der RA-Client die Transportzertifikate aus dem Chip und zeigt die betreffende Karte (weiß) an (ob. Abb.). Dieser Vorgang kann einige Sekunden dauern
- CIN (und/oder Namen) in die Suchefelder links eingeben und Button „Suchen“ klicken: Damit wird die Datenbank durchsucht und dann der Signator rechts angezeigt. Hier bleibt das Kartensymbol grau, bis man die Signator-Karte einsteckt. Nach ein paar Sekunden des Auslesens der Transportzertifikate springt das Kartensymbol in weiß über

Befehl: „Karte aktivieren“:



Nur im weißen Zustand (also bei eingesteckter Signator-Karte) ist der Befehl „Karte aktivieren“ anwählbar.

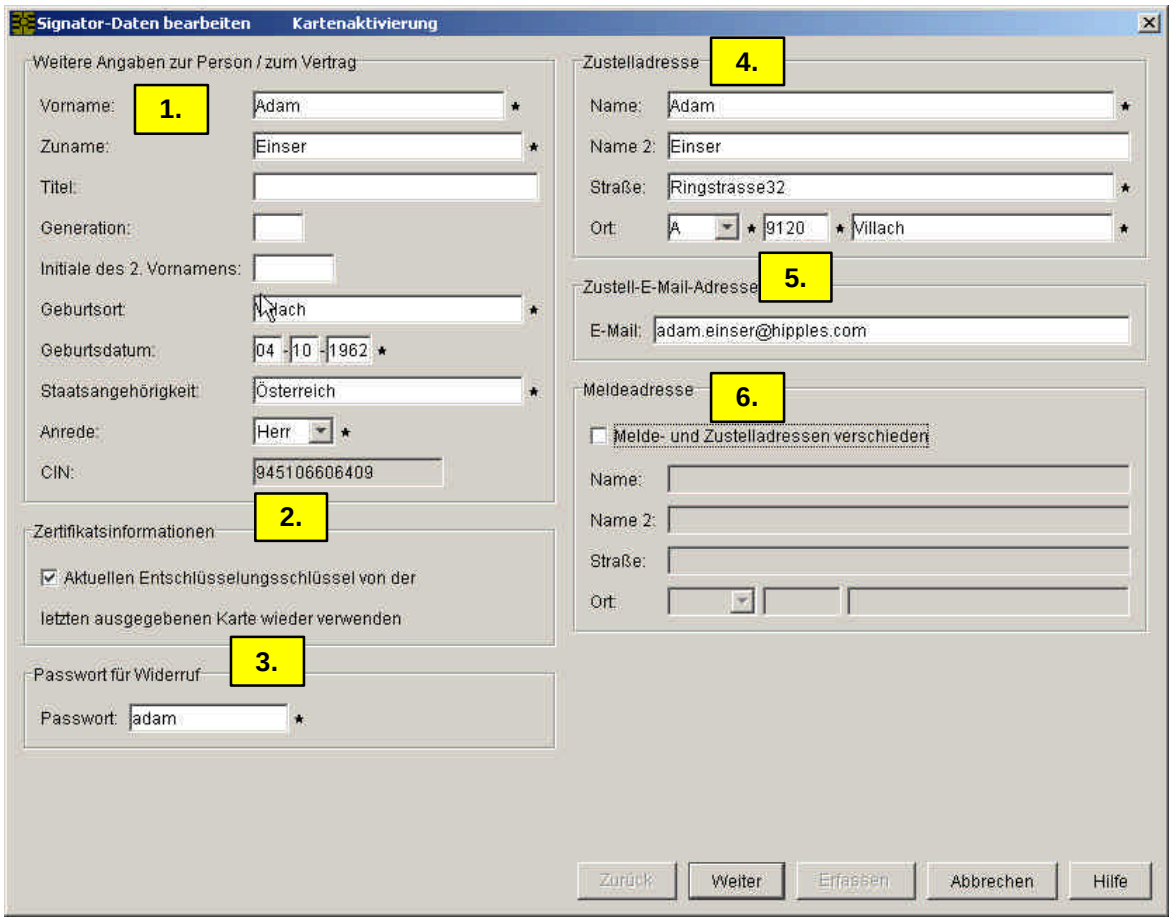
Zwei Wege zu diesem Menü:

- Rechtsklick auf die Karten- (= Vertrags)zeile (ob. Abb.)
- Karten- (= Vertrags)zeile markieren und „Verträge“ in der Menüleiste anklicken

Nach Auswahl des Befehls „Karte aktivieren“ erscheint der Screen „Signator-Daten bearbeiten“:

C) Kontrolle des Antrags

Screen „Signator Daten“:



Der Antrag auf das qualifizierte Zertifikat ist in der Signaturverordnung (§ 11 SigV) geregelt.

Die a.trust (und damit die RA als autorisierte Registrierungsstelle zur Durchführung des Zertifizierungsdienstes „Registrierung“) haftet für die Richtigkeit der Daten zum Zeitpunkt der Ausstellung des Zertifikats.

*In der Folge wird der **RA-Client Screen „Signator Daten bearbeiten“** besprochen:*

1. Weitere Angaben zur Person/zum Vertrag:

Der RO trägt in die Felder „Vorname“, „Zuname“, „Titel“, „Geburtsort“, „Geburtsdatum“ und „Anrede“ **nur jene Daten ein, die er gegen den vorgelegten Ausweis auch kontrollieren kann!**

Beispiel:

- Die Karte wurde von einem Herrn **Dr. Max Mustermann** bestellt
- Der vorgelegte Ausweis beinhaltet keinen Titel
- Im vorgelegten Ausweis ist „Max Jürgen“ als Vorname eingetragen

Daraus folgt:

- Der RO entfernt „Dr.“ aus dem Feld „Titel“
- Der RO ergänzt „Jürgen“ im Feld „Vorname“

Im Feld „Generation“ und „Initiale des 2. Vornamens“ werden KEINE EINTRÄGE gemacht.

Im Feld „Staatsangehörigkeit“ wird immer Österreich vorgeschlagen. Der RO ändert dies laut Angabe des Signators. Die Staatsangehörigkeit wird NICHT überprüft! (Ist im Führerschein z.B. gar nicht ersichtlich.)

2. Zertifikatsinformationen:

Die Verwendung eines Geheimhaltungsschlüssel-Paares auch auf anderen Karten hat den Sinn, dass man ein verschlüsselt abgelegtes Dokument später auch dann noch öffnen können will, wenn man bereits eine neuere Karte hat. Dazu muss natürlich auch auf der neueren Karte der passende Entschlüsselungsschlüssel vorhanden sein.

3. Passwort für Widerruf:

Der Zertifikatswerber legt schon bei der Bestellung sein persönliches Widerrufspasswort fest. Es besteht aus 4 bis 10 Zeichen, wobei Buchstaben und Ziffern möglich sind. Das Widerrufspasswort wird auch in das PUK-Kuvert gedruckt.

4. Zustelladresse:

Auf brieflichen Nachrichten an den Signator wird standardmäßig die Anrede (Herr oder Frau) mitgedruckt. Geben Sie daher den Namen des Signators immer in die erste Zeile und die etwaige Firmenbezeichnung in die zweite Zeile ein.

5. Zustell-E-Mail-Adresse:

Adresse für allfällige elektronische Nachrichten der a.trust an den Signator.

6. Meldeadresse:

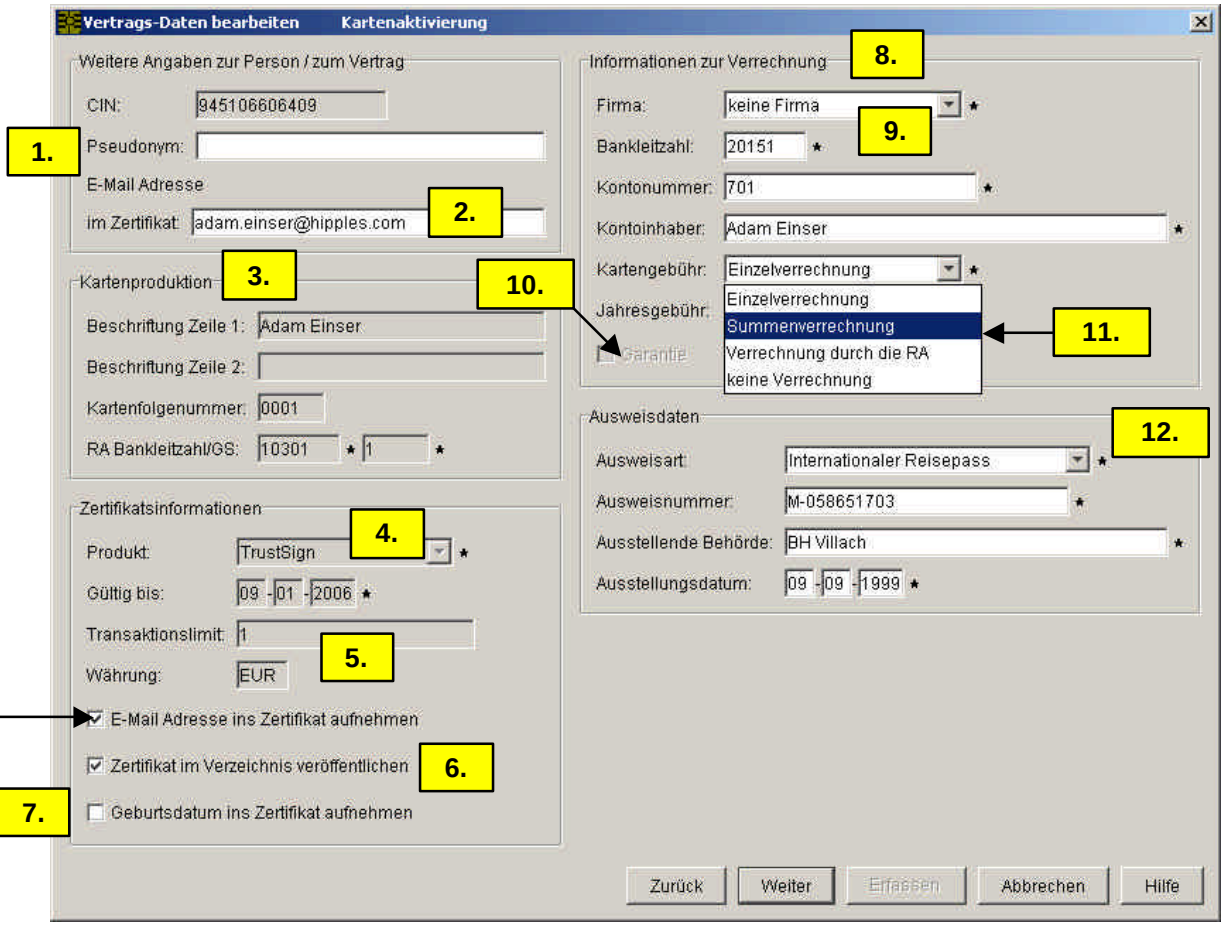
Die Meldeadresse wird derzeit in der Policy nicht behandelt und muss daher nicht erfasst werden.

Nach Kontrolle/Bearbeitung des Screens den Button „Weiter“ klicken.
Es erscheint der Screen „Vertrags-Daten bearbeiten“:

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

D) Kontrolle des Signaturvertrags und der kommerziellen Vereinbarungen

Screen „Vertrags-Daten“:



*In der Folge wird der **RA-Client Screen „Vertrags Daten bearbeiten“** besprochen:*

1. Pseudonym:

Laut SigG ist einem Signator die Verwendung eines Pseudonyms möglich. Tut er dies, so scheint im Zertifikat das Pseudonym (z.B. „Pseudonym: Ali Baba“), nicht aber sein Name auf. a.trust kennt den Namen hinter einem Pseudonym, legt es aber nur auf richterliche Aufforderung offen.

a.trust empfiehlt die Verwendung eines Pseudonyms nur in Ausnahmefällen. Dabei darf auf Grund der Verwechslungsgefahr nichts verwendet werden, das wie ein Vor- und Zuname verstanden werden könnte (Namensrecht).

2. E-Mail Adresse im Zertifikat:

Diese kann sich von der Zustell-E-Mail Adresse unterscheiden!

Die Aufnahme der E-Mail Adresse ins Zertifikat wird auf dem Screen „Vertrags Daten bearbeiten“ im Bereich „Zertifikatsinformationen“ durch Anklicken der entsprechenden Zeile entschieden.

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

Um ein Zertifikat in einem E-Mail Browser, wie MS Outlook oder Netscape Messenger, direkt auf Mails anzuwenden, brauchen diese Browser die Mailadresse zwingend im Zertifikatsinhalt.

Die E-Mail Adresse ist nicht im Sinne des SigG überprüfbar. Deshalb führt auch eine Änderung derselben nicht zur Widerrufspflicht. Allerdings kann man die neue E-Mail Adresse erst wieder in einem neuen Zertifikat eintragen.

3. Kartenproduktion:

Zur Beschriftung der Karte stehen 2 Zeilen à 24 Zeichen zur Verfügung, die nach Kundenwunsch genützt werden können. Die Beschriftung einer zur Abholung bereit liegenden Karte kann natürlich nicht mehr geändert werden.

Die 4stellige Kartenfolgenummer bildet zusammen mit der 12stelligen CIN die Kartennummer.

RA Bankleitzahl wird auch „RA Code“ genannt, weil Nicht-Banken unter den RAs eine 5stellige „fiktive“ Bankleitzahl erhalten. GS meint (Registrierungs-)Geschäftsstelle und wird auch „RA Branch“ genannt.

4. Produkt:

Je nachdem, welche Zertifikatsprodukte der a.trust die RA-Geschäftsstelle vertreiben darf, sind hier in der Auswahlbox die betreffenden Produktnamen aufgelistet.

Der Produktname einer zur Abholung bereit liegenden Karte kann natürlich nicht mehr geändert werden.

Die Auswahl des Produkts bei der Kartenbestellung bestimmt:

- qualifiziertes Signaturzertifikat mit ZMR Personenbingung (a.sign premium)
- qualifiziertes Signaturzertifikat (trust|sign)
- oder einfache Zertifikate (trust|mark)
- Aussehen der Karte (Layout, welche Logos, etc.)

5. Transaktionslimit und Währung:

Wenn kein Transaktionslimit eingetragen ist, dann ist die Haftung der a.trust bei trust|sign bzw a.sign premium Produkten nicht beschränkt.

Das Transaktionslimit ist eine Haftungsbeschränkung, die ein Zertifizierungsdiensteanbieter auf Grund des SigG in ein Zertifikat eintragen kann.

Die Höhe des Transaktionslimits in Euro sagt nichts über die Gültigkeit eines durch den Einsatz eines Zertifikats zustande gekommenen Rechtsgeschäfts aus. Egal, wie hoch das Transaktionslimit ist: Die digitale Signatur des Signators ist immer rechtsgültig.

Das Transaktionslimit ist nur dann von Bedeutung, wenn bei einem Rechtsgeschäft mit sicherer digitaler Signatur a.trust auf Grund eines technischen Fehlers in ihrem Bereich zur Haftung für einen Folgeschaden heran gezogen wird. Dann haftet die a.trust so, als ob das Rechtsgeschäft mit maximal dem im Transaktionslimit festgeschriebenen Betrag abgeschlossen worden wäre.

6. Zertifikat im Verzeichnis veröffentlichen:

Das SigG stellt dem Signator frei, ob er sein Zertifikat im Verzeichnisdienst der a.trust veröffentlichen lassen will.

Die Veröffentlichung erleichtert Kommunikationspartnern die Signaturprüfung, weil jedermann nachsehen kann, ob das hinter einer Signatur stehende Zertifikat tatsächlich mit dem Zertifikat im Verzeichnis der a.trust übereinstimmt (Teil der Signaturprüfung). Wenn das Zertifikat nicht im Verzeichnis ist und die Applikation oder der Signator das Zertifikat nicht mit der Signatur mitschickt, dann ist dem Empfänger die Signaturprüfung nicht möglich. Damit liegt keine gültige digitale Signatur vor.

Für die Geheimhaltung hat die Veröffentlichung den Vorteil, dass sich jeder den öffentlichen Schlüssel des Signators für die Verschlüsselung aus dem Verzeichnis besorgen kann. Ist dies nicht der Fall, muss der Signator demjenigen, der ihm eine verschlüsselte Nachricht schicken will, vorher sein Zertifikat selber übermitteln.

7. Geburtsdatum ins Zertifikat aufnehmen:

Erwachsenen steht diese Entscheidung frei.

Bei Minderjährigen zwischen 14 und 18 Jahren (Jüngeren stellt a.trust keine Zertifikate aus) ist das Geburtsdatum im Zertifikat Pflicht: Dies ist der Hinweis für Signaturempfänger, dass der Signator auf Grund seiner nicht erreichten Volljährigkeit nur beschränkt Geschäftsfähig ist.

Der RA-Client übernimmt das Geburtsdatum von Minderjährigen automatisch in das Zertifikat.

8. Informationen zur Verrechnung:

Prinzipiell werden die Karten- und Zertifikatsgebühren dem Signator durch Bankeinzug verrechnet. Dazu gibt er seine **Kontoverbindung** (BLZ, Kto.Nr., Kto.Wortlaut) bekannt und unterzeichnet am Signaturvertrag die entsprechende **Einzugsermächtigung**.

Auf dem Kontoauszug werden die eingezogenen Gebühren mit Netto-, USt- und Bruttobetrag ausgewiesen.

Der Signator hat zwei Möglichkeiten zu entscheiden, wie die Kartengebühr(en) und die Zertifikatsgebühren eingezogen werden:

- Bei der **Einzelverrechnung** wird jede Gebühr mit zugehöriger CIN in einer eigenen Buchungszeile ausgewiesen
- Bei der **Summenverrechnung** werden alle Gebühren einer Fälligkeitsperiode in einer Buchungszeile zusammen gefasst. Es ist NICHT ausgewiesen, auf welche einzelnen Karten/Zertifikate sich die Gebühren beziehen

Die RA hat die Möglichkeit zu entscheiden, ob sie bestimmten Personen unter ihren Kunden andere Verrechnungsarten anbieten will. Diese Entscheidung wird RA-intern gefällt und dem RO mitgeteilt. In diesem Fall wählt der RO **Verrechnung durch die RA** aus und trägt jenes Konto ein, das von der RA für den Bankeinzug durch a.trust vorgesehen wurde.

9. Firma:

„Firma“ an dieser Stelle bedeutet, dass a.trust mit Unternehmen oder Organisationen einen Vertrag über die Ausgabe von Zertifikaten und die Verrechnung der Gebühren vereinbaren kann.

Diese Unternehmen/Organisationen sind dann „Firmenkunden“ der a.trust, die als „Kommerzieller Vertragspartner“ in die Signaturverträge zwischen a.trust und den einzelnen Signatoren eintreten.

Der RO muss nicht die speziellen Daten dieser Verträge kennen und eingeben, sondern bloß die „Firma“ in der Auswahlbox des RA-Client auswählen.

Am Signaturvertrag muss die Firma unterschreiben, dass der Signator ein Zertifikat im Rahmen dieses Firmenvertrags ausgestellt bekommen darf. Der RO kontrolliert, dass die firmenmäßige Zeichnung des Kommerziellen Vertragspartners am Signaturvertrag vorhanden ist.

10. Garantie:

Für die a.trust-Produkte gelten natürlich die gesetzlichen Bestimmungen zur Gewährleistung. Defekte Karten werden innerhalb der gesetzlichen Zweijahresfrist ausgetauscht, wobei diese Vorgehensweise einzuhalten ist:

- Der Signator muss dem RO die defekte Karte aushändigen (Das vermeidet eine „Garantiebestellung“ bei Verlust einer Karte)
- Der RO überprüft im Zertifikatsinhalt (Gültigkeitsdauer), ob die Zertifikate nicht schon älter als zwei Jahre sind (Verzeichnisdienst auf der a.trust Homepage)
- Dann überprüft der RO im RA-Client, dass die Zertifikate auf der betreffenden Karte bereits Widerrufen sind (roter Kartenstatus)
- Wenn nein, muss DER SIGNATOR den Widerrufsdienst anrufen
- Wenn ja, kann der RO eine „Ersatzbestellung mit Garantie“ durchführen
- Der RO zerstört den Chip der widerrufenen Karte und entsorgt die Karte

11. Unbefristeter Vertrag:

Signaturverträge können befristet oder unbefristet geschlossen werden.

Unbefristete Verträge sind erstrebenswert. Vor allem wegen der automatischen Zertifikatserneuerung vor Ablauf des Zertifikats durch a.trust („Verlängerung“ der Karte).

Der Aufwand bei befristeten Verträgen ist für *alle* Beteiligten größer: Der Signator muss bei Zertifikatserneuerung aktiv werden. a.trust und RA haben ebenfalls administrativen Mehraufwand.

Ein Vertrag beginnt mit der Übergabe der Karte zu laufen. Ein trust|sign bzw. a.sign premium Zertifikat ist lt. SigG maximal (sekunden-)genau drei Jahre lang gültig, dann muss es verlängert werden. D.i. eine sogenannte Zertifikatserneuerung, an die der Signator vor Ablauf des Zertifikats von a.trust erinnert wird.

Die Zertifikatserneuerung ist nur möglich bei einem gültigen Zertifikat und bei einem gültigen Vertrag, das heißt, wird darauf vergessen oder die Gültigkeit auch nur minimal überschritten, muss eine neue Karte gekauft werden. Deshalb ist es aus Signatorsicht sinnvoll, den Vertrag „unbefristet“ abzuschließen. Auch dann wird der Signator an den Ablauf des Zertifikats erinnert, braucht aber nicht selbst verlängern, sondern das geschieht automatisch durch a.trust. Natürlich kann man auch den unbefristeten Vertrag jederzeit stornieren. Man kann beim Storno einen Stichtag angeben oder wahlweise mit Jahresende stornieren, weil bereits eingezogene jährliche

Zertifikatsgebühren nicht zurück erstattet werden. Der Widerruf des Zertifikats geschieht bei Storno eines Vertrags automatisch durch a.trust.

12. Ausweisdaten:

Hinweis zum österreichischen Führerschein:
Die Ausweisnummer ist immer im Bereich der persönlichen Daten und des Lichtbildes zu finden. Ältere Exemplare haben auch auf der Vorderseite eine Nummer. Dabei handelt es sich um die Seriennummer der Formulargattung „Führerschein“ und daher nicht um die zu erfassende Ausweisnummer.

Nach Kontrolle/Bearbeitung des Screens den Button „Weiter“ klicken.

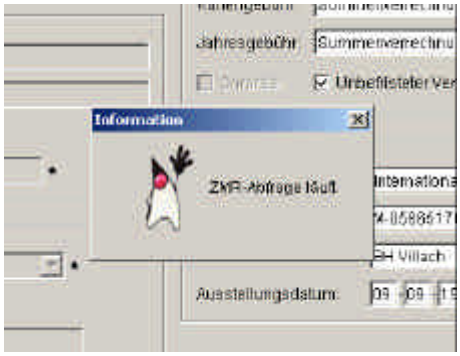
Automatische ZMR (= Zentrales Melderegister) Abfrage bei a.sign premium :

Hintergrund:
a.sign premium unterstützt die „Bürgerkartenfunktionalität“ für das e-Government.

Die Bürgerkartenfunktionalität verlangt zusätzlich zu den Signaturfunktionen der Karte die Verbindung zwischen den Zertifikaten und der ZMR-Nummer jedes Bürgers. Man spricht von der „ZMR-Personenbindung“.

Dabei wird die ZMR-Nummer des Signators mit den öffentlichen Schlüsseln seiner a.sign premium Karte verbunden, diese Verbindung vom ZMR digital signiert und dann auf den Chip der Karte geladen.

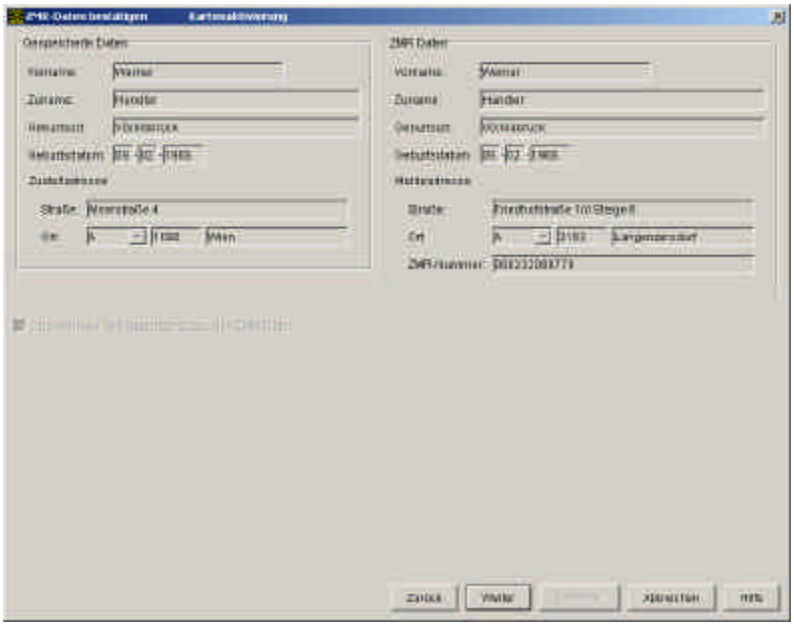
Vorgehensweise:
Nach der Kontrolle der Vertragsdaten durch den RO und dem Klick auf „Weiter“ startet die Registrierungssoftware bei a.sign premium eine ZMR Abfrage. Dabei wird automatisch der Vorname, der Zuname, das Geschlecht und das Geburtsdatum des Signators an das ZMR geschickt.



Dieser Vorgang dauert einige Sekunden. Nur wenn die Abfrage eindeutig ist, gibt es eine positive Rückmeldung.

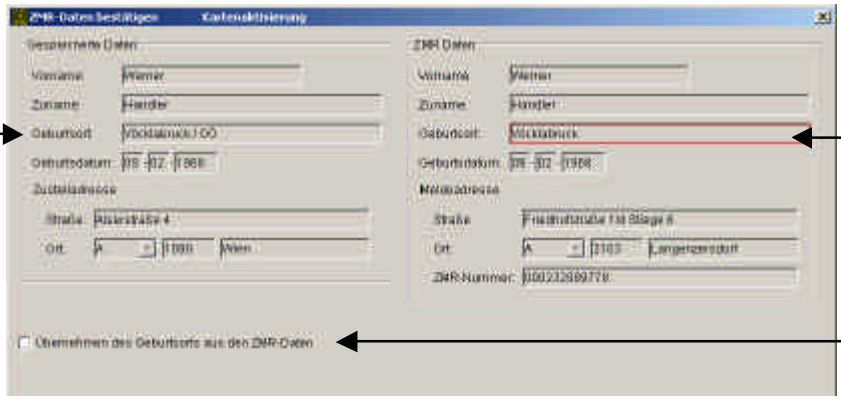
Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

Wenn die ZMR-Abfrage ein positives Ergebnis liefert, werden die Daten wie folgt angezeigt:



Sollte der Signator seine ZMR Daten sehen wollen, so kann der RO ihm den Bildschirm zeigen oder ihm die Daten vorlesen.
Der RO klickt dann den Button „Weiter". → Registrierungshandbuch, Überschrift „Antragstellerformular ausdrucken".

Wenn der Geburtsort laut ZMR Daten rot umrandet ist, dann weicht die **Schreibweise** des Geburtsorts im ZMR von der im vorgelegten Ausweis ab (z.B. „St. Pölten" = „Sankt Pölten").



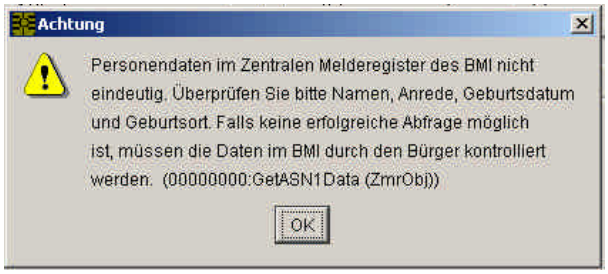
Die Daten aus dem Ausweis haben für den Signaturvertrag IMMER Priorität!
Der RO aktiviert deshalb **NIE** den Punkt „Übernehmen des Geburtsorts aus den ZMR-Daten"!

Sollte der Geburtsort gänzlich anders lauten, dann ist die Kartenaktivierung abzubrechen, da sonst eine falsche ZMR-Personenbindung erstellt wird!

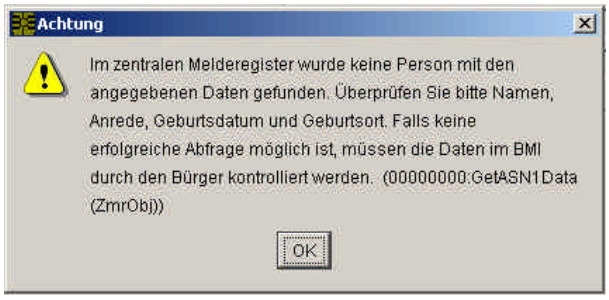
→ Der RO informiert den Kunden laut Merkblatt des BMI, die ZMR Daten richtig stellen zu lassen. Dann kann ein neuer Termin für die Registrierung vereinbart werden.

Mögliche Fehlermeldungen:

Fehlermeldung 1 erscheint, wenn **kein eindeutiger Eintrag im Melderegister** mit den Daten des Antragstellers gefunden werden kann:



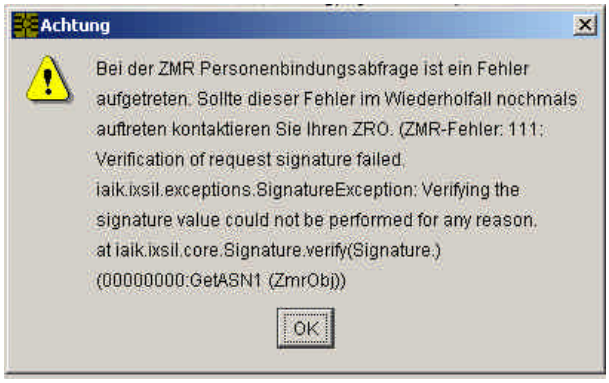
Fehlermeldung 2 erscheint, wenn **gar kein Eintrag im Melderegister** mit den Daten des Antragstellers gefunden werden kann:



Der RO klickt in diesen Fällen „OK“ und in den darauf erscheinenden Screens „Zurück“, um erneut die erfassten Signator-Daten (Vorname, Zuname, Anrede, Geburtsdatum und Geburtsort) anhand des Ausweises zu kontrollieren.
Sollten Datenänderungen laut Ausweis notwendig sein, ist die Kartenaktivierung ab dem Screen „Signator Daten“ zu wiederholen.

Falls wieder keine erfolgreiche Abfrage möglich ist: → Registrierungshandbuch, Überschrift „Weiteres Vorgehen nach der Fehlermeldung 1 oder 2“

Fehlermeldung 3 erscheint, wenn im ZMR (am Server des Bundesministeriums für Inneres) oder in der Verbindung zum ZMR **technische Probleme** bestehen:



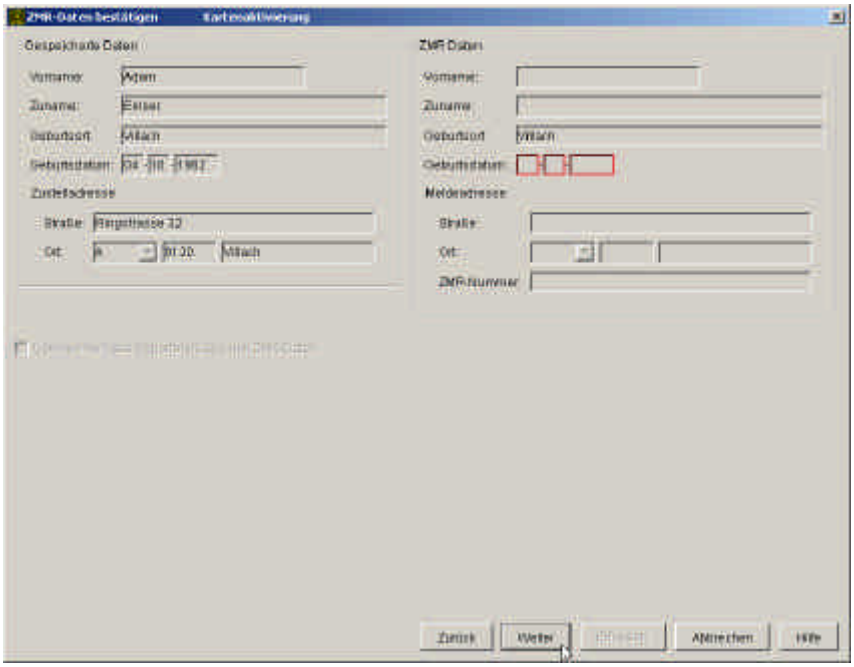
Der RO klickt „OK“ und im darauf erscheinenden Screen „Zurück“. Jetzt startet ein Klick auf „Weiter“ die erneute ZMR-Abfrage.

Falls der Fehler nach mehreren Wiederholungen noch immer auftritt, informieren Sie Ihren zRO. → Registrierungshandbuch, Überschrift „Weiteres Vorgehen nach der Fehlermeldung 3“

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

Weiteres Vorgehen nach der Fehlermeldung 1 oder 2:

Nach dem Drücken des Buttons „OK“ unter Fehlermeldung 1 oder 2 erscheint dieser Bildschirm:



Der RO hat nun diese beiden Möglichkeiten:

Möglichkeit 1:
Kunde will Zertifikate und verzichtet zum jetzigen Zeitpunkt auf ZMR Personenbindung.

Der RO erklärt dem Kunden die weitere Vorgehensweise laut „***Merkblatt des BMI***“, um die ZMR-Daten bei der Meldebehörde richtig stellen zu lassen und händigt dieses Merkblatt aus.

Der RO setzt dann mit der Überschrift „Antragstellerformular ausdrucken“ fort. Somit wird jetzt keine ZMR Personenbindung auf die Karte geschrieben. Die Karte hat dann zwar gültige Zertifikate, aber keine Bürgerkartenfunktion.

Der RO händigt dem Kunden zusätzlich das Dokument „**a.sign premium *Kundeninformationen***“ aus.
Auf diesem befindet sich unter anderem die Information, dass sich der Signator über die Homepage der a.trust auf seine gültige a.sign premium Karte online die ZMR Personenbindung selbst aufbringen können wird. Das entsprechende Tool wird es im Sommer 2003 geben.

Möglichkeit 2:
Kunde will kein Zertifikat ohne ZMR Personenbindung

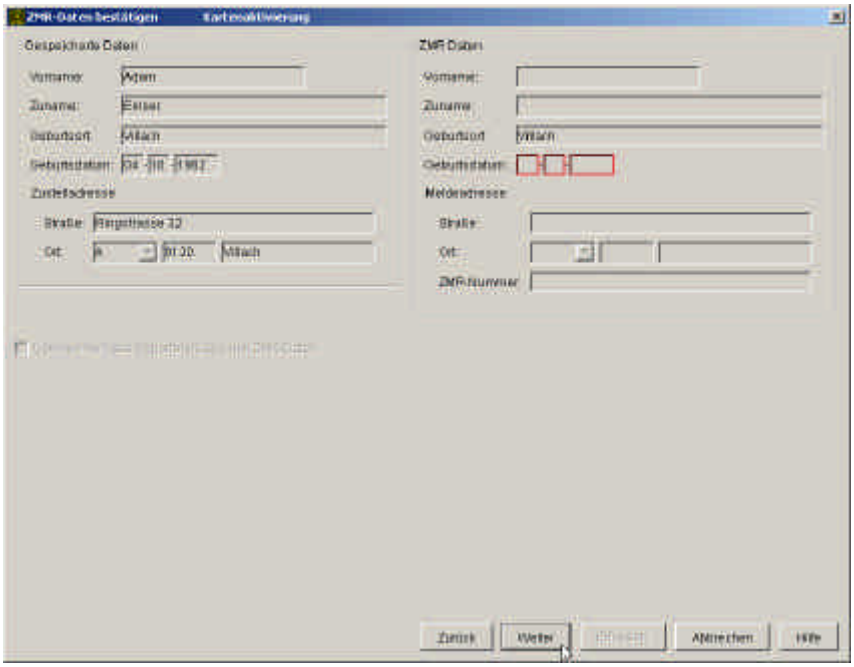
Der RO bricht die Registrierung ab, erklärt dem Kunden die weitere Vorgehensweise laut „***Merkblatt des BMI***“, um die ZMR-Daten bei der Meldebehörde richtig stellen zu lassen und händigt dieses Merkblatt aus.

Der RO macht den Kunden darauf aufmerksam, dass er nach der Änderung seiner ZMR Daten einen neuen Termin zur Kartenabholung machen soll.

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

Weiteres Vorgehen nach der Fehlermeldung 3:

Nach dem Drücken des Buttons „OK“ unter Fehlermeldung 3 erscheint dieser Bildschirm:



Der RO hat nun diese beiden Möglichkeiten:

Möglichkeit 1:
Kunde will Zertifikate und verzichtet zum jetzigen Zeitpunkt auf ZMR Personenbindung.

Der RO setzt mit der Überschrift „Antragstellerformular ausdrucken“ fort. Somit wird jetzt keine ZMR Personenbindung auf die Karte geschrieben. Die Karte hat dann zwar gültige Zertifikate, aber keine Bürgerkartenfunktion.

Der RO händigt dem Kunden zusätzlich das Dokument „**a.sign premium *Kundeninformationen***“ aus.
Auf diesem befindet sich unter anderem die Information, dass sich der Signator über die Homepage der a.trust auf seine gültige a.sign premium Karte online die ZMR Personenbindung selbst aufbringen können wird. Das entsprechende Tool wird es im Sommer 2003 geben.

Möglichkeit 2:
Kunde will kein Zertifikat ohne ZMR Personenbindung

Der RO bricht die Registrierung ab und vereinbart mit dem Kunden einen neuen Termin zur Kartenabholung.

Antragstellerformular ausdrucken:

Sollten an den Daten in den beiden letzten Screens **irgendwelche Änderungen** vorgenommen worden sein, so ist das **Antragstellerformular** (Seite 1 = Antrag; Seite 2 = Signaturvertrag) **jedenfalls neu zu drucken!**

(**Wenn nicht**: Button „Weiter“ klicken, um das Druckprogramm zu überspringen.)

Hier das Druckersymbol links oben klicken (es erscheint dann ein Standard-Druckfenster):

Als Belegexemplar für den Signator kann hier das Antragstellerformular auch doppelt ausgedruckt werden. **Der Nachdruck des Antragstellerformulars ist bei einer aktivierten Karte nicht mehr möglich!**
Das Druckprogramm nach dem Ausdruck durch einfaches Schließen dieses Fensters beenden.

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

E) Belehrung im Sinne des Signaturgesetzes

Der RO muss dem Signator an dieser Stelle des Registrierungsablaufs folgendes mitteilen:

„Wir sind nun Ihre Antrags- und Vertragsdaten durchgegangen. Sie haben mit Ihrem Kartenabholbrief das Merkblatt für die Abholung eines* trust|sign bzw. a.sign premium *Zertifikats zugeschickt bekommen. Darin finden Sie die Auflistung Ihrer Pflichten als Signator nach dem Signaturgesetz und einen Text, der Ihnen erklärt, worauf Sie als Signator achten müssen, damit ein Missbrauch Ihres Signaturzertifikats durch andere ausgeschlossen ist.

Bitte halten Sie sich als Signator zu Ihrer eigenen Sicherheit an diese Empfehlungen und Hinweise. Sie bestätigen dies auch durch Ihre Unterschrift am Signaturvertrag.“

F) Unterzeichnen des Antrags und des Signaturvertrags

Unterschrift des Signators auf Seite 1 des Antragstellerformulars (ANTRAG)

Bestätigung der Richtigkeit und Vollständigkeit der Daten der Identifizierung und der Zertifikatsdaten durch den Signator (wird vom SigG verlangt).

Alle nicht mehr änderbaren Daten sind am Bildschirm grau unterlegt! Sollte in nicht änderbaren Daten (z.B. Kartenbeschriftung) Fehler behoben werden müssen, muss eine neue Bestellung durchgeführt werden. Die Karte mit den falschen/fehlerhaften Daten muss vernichtet, anschließend mit Hilfe des RA-Clients storniert und eine Zusatzbestellung durchgeführt werden.

Sollten Änderungen der Einträge vorgenommen worden sein, ist vom Signator das neuerlich ausgedruckte Formular zu unterschreiben.

Unterschrift des Signators auf Seite 2 des Antragstellerformulars (SIGNATURVERTRAG)

Mit der Unterschrift unter den Signaturvertrag bestätigt der Signator zwei Dinge:

- Den Erhalt des Kartenabholungsbriefs mit Merkblatt und PIN-/PUK-Kuverts und den Erhalt der trust|sign bzw. a.sign premium Karte
- Die Kenntnisnahme der Vertragsdokumente, der Vertragsbedingungen und der gesetzlich vorgeschriebenen Belehrung

Gleichzeitig muss auch der kommerzielle Aspekt des Signaturvertrags erfüllt werden:

Die Einzugsermächtigung muss durch den am Konto *Zeichnungsberechtigen* erfolgen. Ist der Signator nicht selbst der Zeichnungsberechtigte, weil etwa die Verrechnung der Gebühren über ein Firmenkonto erfolgen soll oder z.B. der Ehegatte das Konto zur Verfügung stellt, so muss die Einzugsermächtigung von entsprechend anderen unterzeichnet sein.

Bei *Firmenkunden* wird an Stelle der Einzugsermächtigung am Antragstellerformular unter dem Titel „Kommerzieller Vertragspartner“ die rechnungsbeziehende Firma angedruckt. Der Signator muss die entsprechende firmenmäßige Zeichnung des Kommerziellen Vertragspartners am Signaturvertrag mitbringen.

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

G) Archivierung der Dokumente und Ausstellung der Zertifikate

Der Signator muss das letztgültige, allenfalls neu ausgedruckte Antragstellerformular unterschreiben, weil der RO die Dokumente mit den Originalunterschriften archivieren muss!

Beim Scan eines Ausweises für die elektronische Archivierung ist jene Seite relevant, auf der sich das Lichtbild des Signators befindet. Sollten bei Ausweisen persönliche Daten auch auf der **Rückseite** stehen (z.B. Personalausweis in Kartenform), so ist diese selbstverständlich zu kontrollieren, sie braucht jedoch nicht gescannt oder kopiert werden.

Beim Scan der beiden Seiten des Antragstellerformulars ist darauf zu achten, dass die ***Originalunterschriften*** gescannt werden.

Beim Scannen aller Dokumente überprüft der RO die Erkennbarkeit des Lichtbildes und die Leserlichkeit der Unterschriften auf dem Bildschirm.

Nach dem Scannen der Dokumente

- Gibt der RO den Ausweis zurück
- Behält der RO das Antragstellerformular mit den Originalunterschriften und legt diese ab
- Übergibt der RO dem Signator den Zweitausdruck des doppelt ausgedruckten Antragstellerformulars oder eine Kopie des Originals

Nach dem Scannen werden die Bilder vom RO signiert und an das elektronische Archiv der a.trust gesendet. Zu diesem Zeitpunkt muss der RO die Belehrung durchführen.

Das elektronische Archiv befindet sich im hochsicheren Rechenzentrum der a.trust. Die Dokumente im elektronischen Archiv müssen von a.trust 33 Jahre lang aufbewahrt werden.

Die Ablage der Antragstellerformulare mit den Originalunterschriften erfolgt chronologisch in einem Ordner. Sie werden vier Jahre lang in der RA aufbewahrt.

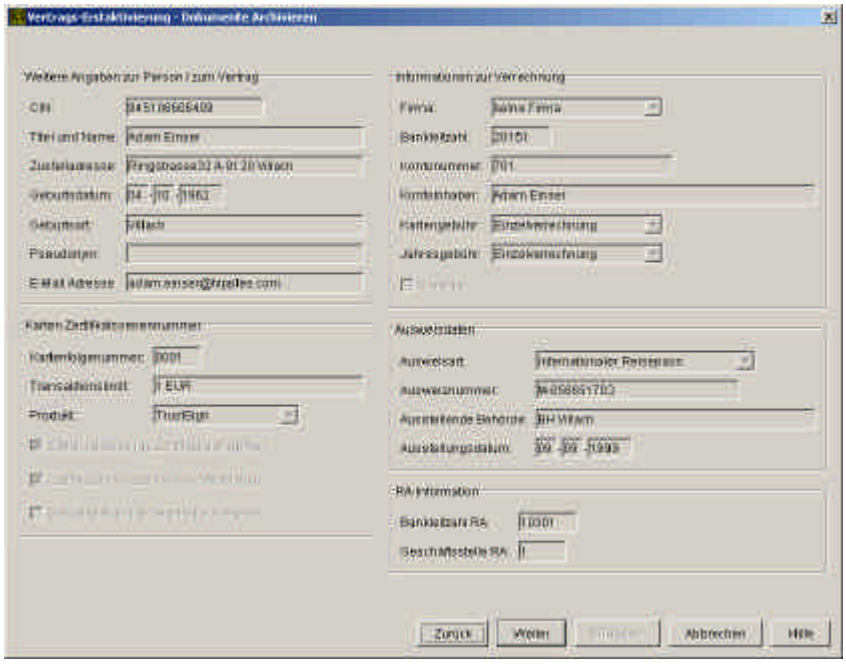
Änderungen im Antragstellerformular bei „Kommerziellem Vertragspartner“:

Auf Seite 1 (Antrag) muss immer der Signator unterschreiben. Somit gibt es kein Problem beim Neuausdruck des Antragstellerformulars.
Sollte bei Firmenkunden eine Änderung den Neuausdruck des Antragstellerformulars notwendig machen, so ist auch die „alte“ Seite 2 (Signaturvertrag) mit der firmenmäßigen Zeichnung des Kommerziellen Vertragspartners im Ordner abzulegen. Gleiches gilt für die Einzugsermächtigung, wenn der Signator nicht der zeichnungsberechtigte Kontoinhaber ist.

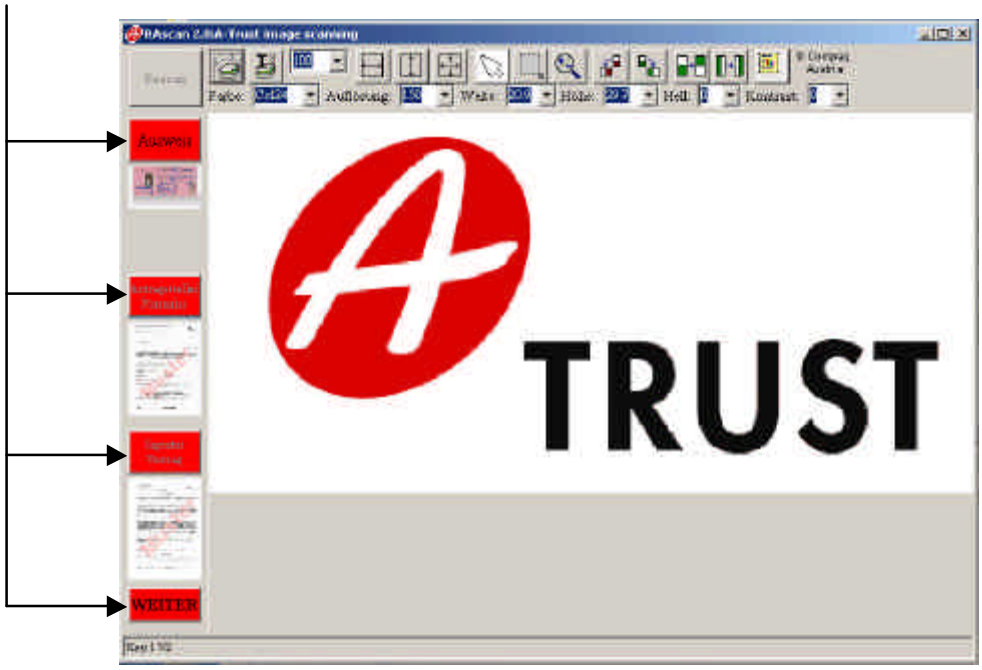
Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

Elektronische Archivierung:

Zum Scan-Programm (elektronische Archivierung) kommt man, indem man hier den Button „Weiter“ klickt:

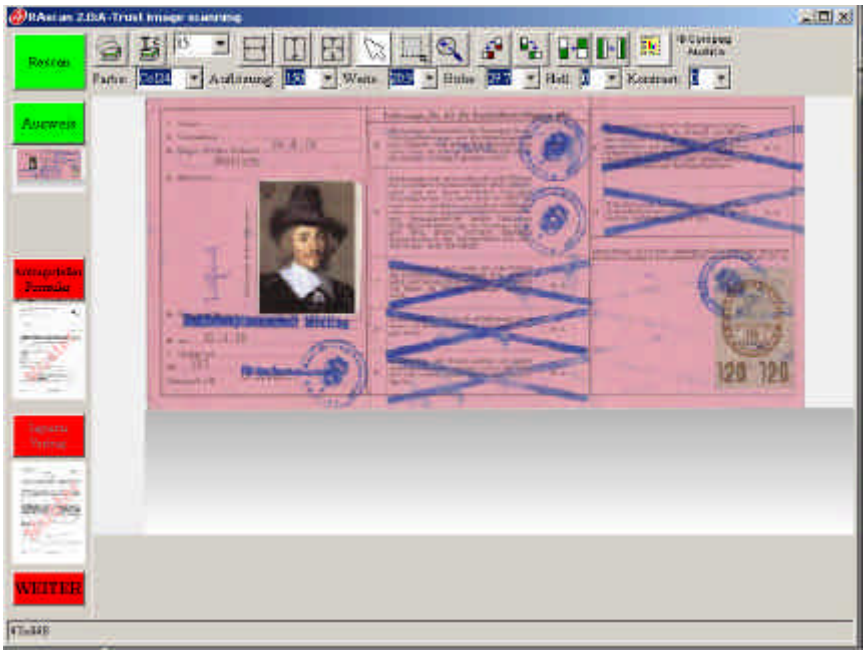


Es öffnet sich das „RA-Scan“-Programm, dessen (noch rote) Buttons der RO von oben nach unten durcharbeitet:

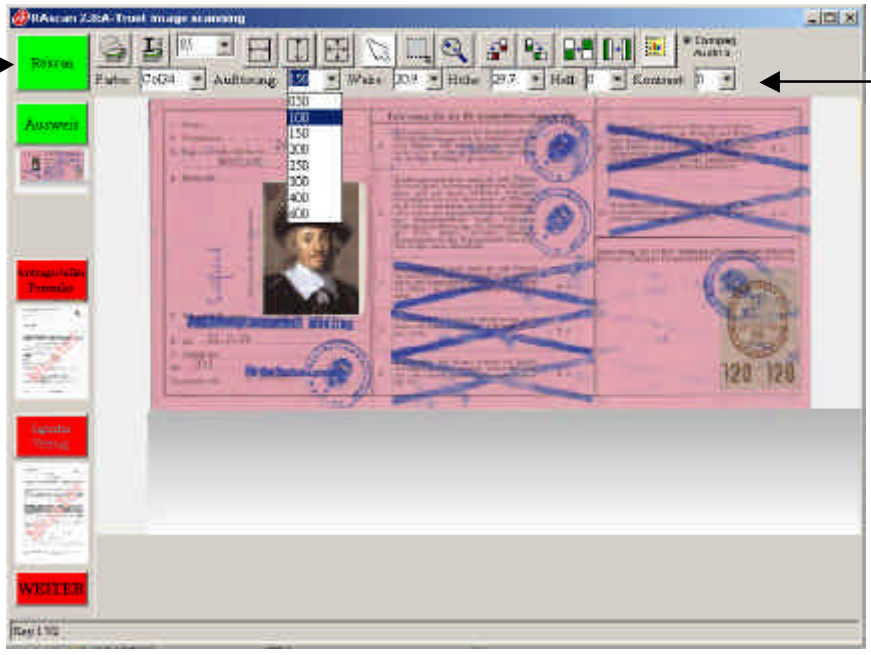


Button „**Ausweis**“: Originaldokument scannen
Button „**Antrag**“: Antragstellerformular Seite 1 (mit **Originalunterschrift** scannen)
Button „**Signaturvertrag**“: Antragstellerformular Seite 2 (mit **Originalunterschriften** sc.)

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.



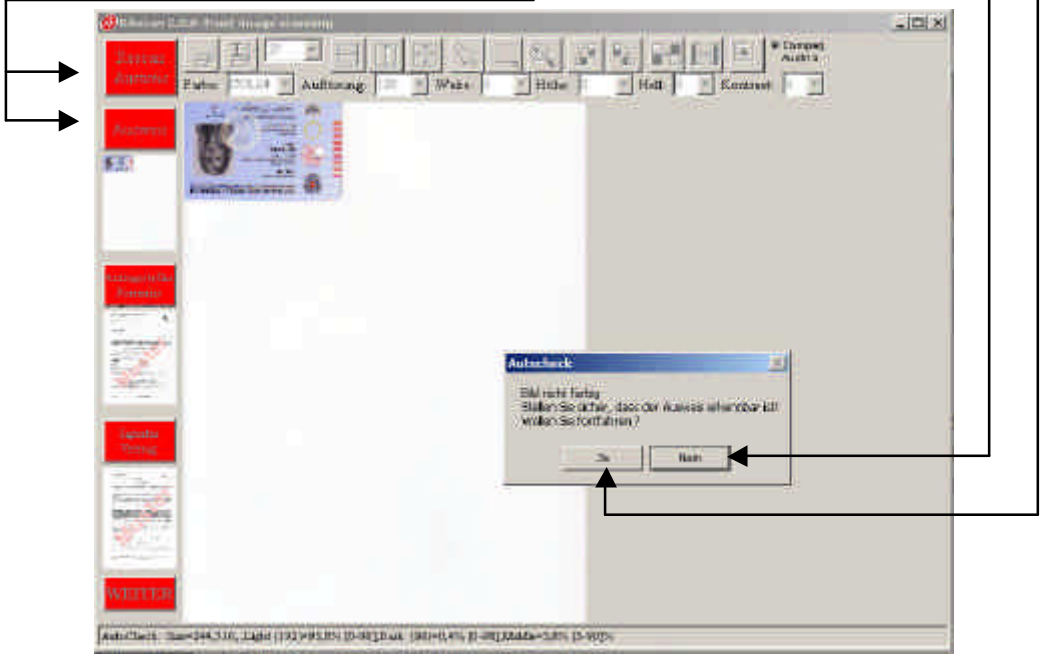
Nach dem jeweiligen Scan mit dem Standard-Button sind in der Kopfzeile die Einstellungen änderbar (Bsp. unten: „Auflösung“).
Um mit **geänderten Einstellungen** neuerlich zu scannen, ist der **oberste Button „Rescan“ zu klicken**, der nach dem Klick auf „Ausweis“ ebenfalls grün wurde:



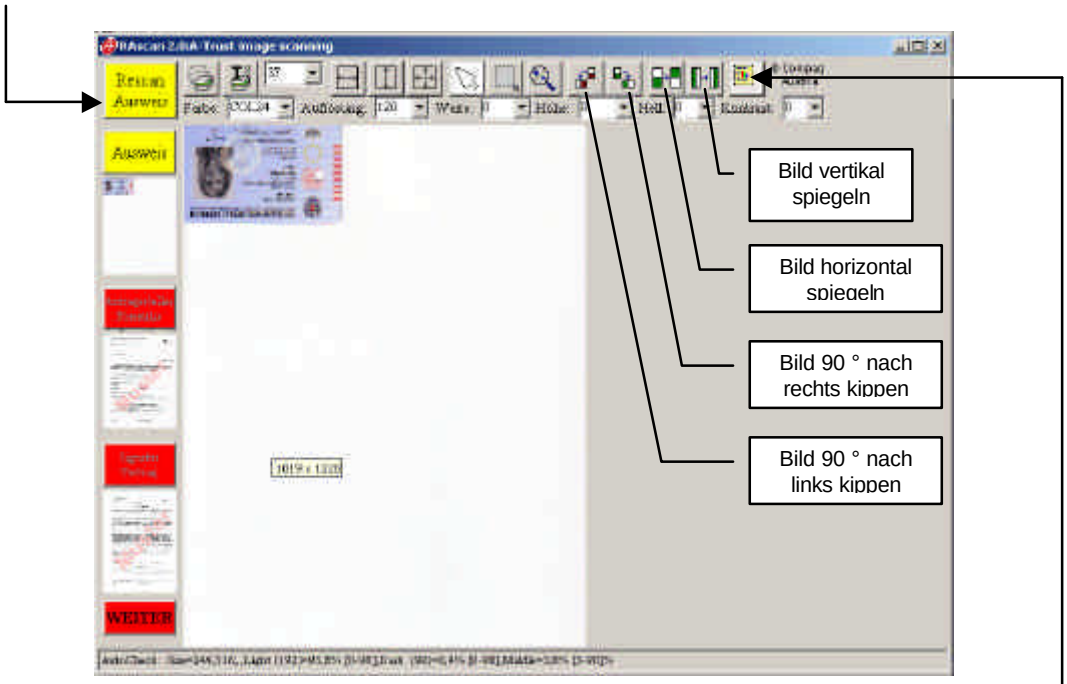
Der RO hat in der oberen Symbolleiste diverse Tools, mit denen er die **Lesbarkeit der Scans überprüfen muss** (auch die Unterschriften des Signators!). Eine kleinere Auflösung z.B. darf nicht auf Kosten der Lesbarkeit gehen, kann aber die Bildübertragung ebenso beschleunigen, wie das Abschneiden überflüssigen weißen Randes um den Ausweis.

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

Sollte der Button nicht grün werden, so gibt der grobe Autocheck des Programmes von sich aus einen Warnhinweis und fragt „Wollen Sie fortfahren?“. **Der RO prüft den Scan nochmals optisch!**
Scan ist in Ordnung, nicht noch mal scannen (Button soll grün werden) Klick auf „Ja“
Scan ist nicht in Ordnung, noch mal scannen (Button soll gelb werden) Klick auf „Nein“



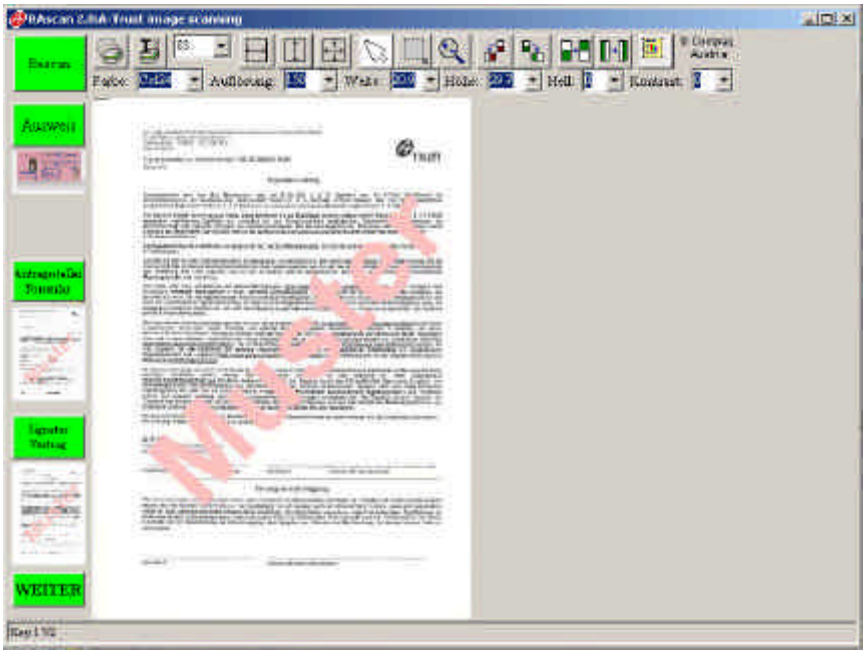
Der RO unternimmt seine Änderungen und klickt dann auf den gelben Button „Rescan Ausweis“.



Mit dem Symbolbutton ganz rechts kann der RO durch mehrmaliges Klicken überflüssigen weißen Rand um den Ausweis ausschneiden.
Der kopfüber gescannte Ausweis kann durch 2x „Bild 90° kippen“ in die richtige Lage gebracht werden.
Die nächste Abbildung zeigt das Ergebnis dieser Korrekturen.

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

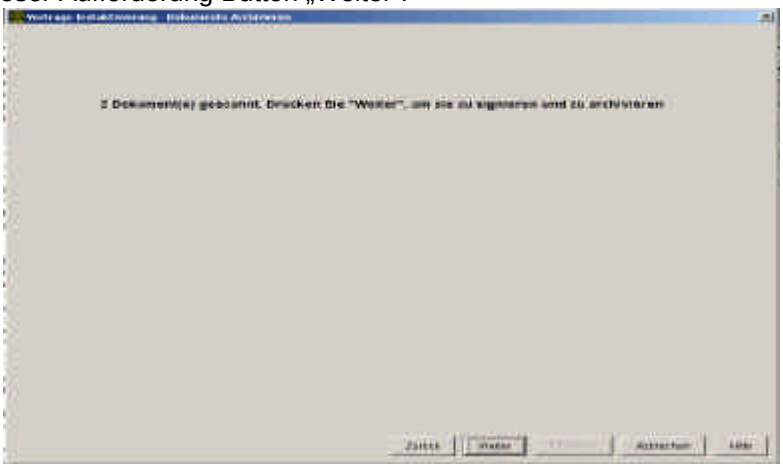
Nach den erfolgreichen Scans (alle Buttons grün): Scan-Programm mit Button „WEITER“ beenden:



Es erscheint eine Info über die Größe der gescannten Bilder, aus der sich ableiten lässt, wie lange die Bildübertragung in das Rechenzentrum der a.trust ungefähr dauern wird:

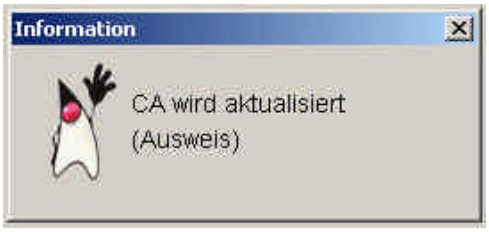
Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

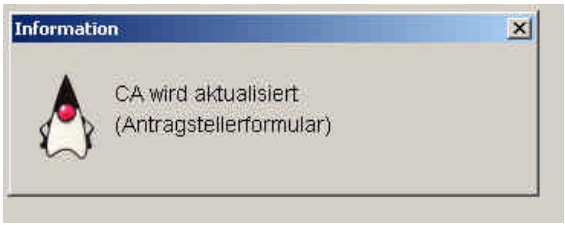
Entsprechend dieser Aufforderung Button „Weiter“:



Der RO signiert ZWEI MAL mit seiner SignaturPIN (!!!):
1 x Ausweis und 1 x Antragstellerformular (Blatt 1 = Antrag, Blatt 2 = Signaturvertrag)
Achtung: Diese Informationen werden teilweise durch den PIN-Eingabe Dialog überdeckt.

Übermittlung der Scans in das Rechenzentrum der a.trust:
An dieser Stelle geht der RO mit dem Signator den auf der folgenden Seite dargestellten „Belehrungstext“ durch (Die Hintergründe der Belehrung finden Sie im entsprechenden Kapitel des Handbuchs. Damit können Sie auch mögliche weitere Fragen des Kunden beantworten):





Bevor der RO mit Punkt H) fortsetzt, **wird der Signator aufgefordert**, seine **GeheimhaltungsPIN (!!)** einzugeben:

- Der Signator autorisiert damit das Schreiben der Echtzertifikate auf die Karte
- Die Funktionsfähigkeit der Karte wird damit getestet

Der RO informiert den **Signator** dazu wie folgt:

> ***„Sobald Ihr Kartenleser ´Bitte Geheimzahl eingeben´ meldet, geben Sie bitte Ihre GeheimhaltungsPIN (!!!) ein. Das ist die zweite PIN aus Ihrem Kuvert, wo GeheimhaltungsPIN dabei steht. Bestätigen Sie die Eingabe dann bitte mit der grünen Taste.“***

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

Belehrung des Signators durch den RO

„Dem Signaturgesetz entsprechend muss sich der Signator an die Inhalte des Merkblatts halten. Diese sind hier nochmals zusammen gefasst:

a.trust haftet für die Vollständigkeit und Richtigkeit des trust|sign bzw. a.sign premium Zertifikats zum Zeitpunkt der Ausstellung und für die technische Sicherheit des Chips Ihrer Karte.
Das qualifizierte trust|sign bzw. a.sign premium Signaturzertifikat dient ausschließlich der Erstellung sicherer digitaler Signaturen. Diese sind laut Signaturgesetz Ihrer eigenhändigen Unterschrift bis auf wenige Ausnahmen gleichgestellt. Für alle anderen Zwecke haben Sie ein einfaches Zertifikat auf Ihrer Karte, das Verschlüsselungszertifikat zum Geheimhaltungsschlüsselpaar.

Die Zertifikate auf dieser Karte sind von Gesetz wegen ausschließlich zu Ihrer persönlichen Verwendung vorgesehen.

- Bewahren Sie diese Karte deshalb sorgfältig auf, und geben Sie sie unter keinen Umständen in andere Hände.
- Halten Sie Ihre PIN geheim. Notieren Sie sie keinesfalls auf der Karte und wählen Sie eine PIN, die nicht von Ihrer Person ableitbar ist. Verwenden Sie beispielsweise NICHT Ihr Geburtsdatum als SignaturPIN.
- Bei Verlust oder Unauffindbarkeit der Karte verständigen Sie bitte umgehend den Widerrufsdienst der a.trust.
- Dies ist auch notwendig, wenn Sie Ihre SignaturPIN vergessen haben oder sich Inhalte Ihres Zertifikats ändern.
- Die Nummer des Widerrufsdienstes finden Sie auf Ihrem Merkblatt und auf der Homepage der a.trust.
- Beachten Sie auch die weiteren Pflichten, die auf das Signaturgesetz begründet sind. Diese sind auf dem Merkblatt übersichtlich angeführt.

Halten Sie sich bei der Hard- und Software Ihrer PC-Signaturumgebung für die Erstellung von sicheren digitalen Signaturen mit trust|sign bzw. a.sign premium an die Empfehlungen der a.trust. Auf deren Homepage sind die für sichere Signaturen empfohlenen Hard- und Softwarekomponenten veröffentlicht. Wenn Sie sich an diese Empfehlungen halten, dann haftet a.trust über das Zertifikat hinaus auch für Ihre sichere digitale Signatur mit trust|sign bzw. a.sign premium.

Softwareprogramme, die auf dem S/MIME-Dateiformat aufbauen (E-Mail-Browser wie MS Outlook oder Netscape Messenger) sind derzeit nicht für sichere digitale Signaturen geeignet. Daher signieren Sie e-Mails mit Ihrem einfachen Zertifikat.

Zu allen Punkten können Sie sich stets aktuell und im Detail auf der Homepage www.a-trust.at informieren. Die genauen Stellen sind auf dem Merkblatt angeführt.

Mit Ihrer Unterschrift akzeptieren Sie die Allgemeinen Geschäftsbedingungen der a.trust, welche auch Ihre Kenntnisnahme dieser gesetzlich geforderten Belehrung umfassen.“

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

H) Aktivierung der Karte durch Eingabe der SignaturPIN des RO

Jetzt sind alle Daten für das Zertifikat und den Signaturvertrag am letztgültigen Stand, archiviert, in das System eingegeben und somit die Echtzertifikate erstellt. Auf der Karte des Signators befinden sich noch die Transportzertifikate, die im nächsten Schritt durch die Echtzertifikate ersetzt werden.

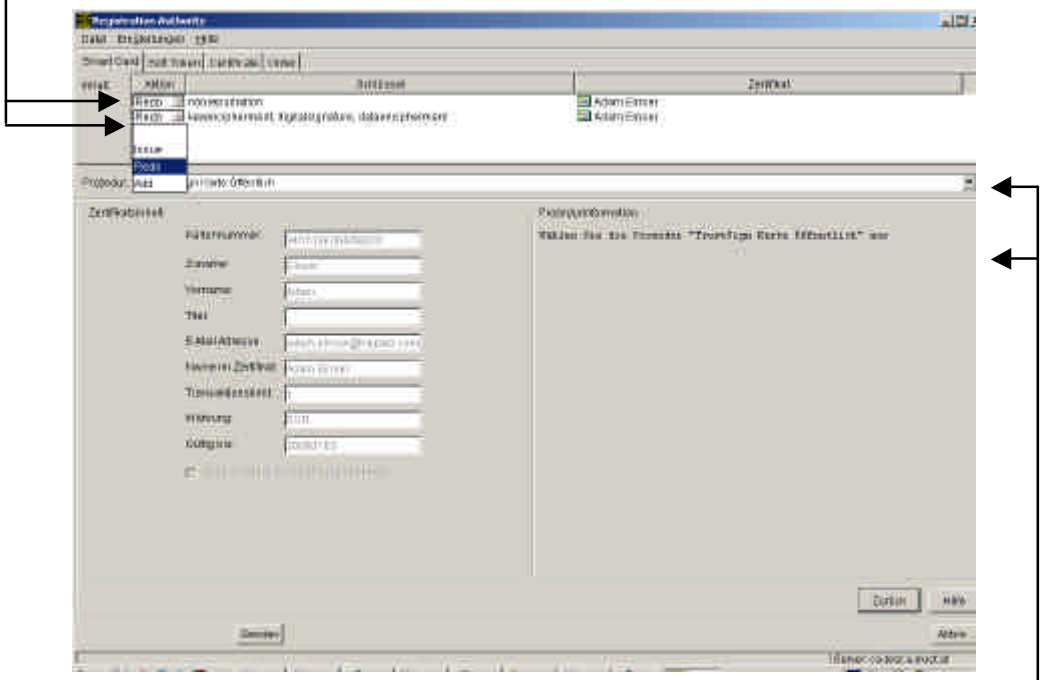
Zur Aktivierung der Karte ist die Signatur des RO (SignaturPIN des RO) notwendig.

Das Ersetzen der Transportzertifikate durch die Echtzertifikate ist ein neuralgischer Schritt im Ablauf der Kartenaktivierung. Das System führt hier aus Sicherheitsgründen im Hintergrund eine Anzahl von Checks und Gegenchecks durch und kontrolliert auch die Zeitabläufe.

Laden der Echtzertifikate auf den Chip:

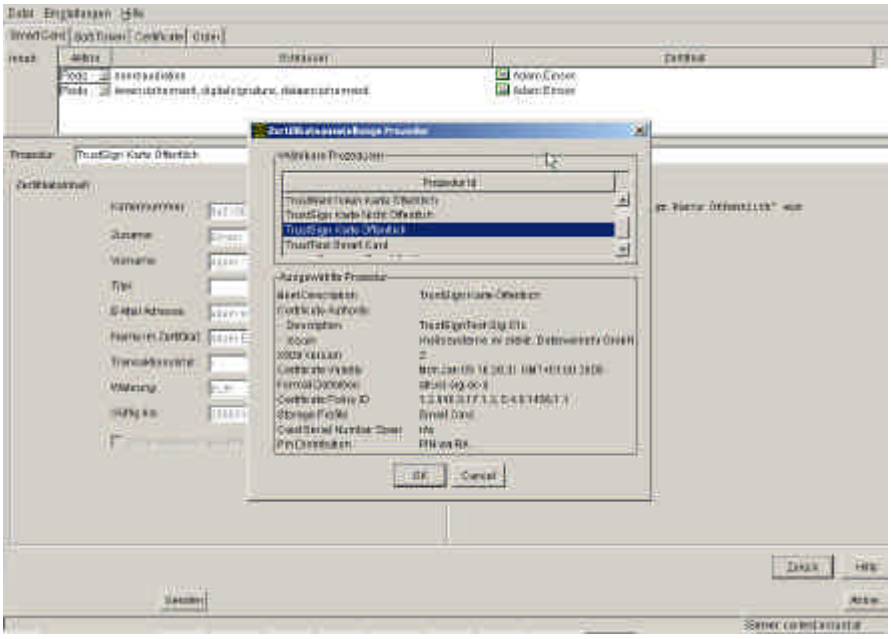
Mit diesem Screen werden die Echtzertifikate auf die Signator-Karte gespeichert.
Im oberen Feld werden noch die Transportzertifikate angezeigt, die ersetzt werden müssen:

Zu jedem Zertifikat – also **2 mal** – muss **immer die Aktion „Redo“ gewählt** werden

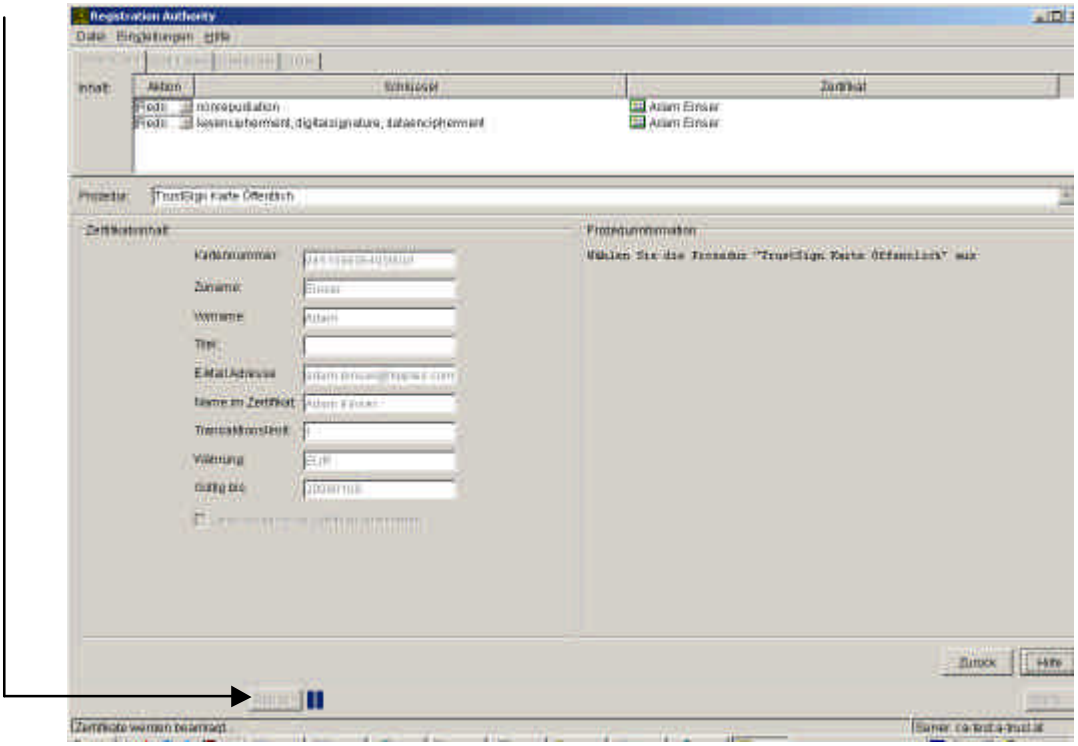


Die **Prozedur** muss **wortwörtlich** immer **entsprechend der Prozedurinformation gewählt** werden.
(Die Abb. auf der nächsten Seite zeigt das aufpoppende Auswahlfenster):

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.



1. Button „Senden“ klicken



2. Der **RO** signiert mit seiner **SignaturPIN** (!!!)

In diesem Dialogfenster sagt der RA-Client dem RO, dass zwei neue Zertifikate erzeugt wurden. (Das Java-Männchen „winkt“ dem RO gleichzeitig mit dem Hinweis „CA wird aktualisiert“):

Der RO bestätigt mit „OK“. Der RA-Client springt in den Screen „Suche nach Signatoren/Verträgen“ zurück, und das Kartensymbol ist grün.

I) Erstellen der SignaturPIN mit Hilfe der InitialPIN

Aus Sicherheitsgründen wird dem Signator empfohlen, sich gleich vor Ort seine persönliche, geheime **sechs- bis achtstellige SignaturPIN** zu erstellen. Damit ist ausgeschlossen, dass nach Verlassen der RA einem Unbefugten die aktivierte Karte mitsamt dem InitialPIN im PIN-Kuvert in die Hände fällt.

Außerdem ist dadurch gewährleistet, dass der Signator bei der Herstellung der vollen Einsatzbereitschaft seiner Karte die Anleitung des RO hat. Die Gefahr, dass der Signator durch falsches Handling des iD2 **Administration Utility** (Administrationsprogramm) seine Zertifikate blockiert, wird dadurch minimiert.

Der RO muss den Signator bezüglich der PIN wie folgt informieren:

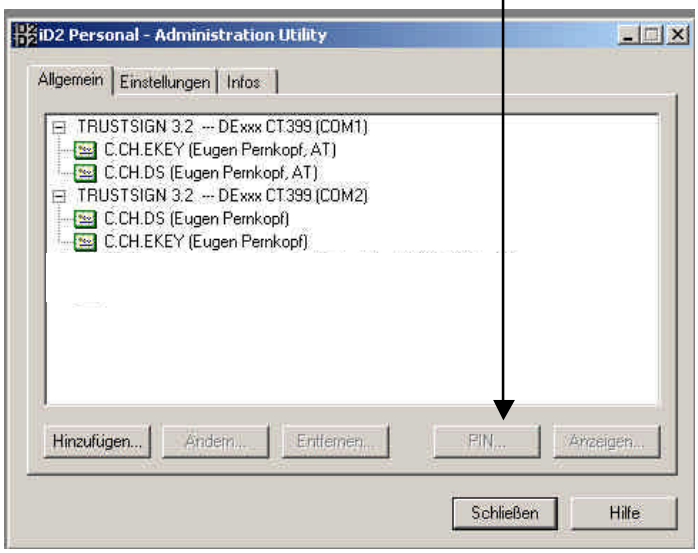
„Mit der vierstelligen SignaturPIN in Ihrem PIN-Kuvert kann nicht signiert werden. Das beweist, dass Ihre Karte noch nie verwendet wurde. Aus Sicherheitsgründen sollten Sie die PIN jetzt sofort ändern:
Ihre echte SignaturPIN muss zwischen 6 und 8 Ziffern haben. Sie sollten dazu nicht Ihr eigenes Geburtsdatum oder das Ihrer Angehörigen verwenden, weil das von einem Unbefugten leicht herausgefunden werden könnte. a.trust empfiehlt Ihnen, die SignaturPIN von Zeit zu Zeit auch in Zukunft zu ändern.“

Zuerst ruft der RO das Administrationsprogramm auf. Das Administrationsprogramm zeigt an, wo es überall nach Zertifikaten sucht.

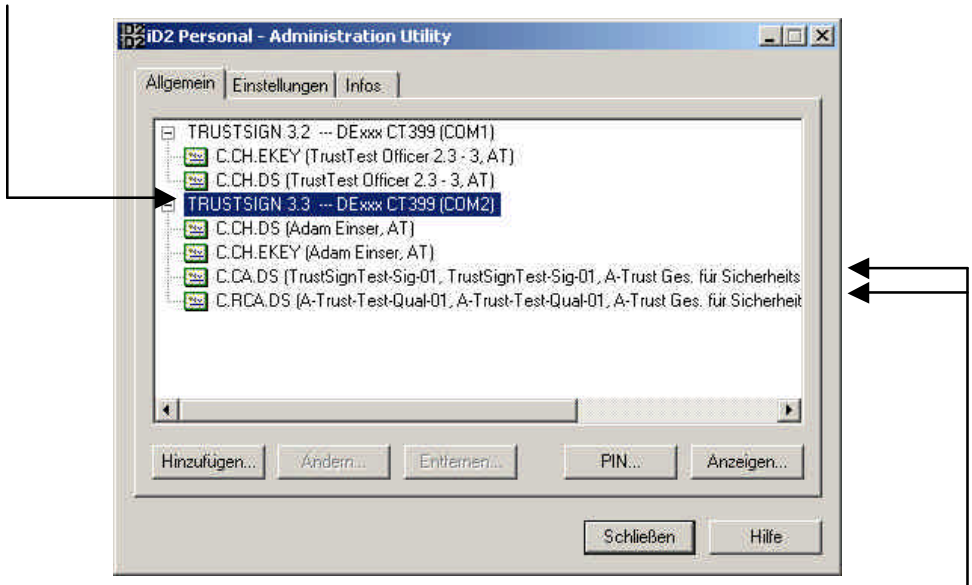
Im Bespiel unten ist dies ein RO-Arbeitsplatz mit
- COM1 Anschluss mit dem Kartenleser des RO
- COM2 Anschluss mit dem Kartenleser des Kunden/Signators

An jeder der Anschlussstellen werden die gefundenen Zertifikate angezeigt:
- Verschlüsselungszertifikat der RO-Karte
- Signaturzertifikat der RO-Karte
- Signaturzertifikat der Signator-Karte
- Verschlüsselungszertifikat der Signator-Karte
- (Bei a.sign premium werden auch die Stammzertifikate angezeigt)

Der Button „PIN...“ ist zu diesem Zeitpunkt inaktiv!



Der RO muss jenen Anschluss markieren, der zu der Karte gehört, deren PIN bearbeitet werden soll. Er markiert sozusagen den „Kunden-Kartenleser“. Damit wird der Button „PIN...“ aktiv:

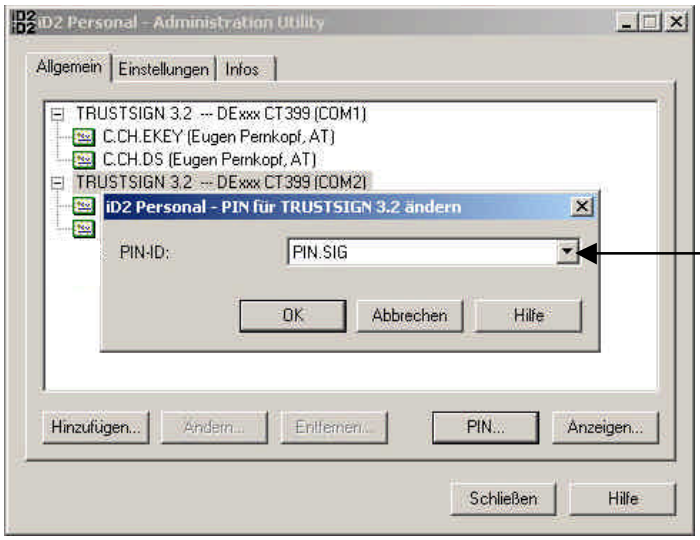


Bei a.sign premium werden auch die Stammzertifikate auf den Chip geschrieben

Bei trust|sign ist dies nicht der Fall (vergleiche die beiden Abb. dieser Seite!)

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

Im Dialogfenster muss nun der RO auswählen, welche PIN geändert werden soll.
PIN.SIG steht für SignaturPIN.
PIN.DEC (wie „decryption“, engl. f. „Entschlüsselung“) steht für GeheimhaltungsPIN.



Nach Klick auf Button „OK“ fordert der **Kartenleser sofort auf seinem Display** die PIN-Eingabe:
→ vierstellige SignaturPIN (= InitialPIN) des Signators aus dem PIN-Kuvert + Bestätigungstaste
→ sechs- bis achtstellige echte SignaturPIN des Signators + Bestätigungstaste
→ diese wiederholen + Bestätigungstaste

Am Bildschirm des RO-Arbeitsplatzes erscheint „PIN wurde erfolgreich geändert“ oder die Aufforderung, den Vorgang zu wiederholen. **Achtung! – 3 mal falsche InitialPIN → Karte kaputt**

HINWEIS: Bei trust|sign bzw. a.sign premium Karten kann der GeheimhaltungsPIN nicht mit dem Administrationsprogramm geändert werden. Die Auswahlmöglichkeit muss jedoch gegeben sein, weil das Programm auch für trust|mark|token (bzw. a.sign token) und trust|mark|VSC (bzw. a.sign light) eingesetzt werden kann.

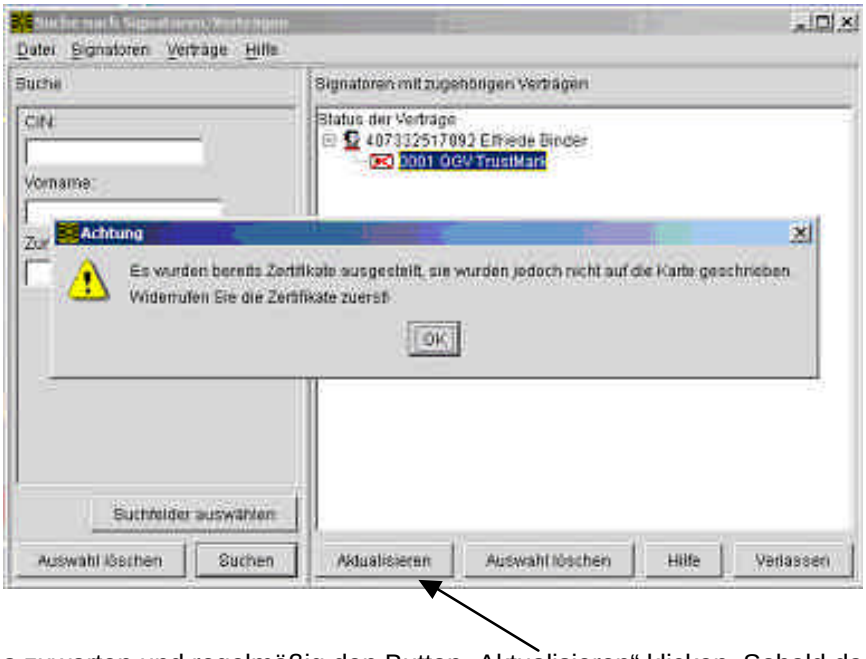
(zur Checkliste)

Aktivierungsfehler: Kartensymbol weiß, rot durchkreuzt

Sehr selten kann es zu diesem Kartenstatus weiß, rot durchkreuzt kommen. Der Warnhinweis erscheint:

„Es wurden bereits Zertifikate ausgestellt, sie wurden jedoch nicht auf die Karte geschrieben. Widerrufen Sie die Zertifikate zuerst!“

Keinen neuerlichen Aktivierungsversuch unternehmen, bevor der RO dieser Anweisung durch den Anruf beim **Widerrufsdienst (+43 1 90337 3072)** entsprochen hat:



Danach etwas zuwarten und regelmäßig den Button „Aktualisieren“ klicken. Sobald das Kartensymbol wieder grau (bzw. weiß bei eingesteckter Signator-Karte) ist, darf die Aktivierung erneut durchgeführt werden.

PIN-Eingabe Dialoge

Am Bildschirm wird dem RO aufgezeigt, welches Zertifikat im jeweiligen Schritt benötigt wird und welche PIN bei diesem Schritt verlangt wird.

Beim **Verbindungsaufbau** muss
- die RO-Karte im
- RO-Kartenleser stecken und die
- RO-GeheimhaltungsPIN eingegeben werden

Sollte hier „Kunden-Kartenleser“ stehen, so steckt die RO-Karte falsch!
In diesem Fall am besten den RA-Client schließen, die Karte umstecken und nochmals starten.

(Markieren Sie den Kartenleser für die RO-Karte und achten Sie bei etwaigem Umstecken der Kabel darauf, welcher Kartenleser an welchem Kabel steckt!)

Bei der **elektronischen Archivierung** muss
- die RO-SignaturPIN (Ausweis) und nochmals
- die RO-SignaturPIN (Antragstellerformular) eingegeben werden

Nach der elektronischen Archivierung muss der Kunde das **Speichern der Zertifikate auf seinem Chip autorisieren**:
- Die Kunden-GeheimhaltungsPIN muss eingegeben werden

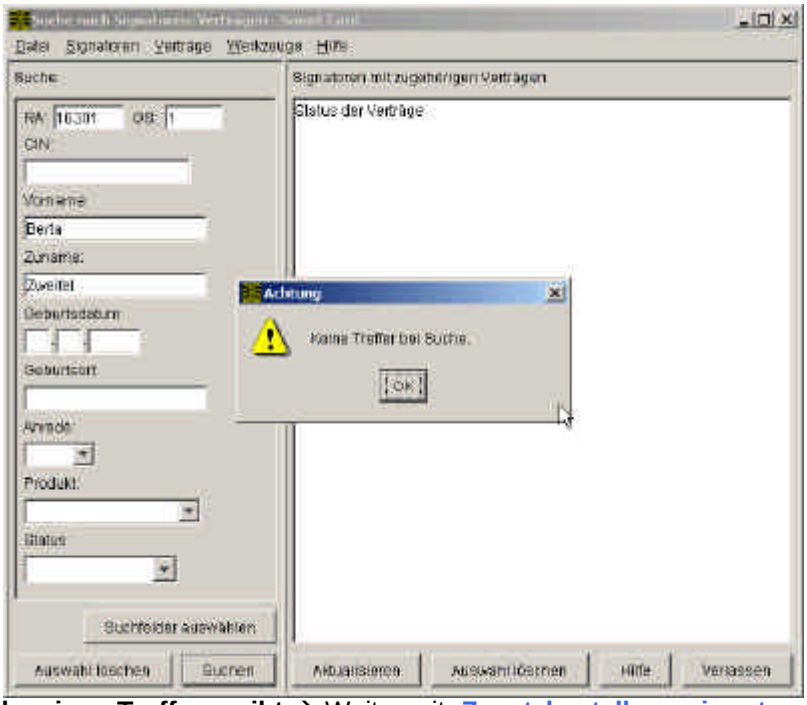
Beim **Abspeichern der Zertifikate auf der Signatorkarte** (Am Screen 2 mal „Redo“ und richtige „Prozedur“ auswählen, Button „Senden“ klicken) muss
- die RO-SignaturPIN (Abb. wie bei der elektronischen Archivierung) eingegeben werden

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

RA-Client – Zusatzfunktionen

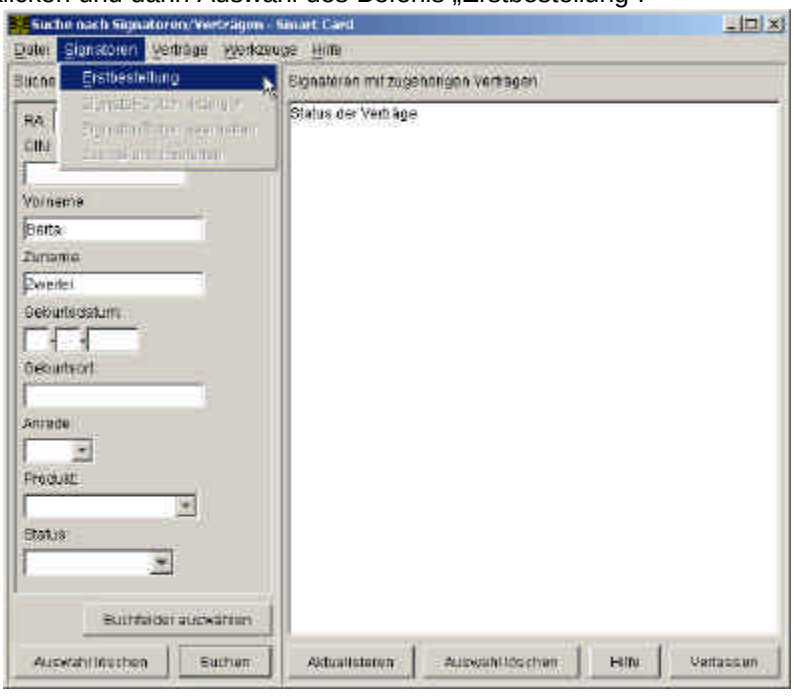
Erstbestellung einer trust|sign *oder* a.sign premium *Karte in Screenshots*

1. Stellen Sie vor der Erstbestellung sicher, ob der Zertifikatswerber schon ein Kunde der a.trust ist, er also schon mindestens ein Zertifikatsprodukt der a.trust und damit eine CIN besitzt oder nicht.



(**Wenn die Suche einen Treffer ergibt** → Weiter mit „**Zusatzbestellung einer trust|sign bzw. a.sign premium Karte**“.)

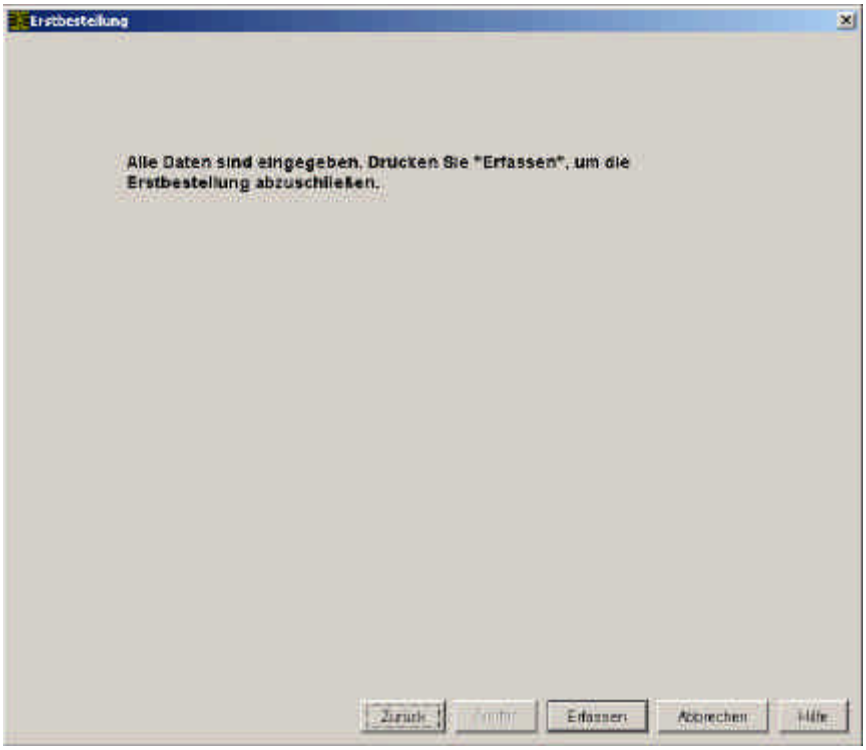
2. Button „OK“ klicken und dann Auswahl des Befehls „Erstbestellung“:



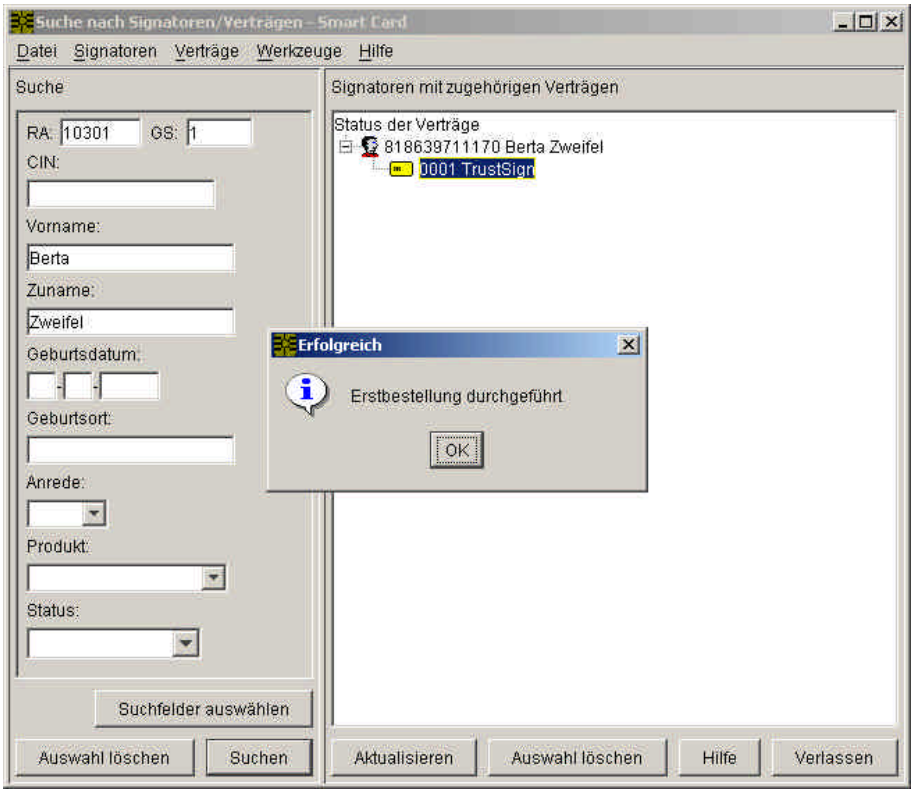
Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

3. Die Screens „Signator-Daten“ und „Vertrags-Daten“ ausfüllen (Siehe „Aktivierung einer...“)

4. Die Erstbestellung erfassen:



5. Erfolgsmeldung

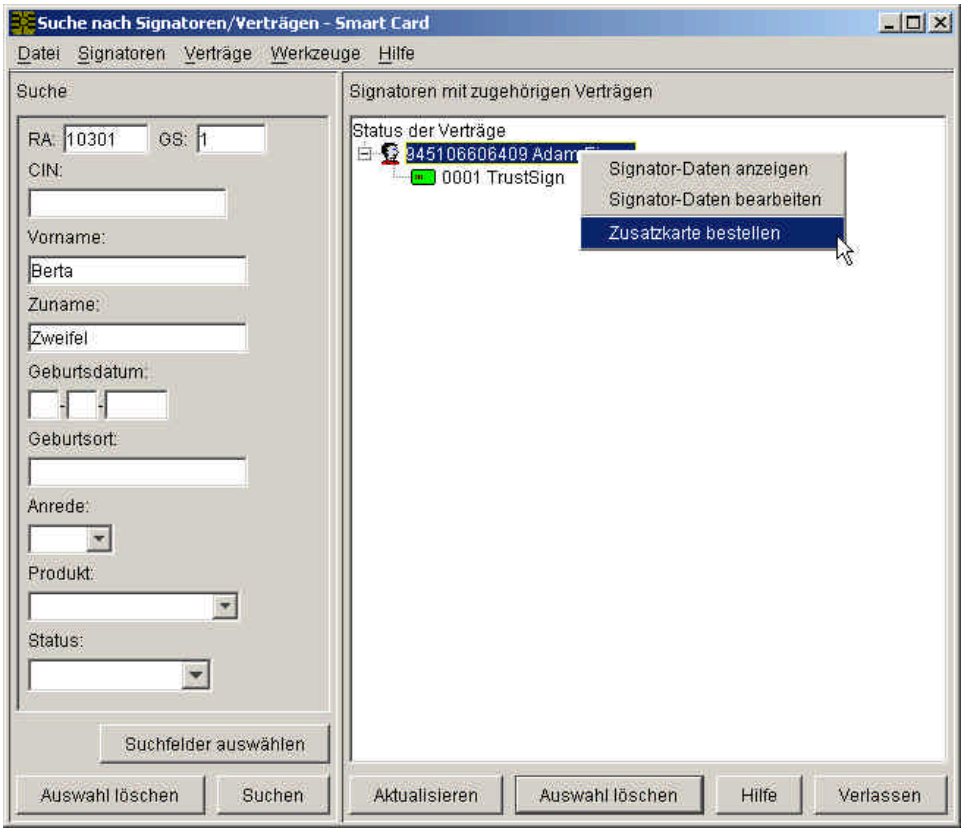


Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

Zusatzbestellung einer trust|sign *oder* a.sign premium *Karte in Screenshots*

1. Stellen Sie vor der Erstbestellung sicher, dass der Zertifikatswerber wirklich schon ein Kunde der a.trust ist und dass der im RA-Client gefundene Kunde/Signator wirklich die Person des Zertifikatswerbers ist.

2. Auswahl des Befehls „Zusatzbestellung“:



Rechtsklick auf die Signator-Zeile oder Signator-Zeile markieren und Hauptmenü „Signatoren“.

3. Weiter wie bei „Erstbestellung“, nur dass die Signator-Daten bereits bekannt sind.

VORSICHT bei den (Vertrags-)Daten !!!

Der Kunde kann bei der Zusatzbestellung durchaus ein anderes Produkt bestellen wollen (a.sign token oder a.sign premium Karte zu einer bestehenden trust|sign Karte oder umgekehrt). Er kann auch andere Vertrags-Daten der Zusatzkarte wählen als im schon bestehenden Vertrag.

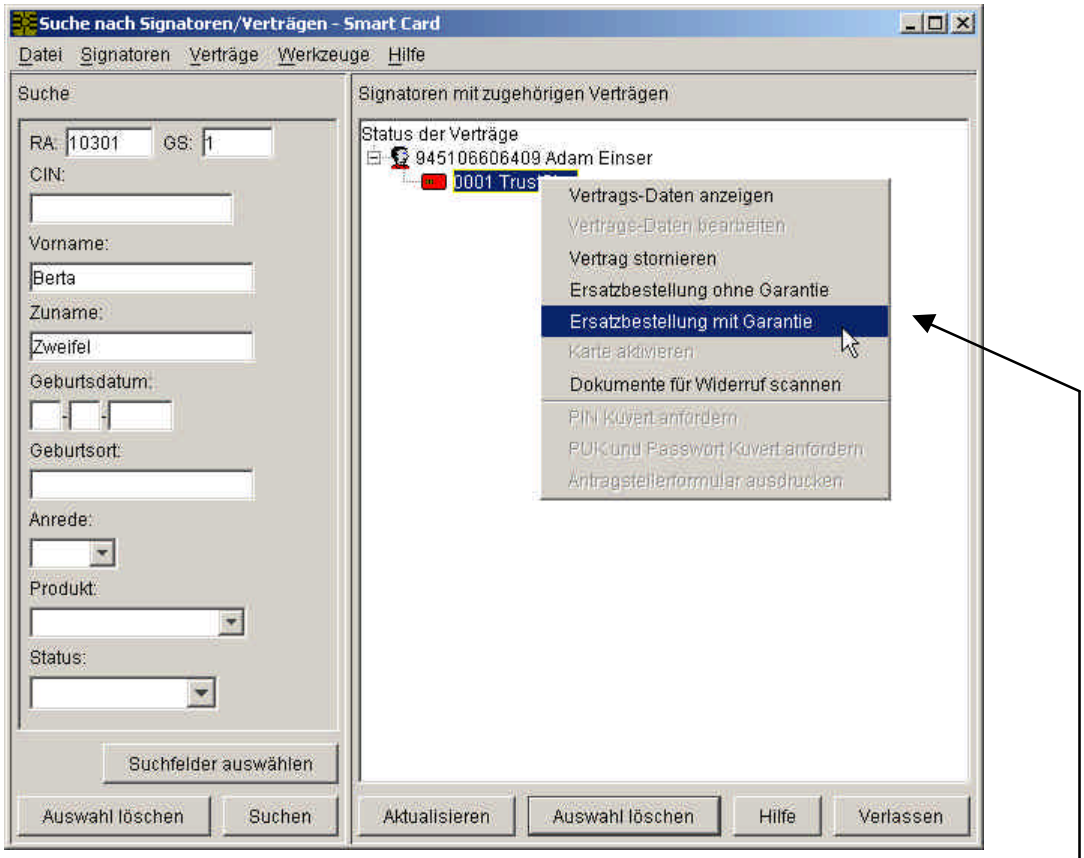
Hinterfragen Sie also gerade auch bei der Zusatzbestellung, ob die bereits bekannten Daten auch für die Zusatzbestellung gelten sollen und kontrollieren Sie auch das „Produkt“.

Ersatzbestellung einer trust|sign *oder* a.sign premium *Karte in Screenshots*

Die Ersatzbestellung ist prinzipiell ein Service, das vom Widerrufsdienst gleich im Zuge eines Widerrufs von Zertifikaten angeboten wird. Das hängt damit zusammen, dass der vorherige Widerruf Voraussetzung der Ersatzbestellung ist.

Doch auch die RA muss dieses Service anbieten können. Etwa, wenn der Kunde nicht gleich beim Widerruf seiner Zertifikate eine Ersatzbestellung abgeben will oder einen Gewährleistungsfall geltend macht (Siehe „Garantie“).

Befehle „Ersatzbestellung mit / ohne Garantie“



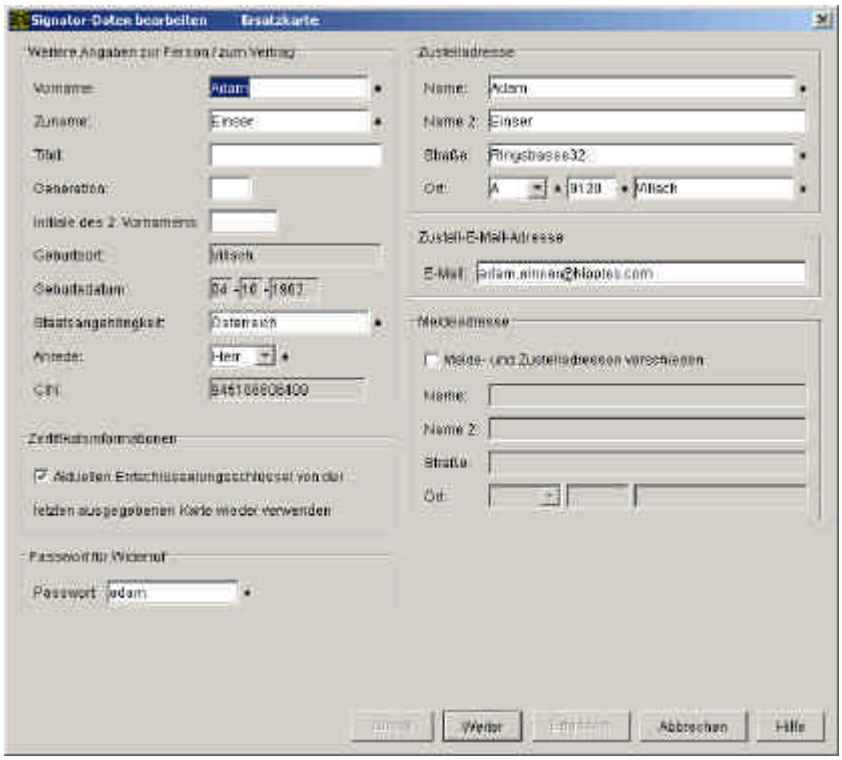
Beim Widerruf der ursprünglichen Karte aufgrund von Änderungen der Zertifikatsdaten ist es ***empfehlenswert***, gleich bei der Ersatzbestellung die Daten zu aktualisieren.

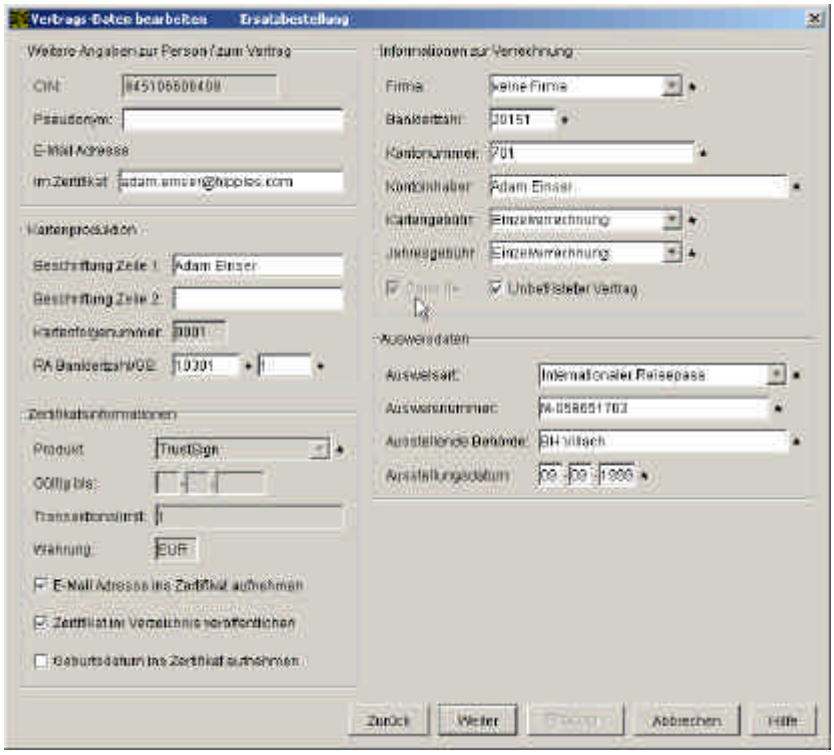
Will der Kunde auch Änderungen am Aussehen der Karte (Beschriftung!), dann ist die entsprechende Aktualisierung ***notwendig***.

ACHTUNG:
Im **Gewährleistungsfall** muss der RO **„Ersatzbestellung mit Garantie“** in allen anderen Fällen **„Ersatzbestellung ohne Garantie“ anklicken-**

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

Screen „Signator Daten“ und „Vertragsdaten”

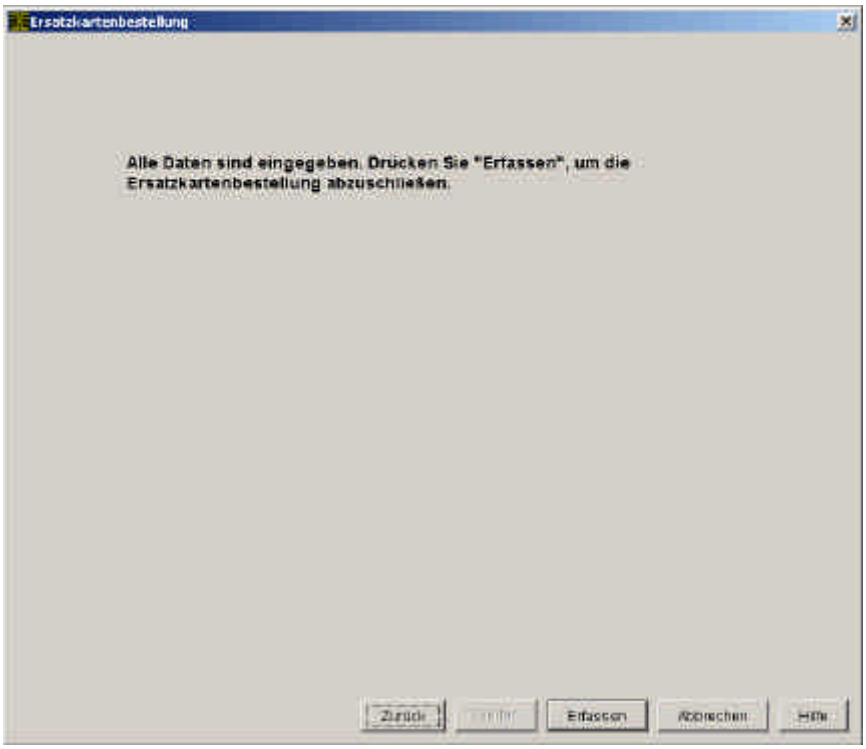




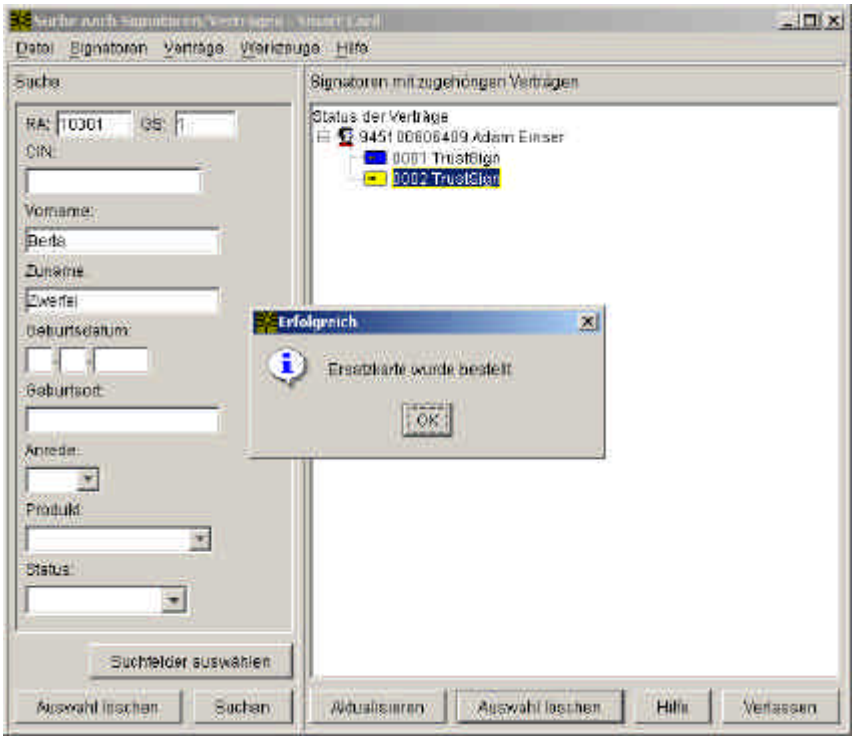
Diese beiden Screens werden im Rahmen der Erstregistrierung (Signator-Daten und Vertrags-Daten) ausführlich erläutert.

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

Mit dem Button „Erfassen“ wird die Ersatzbestellung abgeschlossen.

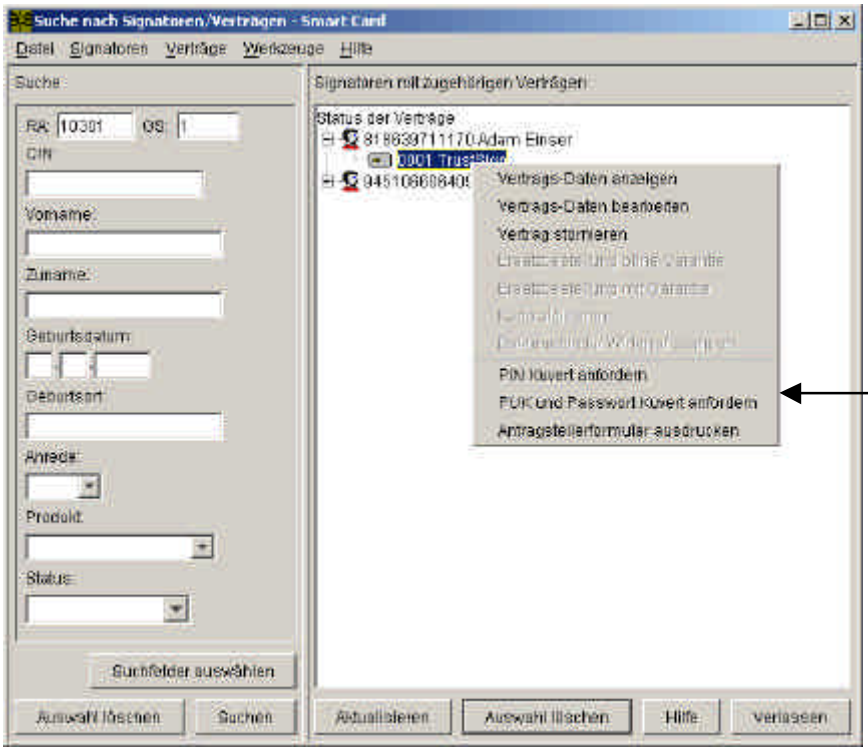


Der RA-Client gibt eine Erfolgsmeldung



Nachbestellung von PIN, PUK und Passwort in Screenshots

Im Screen „Suche Signatoren/Verträge“ zuerst die betreffende Karte suchen, dann die gewünschten Kuverts anfordern.



Der RO muss aus **3 Varianten** auswählen, welchen Inhalt das „**PIN Kuvert**“ haben soll („Verschlüsselung“ bedeutet GeheimhaltungsPIN):

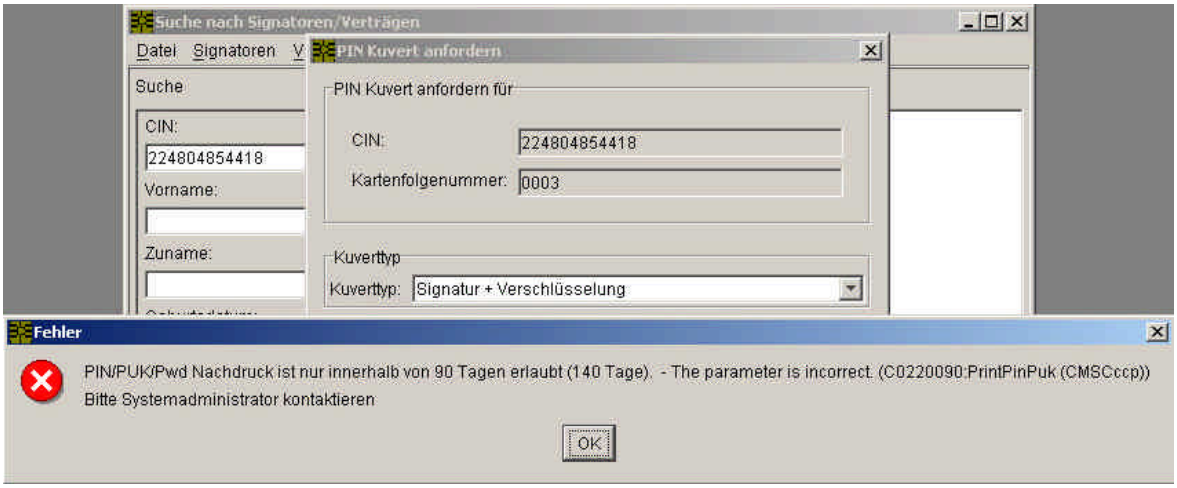
Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

Der RO muss aus **3 Varianten** auswählen, welchen Inhalt das „**PUK und Passwort Kuvert**“ haben soll („Verschlüsselung“ bedeutet GeheimhaltungsPUK):

Mit dem Klick auf „Drucken“ wird das Kuvert angefordert und es erscheint eine Erfolgsmeldung:

(Bzw. „PIN Kuvert wurde angefordert“)

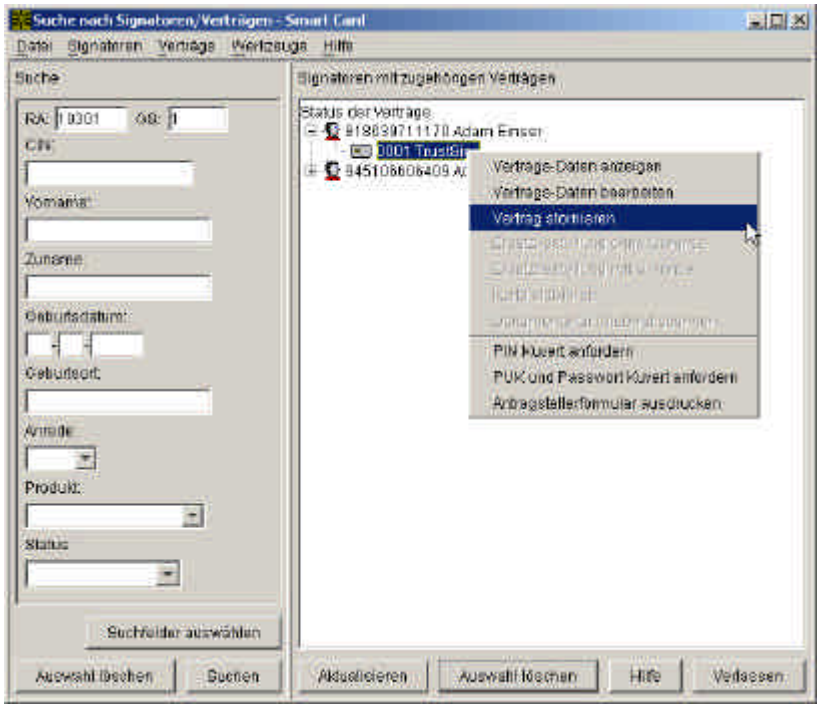
Ein „**PIN Kuvert**“ kann **nur vor der Kartenaktivierung und bis maximal 90 Tage** ab der Kartenproduktion nachbestellt werden!
(Ein „PUK und Passwort Kuvert“ kann immer nachbestellt werden.)



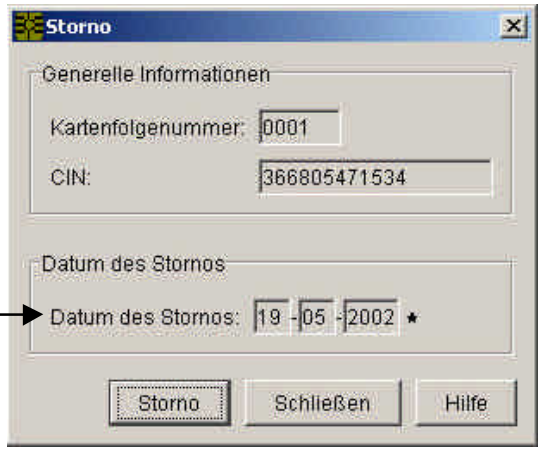
Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

Storno eines Vertrags/einer Karte in Screenshots

1. Der richtige Kartenvertrag muss ausgesucht werden:



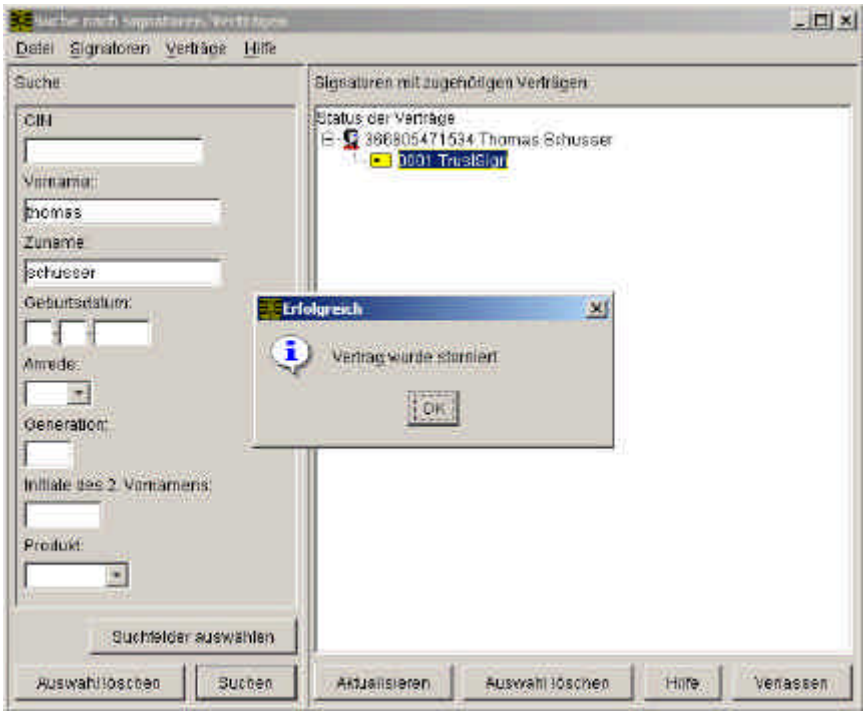
2. Das richtige Stornodatum (Stornostichtag) muss eingetragen werden:



Hier ist jedes Datum von heute bis längstens 31. Dezember möglich. Wenn der Signator die Karte nutzen will, solange er sie auch bezahlt hat, muss der RO den 31. Dezember eintragen.

Am Stornostichtag widerruft a.trust die Zertifikate der stornierten Karte.

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.



Nach „OK“ wird das Kartensymbol schwarz, der Storno ist durchgeführt.

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

Belehrungs- u. Vertragshintergründe: Details für den RO

Dieser Abschnitt des Registrierungshandbuchs liefert Ihnen das Hintergrundwissen zum Zertifizierungsdienst „Registrierung“. Dies versetzt Sie in die Lage, tiefer gehende Fragen Ihres Kunden betreffend die Übergabe von Zertifikaten, den Signaturvertrag der a.trust und mit den Zertifikaten erstellte Signaturen vor dem rechtlichen Hintergrund von SigG und SigV zu beantworten.

Technische Aspekte der Zertifikatsanwendung in Signatur-Applikationen diverser Dienstleister sind hier bewusst ausgespart. Diese zu erläutern geht über die Aufgaben des RO als Ausführender des Zertifizierungsdienstes Registrierung ebenso hinaus, wie die Erklärung der Konfiguration der Soft- und Hardwarekomponenten der PC-Signaturumgebung des Signators.

Hintergründe der Belehrung des Signators:

Laut Signaturgesetz (§ 20 SigG) muss der Signator vor Ausstellung seines Zertifikats über den Umgang mit einem qualifizierten Zertifikat und über die Erstellung einer sicheren digitalen Signatur belehrt werden. Diese „Belehrung“ ist eine **Information für den Signator** darüber, was er selbst dazu beitragen kann, dass ein Missbrauch seiner persönlichen digitalen Signatur ausgeschlossen ist.

Diese Eigenverantwortlichkeit des Signators (§ 21 SigG spricht von „Pflichten des Signators“) ist ein wichtiger Bestandteil der Gesamtsicherheit von sicheren digitalen Signaturen im elektronischen Datenverkehr. Daraus folgt, dass die optimale Versorgung des Signators mit diesen Informationen ein Qualitätskriterium von trust|sign bzw. a.sign premium darstellt und bei a.trust einen entsprechend hohen Stellenwert hat.

a.trust stellt ihren Kunden daher diese Informationen nicht bloß punktuell, sondern in einem Kommunikationsprozess zur Verfügung. Dabei werden verschiedene „Medien“ genutzt, die den Interessenten an einem a.trust Zertifikat bei unterschiedlichen Gelegenheiten direkt ansprechen:

Die Informationen stehen jedermann, jederzeit und stets aktuell auf www.a-trust.at zur Verfügung.
Interessenten an einem Zertifikat ist die Einsichtnahme bereits im Vorfeld einer Bestellung möglich
Nach einer Kartenbestellung erhält der Zertifikatswerber seinen persönlichen Kartenabholbrief. Darin befindet sich ein Merkblatt mit der genauen Aufstellung der Pflichten eines Signators laut SigG und einem klaren „Belehrungs“-Text in Ich-Form. Der Zertifikatswerber wird deutlich darauf hingewiesen, dass er die Informationen mit seiner Unterschrift auf dem Signaturvertrag zur Kenntnis nehmen wird
Bei der persönlichen Zertifikatsübergabe wird der Signator durch den RO nochmals und leicht verständlich auf diese Informationen hingewiesen und kann direkte Fragen stellen

Dieser Prozess der Informationsleistung in Richtung des Signators verfolgt natürlich nicht zuletzt aus ökonomischen Gesichtspunkten heraus auch das Ziel, den Aufwand in der Registrierungsstelle nach zwei Aspekten zu minimieren:

- Der RO kann nur hinsichtlich seiner Aufgaben im Zuge der Registrierung klar definierte Inhaltsbereiche in der erforderlichen Qualität abdecken
- Der RO muss angesichts des komplexen Themas „Digitale Signatur“ die Kontrolle über die Informationsnachfrage durch Kunden behalten und diese gegebenenfalls treffsicher zu anderen Quellen leiten

Hinsichtlich des Qualitätsanspruchs der a.trust gehören die im Folgenden erläuterten Hintergründe zum Know-how des RO. Nachdem a.trust von Fragen des Signators ausgeht, sind diese Hintergründe für den RO als entsprechender Vorschlag zu einem Sprechertext formuliert:

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

Allgemeine Geschäftsbedingungen (AGB) der A-Trust zu trust|sign bzw. a.sign premium

„Sie schließen diesen Vertrag mit der A-Trust GmbH, einem akkreditierten Zertifizierungsdiensteanbieter, der sich zur Registrierung und zum Vertrieb autorisierter Registrierungsstellen, wie wir eine sind, bedient. Der Vertrag ist auf folgende Dokumente, die von der staatlichen Aufsichtsstelle (TKK: Telekom Control Kommission) geprüft worden sind, begründet: die Zertifizierungsrichtlinie (CPS: Certification Practice Statement), die Certificate Policy (CP), die AGB, die Entgeltbestimmungen der A-Trust sowie die technischen Komponenten und Verfahren und die gesetzliche Belehrung einschließlich der Pflichten des Signators.
Der Umgang mit den Daten ist im Datenschutzgesetz und dem SigG geregelt und wird von A-Trust auf ihre Betreibertätigkeit als ZDA beschränkt. Eine Offenlegung erfolgt nur auf richterliche Anordnung. A-Trust haftet für ihre Leistungserbringung in der Registrierung, bei der Ausstellung des Zertifikats, beim Verzeichnisdienst, beim Widerrufsdienst und für die von ihr eingesetzten, bzw. dem Signator von ihr empfohlenen technischen Komponenten und Verfahren."

Zertifizierungsrichtlinie (CPS)

„Die Zertifizierungsrichtlinie (= Certification Practice Statement, kurz CPS) ist die allgemein verständliche Zusammenfassung des Sicherheits- und Zertifizierungskonzepts der A-Trust, welches von der staatlichen Aufsichtstelle geprüft und akkreditiert wurde.
In der Zertifizierungsrichtlinie werden die technischen und organisatorischen Bedingungen (technische Normen, Haftung, Öffnungszeiten etc.) der Erstellung des qualifizierten Zertifikats durch A-Trust und seiner Übergabe an den Signator (Registrierungsablauf) bekannt gegeben. Damit kann sich jeder, auch die Empfänger Ihrer Signaturen, ein Bild von der Gesamtsicherheit von trust|sign bzw. a.sign premium machen."

Certificate Policy (CP)

„Die Policy beschreibt den Inhalt des Zertifikats und die Bedingungen der sicheren Verwendung des Zertifikats durch den Signator. Somit gibt sie dem Empfänger einer Signatur die Sicherheit, ob es eine sichere digitale Signatur ist und ob das ihr zu Grunde liegende Zertifikat ein qualifiziertes ist. Neben den Rechten und Pflichten des Signators sind dort auch jene des Zertifizierungs-diensteanbieters dargestellt. Auf die CP stützt sich somit die Vertrauenswürdigkeit eines Zertifikats.

Z.B. darf das qualifizierte Zertifikat nur für sichere Signaturen laut SigG verwendet werden. Für alle anderen Zwecke haben Sie deshalb auch ein einfaches Zertifikat mit einem Geheimhaltungs-schlüsselpaar auf Ihrer trust|sign bzw. a.sign premium Karte (Ver- und Entschlüsseln, einfache Signatur, SSL-Login).

Dieses darf man auch auf mehreren Karten verwenden, um das selbe verschlüsselte Dokument mit unterschiedlichen Karten entschlüsseln zu können."

Ausnahmen des Ersatzes der eigenhändigen Unterschrift durch trust|sign bzw. a.sign premium

„Paragraph 4 des Signaturgesetzes nennt folgende vier Ausnahmen, wo die sichere digitale Signatur NICHT die Schriftform im Sinne des § 886 ABGB ersetzt:

- An Schriftform oder strengeres Formerfordernis gebundene Rechtsgeschäfte des Familien- und Erbrechts
- Andere Willenserklärungen oder Rechtsgeschäfte, die zu ihrer Wirksamkeit an die Form einer öffentlichen Beglaubigung, einer gerichtlichen oder notariellen Beurkundung oder eines Notariatsakts gebunden sind
- Willenserklärungen, Rechtsgeschäfte oder Eingaben, die zu ihrer Eintragung ins Grundbuch, ins Firmenbuch oder in ein anderes öffentliches Register einer öffentlichen Beglaubigung, einer gerichtlichen oder notariellen Beurkundung oder eines Notariatsakts bedürfen

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

- Bürgschaftserklärung, die von Personen außerhalb ihrer gewerblichen, geschäftlichen oder beruflichen Tätigkeit abgegeben wird“

Empfohlene technische Komponenten und Verfahren (Signaturprodukte)

„A-Trust haftet für die Sicherheit des Chips Ihrer Karte, für die von A-Trust selbst eingesetzten technischen Komponenten und Verfahren zum Schutz Ihres privaten Signaturschlüssels und für die Vollständigkeit und Richtigkeit Ihres Zertifikats zum Zeitpunkt der Ausstellung.

Wenn Sie sich bei den Hard- und Softwarekomponenten Ihrer eigenen PC-Signaturumgebung für die Erstellung von sicheren digitalen Signaturen an die Empfehlungen der A-Trust halten, dann haftet A-Trust über das Zertifikat hinaus auch für Ihre sichere digitale Signatur.

Auf www.a-trust.at/docs/verfahren veröffentlicht A-Trust jene Hard- und Softwarekomponenten, die sie für sichere digitale Signaturen empfiehlt.

Bei diesen empfohlenen Signaturprodukten geht es um die sichere PIN-Eingabe auf dem Smart Card Reader und die sichere Hashwertbildung/Datenanzeige durch die eingesetzte Software. Softwareprogramme, die auf dem S/MIME-Dateiformat aufbauen (E-Mail-Browser wie MS Outlook oder Netscape Messenger) sind derzeit nicht für sichere digitale Signaturen geeignet. Ebenso Softwareprogramme, die etwa dynamische Datumsfelder oder Weiß-auf-Weiß-Darstellungen beinhalten können, wie z.B. MS Word.

A-Trust hält zudem in ihrem hochsicheren Rechenzentrum technische Komponenten und Verfahren bereit, um im Schadenfall auf Verlangen der nach dem SigG dafür autorisierten Stellen (staatliche Aufsichtsstelle, Gerichte) die sichere Signaturprüfung zu ermöglichen.“

Widerrufs- und Verzeichnisdienst

„A-Trust stellt mit dem **Widerrufsdienst** sicher, dass Ihnen bei Bedenken hinsichtlich der Sicherheit Ihrer Signaturerstellungsdaten oder Ihrer PIN oder bei Änderung von Zertifikatsdaten jederzeit, schnell und einfach der Widerruf bzw. die Sperre des Zertifikats möglich ist. Dies und die allfällige Aufhebung einer Sperre sind die einzigen, aber sehr wichtigen Aufgaben des Widerrufsdiensts.

Die Erreichbarkeit des Widerrufsdiensts für Widerruf, Sperre oder Aufhebung einer Sperre finden Sie auf der A-Trust Homepage und auf dem Merkblatt. Das von Ihnen bei der Kartenbestellung selbst gewählte Passwort spielt bei der Kommunikation mit dem Widerrufsdienst eine große Rolle. Bitte sorgen Sie dafür, dass Sie das Passwort bei Bedarf auch wirklich wissen (Es wird Ihnen im Kartenabholbrief im PUK-Kuvert zugeschickt). Der Widerruf ist unter Nennung des Namens, der Kartennummer und des Passworts telefonisch und per Fax möglich.

Die Gründe für einen **Widerruf** können sein:

- Karte wurde verloren oder gestohlen
- geheimer Schlüssel wurde kompromittiert
- Karte ist defekt
- PIN wurde vergessen oder kompromittiert
- Zertifikatsdaten (z. B. Ihr Name) haben sich geändert

Der Grund für eine **Sperre** kann eigentlich nur einer sein:
Man findet seine Karte nicht und man hofft, sie noch innerhalb der Sperrfrist wieder zu finden. Die Sperraufhebung kann nur mittels jenes Aufhebungspasswortes erfolgen, welches Sie für diesen Zweck bei der **Beantragung** der Sperre vom Widerrufsdienst erhalten. Die Sperre ist aus diesem Grund **nur telefonischen** möglich. Die Nennung des Passworts aus dem PUK-Kuvert ist bei der Sperre nicht unbedingt notwendig.
Sperrfrist: Wenn eine Sperre nicht bis 22 Uhr des zweiten auf den Tag der Sperre folgenden Werktags telefonisch aufgehoben wird, dann geht die Sperre automatisch in den Widerruf über.

Die Zertifikatsnummern widerrufener oder gesperrter Zertifikate stehen in der Widerrufsliste, der sogenannten Certificate Revocation List = **CRL**. Diese Liste wird von A-Trust laufend aktualisiert, und somit können Sie hier jederzeit den Status eines Zertifikats nachprüfen. Aufgehobene Sperren scheinen nie mehr in einer CRL auf.

Die Gültigkeitsdauer eines Zertifikats ist im Zertifikatsinhalt überprüfbar. Damit Sie Ihr Zertifikat nicht mit jeder Signatur mitschicken müssen, empfehle ich Ihnen, das Zertifikat im **Verzeichnisdienst** veröffentlichen zu lassen.

Der Verzeichnisdienst, in dem Sie auch den Status eines Zertifikats prüfen können, ist auf der A-Trust Homepage einsehbar.“

Call Center

„Falls Sie technische Probleme beim Einsatz Ihrer trust|sign bzw. a.sign premium Karte haben oder Auskunft zu weiteren A-Trust-Produkten und Preisinformationen benötigen, können Sie die kostenpflichtige Hotline der A-Trust kontaktieren. Die MitarbeiterInnen dieses Call Centers sind in Fragen zur A-Trust und deren Produkte geschult.

Die Telefonnummer und Geschäftszeiten des Call Centers finden Sie auf dem Merkblatt und auf der Homepage der A-Trust

Das Call Center hat nichts mit dem kostenlosen Widerrufsdienst zu tun.“

Nachsignieren

„Ob eine Signatur mit der damals eingesetzten Technik noch als sicher einzustufen ist, regelt die österreichische Signaturverordnung. Sollte es laut SigV absehbar werden, dass diese Sicherheit nachzulassen beginnt, wird dies auf der A-Trust Homepage verlautbart.

In einem solchen Fall werden die signierte Datei und die zugehörige digitale Signatur gemeinsam neu signiert und mit einem sicheren Zeitstempel versehen. Man spricht von **Nachsignieren**, was eine lückenlose Sicherheitskette über lange Zeiträume (100 Jahre und mehr) gewährleistet. Damit behält die ursprüngliche Signatur immer ihre rechtliche Gültigkeit.

Die zum jeweiligen Zeitpunkt genaue Vorgehensweise des Nachsignierens wird jeweils rechtzeitig auf der A-Trust Homepage zu erfahren sein.“

Akkreditierung

„A-Trust hat sich von der staatlichen Aufsichtsstelle, der Telekom-Control-Kommission, auf Einhaltung von Signaturgesetz und -verordnung überprüfen lassen und lässt dies laufend von der Aufsichtsstelle kontrollieren. A-Trust hat sich von der staatlichen Aufsicht freiwillig akkreditieren lassen. Mit der staatlichen Akkreditierung kann die A-Trust auch nach außen beweisen, dass sie absolut den Anforderungen von Signaturgesetz und Signaturverordnung entspricht und höchste Qualität bietet.“

(Zurück zu AGB)

Deblockieren einer PIN mit dem UnblockUtil

Der Umgang mit dem Administration Utility (Administrationsprogramm), das zur **Änderung der SignaturPIN** benötigt wird, ist im Schritt I) des Registrierungsablaufs beschrieben.

Dieser Abschnitt beschreibt, wie man mit dem **UnblockUtil** eine blockierte **GeheimhaltungsPIN deblockieren** kann.

Grundsätzliches:

Wenn man eine PIN bei a.sign premium zehn mal falsch eingibt (bei trust|sign drei mal), dann ist die PIN blockiert. Dies ist notwendig, um das Herausfinden einer PIN durch Probieren eines Unbefugten so gut wie auszuschließen.

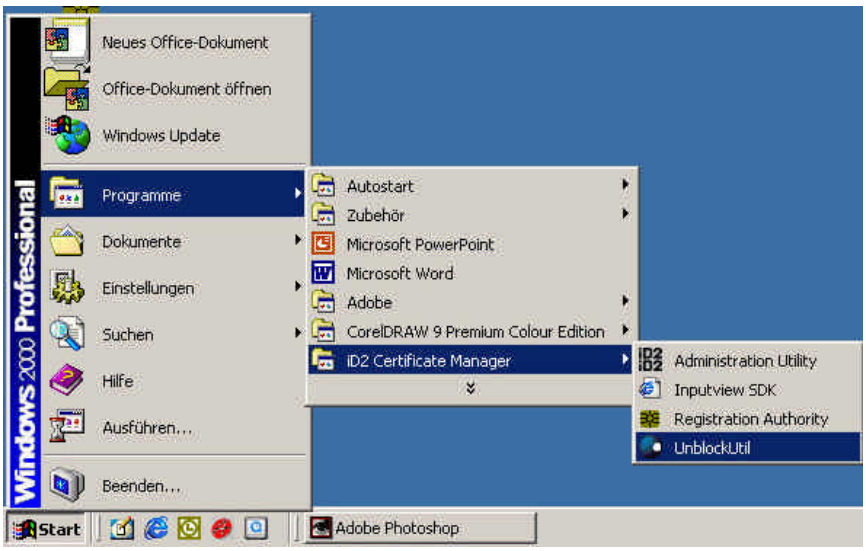
Zum Deblockieren der GeheimhaltungsPIN hat der Signator in seinem „PUK- und Passwortkuvert" einen **GeheimhaltungsPUK** (Personal Unblocking Key), den er im UnblockUtil auf sein Geheimhaltungszertifikat anwenden kann.
(Einen SignaturPUK darf a.trust aus Sicherheitsgründen nicht anbieten. Wird eine SignaturPIN bei a.sign premium durch zehnmalige, bei trust|sign dreimalige Falscheingabe blockiert, so ist die Karte damit kaputt!)

Das UnblockUtil ist Teil der Registrierungssoftware und wird deswegen hier erklärt.

UnblockUtil starten:

WENN DIE SIGNATORKARTE DEBLOCKIERT WERDEN MUSS, DANN MUSS DER RO SEINE RO-KARTE AUS DEM RO-KARTENLESER HERAUSNEHMEN und den RA-Client beenden.

Das UnblockUtil wird aus dem START-Programm aufgerufen:



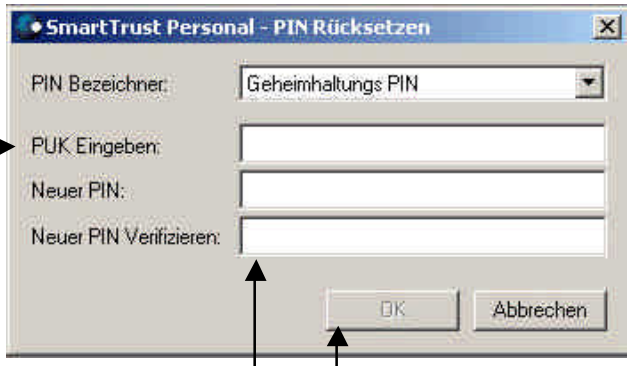
Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

PUK-Eingabe:

Es dauert einige Sekunden...

... bis das UnblockUtil bereit ist:

„GeheimhaltungsPIN“ muss im aufpoppenden Fenster ausgewählt sein/werden



Auf der PC-Tastatur wird **1.** der PUK eingegeben, dann **2.** die **vierstellige** GeheimhaltungsPIN.

Diese muss wiederholt werden **3.** und **4.** die Eingaben mit OK bestätigt werden.

Dann erscheint zum Abschluss die Erfolgsmeldung:

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

Tabelle I) Anlieferung der trust|sign bzw. a.sign premium Karten in der Geschäftsstelle und Lagerführung

TABELLE I) Anlieferung der Karten in der Geschäftsstelle und Lagerführung		
A) Die Karten überprüfen auf: Übereinstimmung mit dem Produktionsprotokoll Erkennbare Schäden	**Das Layout der Karten und die bereits eingravierten Zeilen mit dem Namen und der Kartennummer können nicht verändert werden!**	**Fehlbestand: Meldung an zRO** **Wenn die Karte offensichtliche Beschädigungen aufweist und/oder der Signator eine andere Beschriftung will:** • **Karte/Chip vernichten** • **vernichtete Karte stornieren** • **neue Karte bestellen (Zusatzkarte)**
B) Karten und dazugehöriges Produktionsprotokoll im Tresor einlagern		
C) Entnahmen	**Bei Kartenausgabe: Jede Entnahme mit Datum im Produktionsprotokoll vermerken. Gewährleistet jederzeit exakten Lagerstand (Revision!).**	Check der Karte im RA-Client und Antragsarchiv (Farben siehe TABELLE II); *immer* Vermerke im Produktionsprotokoll! **Bei Fehlbestand Meldung an zRO!**

Tabelle II) Farben der Symbole im RA-Client je Status der betreffenden trust|sign bzw. a.sign premium Karte

TABELLE II) Farben der Kartensymbole im RA-Client je Status der betreffenden Karte		
GELB	Karte ist bestellt	Karte noch nicht von Austria Card produziert
TÜRKIS	Karte ist bei Austria Card in Produktion	Karte noch nicht von Austria Card ausgeliefert
GRAU	Karte wurde von Austria Card produziert	Karte von Aus.Card bereits an RA ausgeliefert
WEISS	Karte steckt zur Aktivierung im Kundenreader der RA	Nur zwischen GRAU und GRÜN möglich
WEISS, ROT durchkreuzt	Aktivierungsabbruch wegen technischem Fehler	Widerruf der beiden betreffenden Zertifikate, dann ist neue Aktivierung der Karte möglich
GRÜN	Karte ist aktiv	
SCHWARZ	Karte ist aktiv, Vertrag ist mit späterem Datum storniert	Karte ist gültig, Zertifikate werden erst mit dem Stornostichtag widerrufen
ROT	Karte ist gesperrt oder widerrufen	
BLAU	Karte ist widerrufen, Ersatzkarte ist bestellt	Doppelbestellung ist dadurch nicht möglich
SCHWARZ, ROT durchkreuzt	Karte ist auf Grund von Vertragsstorno widerrufen	Mit dem Stornostichtag werden die Zertifikate der Karte von a.trust widerrufen

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.