Registrierungshandbuch

für Registration Officers

-

Ausstellung von qualifizierten Zertifikaten

Handy-Signatur

In diesem Dokument wurde aus Gründen der besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet

1. Inhalt

2. Grundinformationen

2.1 Zertifikat, Personenbindung

Im Laufe des Registrierungsprozesses wird **ein qualifiziertes Zertifikat** sowie die **Personenbindung** erstellt. Die Speicherung des Zertifikates erfolgt im Hochsicherheitsbereich des A-Trust Rechenzentrums.

- ein qualifiziertes Zertifikat
  - ist wesentliche Grundvoraussetzung für die Erstellung einer qualifizierten Signatur
  - Basis für e-Government-Anwendungen
  - Inhalt: Name inkl. Titel*, Geburtsdatum bei Minderjährigen (zwischen 14 und 18),

  *Titel können nur im Zuge der Aktivierung in einer Registrierungsstelle in das Zertifikat aufgenommen werden

- Personenbindung
  - verknüpft mit der Handy-Signatur durchgeführte Signaturen mit der Person
  - ermöglicht Identifizierung des Signators auf Basis des Zentralen Melderegisters (ZMR) oder Ergänzungsregisters für natürliche Personen (ERnP)
  - somit Grundlage für e-Government
  - Inhalt: Name ohne Titel, Geburtsdatum, verschlüsselte ZMR-Zahl

Um einen Abgleich zwischen dem Zentralen Melderegister bzw. dem Ergänzungsregister für natürliche Personen (ERnP) und dem auszustellenden Zertifikat (= Personenbindung) herzustellen, werden *Vorname*, *Familienname* und *Geburtsdatum*, die während der Aktivierung angegebenen werden, mit dem ZMR verglichen. Sollte es hier zu einem Fehler kommen (keine Person mit den entsprechenden Daten gefunden bzw. mehrere Personen mit denselben Daten vorhanden), so muss der Eintrag im Zentralen Melderegister durch den Signator korrigiert werden (sofern die Daten, die bei der Aktivierung aus dem Ausweis übernommen wurden, in Ordnung sind). Dies kann am zuständigen Melde- bzw. Gemeindeamt erfolgen. Die Eingabe der Postleitzahl ist zwar kein Pflichtfeld, erleichtert aber den Abgleich mit den Daten im ZMR oder ERnP.

Solange keine Personenbindung erstellt werden kann, ist eine Ausstellung des Zertifikats nicht möglich. Soll eine Person zum Zwecke der Ausstellung einer Handy-Signatur im ERnP eingetragen werden, so kann dies bei der Datenschutzbehörde beauftragt werden (https://www.dsb.gv.at).

2.2 Erstellung einer Signatur

Im Laufe der Aktivierung der Handy-Signatur wird durch den User ein Signaturpasswort festgelegt, das aus sechs bis zwanzig (alpha)numerischen Zeichen (= Ziffern, Buchstaben und Sonderzeichen) bestehen

muss. Mit diesem Signaturpasswort wird der private Schlüssel des Signators geschützt. Das Signaturpasswort wird somit für die Erstellung von Signaturen benötigt und gewährleistet dadurch den alleinigen Zugriff durch den Signator.

Um eine Handy-Signatur durchzuführen, befüllt der Signator die dafür vorgesehene Maske in der gewünschten Applikation mit seiner Handynummer und dem Signaturpasswort. Nur die erfolgreiche Kombination dieser beiden Werte führt zum Auslösen einer Signatur (z.B. Versand einer TAN per SMS, TAN-Anzeige in der App oder speed-sign Verfahren mittels Handy-Signatur App, siehe Kapitel 5). Die Mittel der Signaturauslösung (z.B. TAN, QR-Code, biometrische Daten) sind in der Regel **fünf Minuten** gültig.

Schritte zur Durchführung einer Signatur:

1. Eingabe der Handynummer (+43…) und des zugehörigen Signaturpassworts
2. Optional: Überprüfung durch Anzeige der zu signierenden Daten und/oder Kontrolle der Vergleichswerte im Browserfenster und in der SMS bzw. App
3. Signaturauslösung mittels TAN per SMS, TAN-Anzeige in der App oder speed-sign Verfahren (QR-Code Scannen oder Eingabe der biometrischen Daten)

Achtung: Die Benutzung etwaiger Zusatzsoftware wie einer Bürgerkartenumgebung ist NICHT notwendig.

2.3 Gültigkeit der Zertifikate

Wie bei den meisten a.sign premium Produkten üblich, werden Handy-Signatur-Zertifikate für fünf Jahre ausgestellt.

2.4 Widerruf und Sperre

Das Sicherheitskonzept von a.sign premium sieht vor, dass eine Signatur als „sicher“ gilt, da ausschließlich der Signator über *Besitz* (SIM-Karte bzw. Handy) und *Wissen* (Signaturpasswort) verfügt. Wird das Handy inklusive SIM-Karte beispielsweise gestohlen, so ist die Gesamtsicherheit nicht mehr gewährleistet – die Zertifikate müssen somit umgehend widerrufen werden (Pflicht des Signators laut Merkblatt zur Kenntnis genommen). Ein Widerruf ist daher täglich rund um die Uhr möglich.

Ein Widerruf kann sowohl telefonisch (01 715 20 60) als auch per Fax erfolgen (Formular und Nummer unter www.a-trust.at/widerruf). In beiden Fällen ist die Nennung des selbst gewählten Widerrufspasswortes erforderlich (wird vom Signator im Registrierungsvorgang festgelegt). Die Angabe des Widerrufspasswortes ist notwendig, um einen Widerruf durch eine andere Person als den Zertifikatsinhaber zu verhindern. Ist dem Signator das Widerrufspasswort entfallen, so ist es möglich das **Zertifikat zu sperren**. In diesem Fall wird der Signator per Brief an seinen aus dem ZMR übernommenen Hauptwohnsitz von der Sperre seiner Zertifikate informiert und kann diese im gegebenen Fall mit seinem

Sperraufhebungs-Passwort (wird bei der Sperre telefonisch definiert) wieder aufheben. Nach zehn verstrichenen Kalendertagen geht eine Sperre automatisch in einen Widerruf über.

Ein Widerruf wirkt sofort und ist endgültig, einmal widerrufene Zertifikate sind nicht wiederherstellbar!

2.5 Kontakt und Support

Treten Probleme beim Registrierungsprozess auf, so ist zuerst selbstständig der (z)RO-Bereich (https://www.a-trust.at/zro/) zu frequentieren. Dort werden in digitaler Form Handbücher, Merkblätter und andere Hilfestellungen veröffentlicht. Auch eine Liste der Sicherheitsmerkmale der von A-Trust akzeptierten Ausweisdokumente ist dort einsehbar.

Kann an dieser Stelle keine Lösung gefunden werden, so sollte zuerst der zuständige zRO (zentraler Registration Officer) kontaktiert werden. Ist der zRO nicht in der Lage das Problem zu lösen, so verfügt er über zusätzliche Informations- und Supportkanäle, über die Hilfe angefordert werden kann.

2.6 Ausweise

Von A-Trust akzeptierte Ausweisdokumente

- Internationaler Reisepass
- Österreichischer Führerschein (nur österreichische Führerscheine werden akzeptiert!)
- Österreichischer Personalausweis
- Deutscher Personalausweis
- Österreichische Identitätskarte
- Schweizer Identitätskarte
- Liechtensteinische Identitätskarte
- Apothekerausweis
- Notarausweis
- Rechtsanwaltsausweis
- Dolmetscherausweis
- Ziviltechnikerausweis
- Sachverständigenausweis
- Studentenausweise
- Behindertenpass
- eDA Dienstausweis Republik Österreich
- EDU-Card
- Gemeindeausweis
- Waffenbesitzkarte
- Waffenpass

Anforderungen an die Ausweisprüfung

- Stimmt das Lichtbild mit dem Zertifikatswerber überein?
- Ist der Inhalt klar lesbar (Sprache Deutsch oder Englisch, keine Vergilbung und Verschmutzung)?
- Ist das Ablaufdatum nicht überschritten (auch bei Reisepässen)?
- Weist der Ausweis die (erkennbaren) Sicherheitsmerkmale auf (Gesamteindruck des Ausweises)?
- Ist der Ausweis nicht älter als 40 Jahre (wird vom System automatisch abgelehnt)?

AUSNAHME: Wenn am verwendeten Ausweis kein Ausstellungsdatum aufgedruckt ist, bitte das Datum vom Vortag der Registrierung eintragen!

Bei Bedenken hinsichtlich mindestens eines Kriteriums kann der RO die Vorlage eines anderen Ausweises aus der Liste der von A-Trust akzeptierten Dokumente verlangen.

Falls Sie bei der Kontrolle der Ausweisdokument nicht sicher sind, können Sie auf die digitale Liste bzgl. der „Sicherheitsmerkmale bei Ausweisen“ (https://www.a-trust.at/zro/) zurückgreifen. In dieser Aufstellung finden Sie die akzeptierten Ausweisdokumente inklusive Beschreibung. Bei Unsicherheit über die Sicherheitsmerkmale steht auch „PRADO - Das öffentliches Online-Register echter Identitäts- und Reisedokumente“ unter http://www.consilium.europa.eu/prado/de/prado-start-page.html zur Einsichtnahme zur Verfügung.

3. Anforderungen

3.1 Anforderungen für die Ausstellung einer Handy-Signatur

Um eine Handy-Signatur erfolgreich zu aktivieren, müssen folgende Rahmenbedingungen gegeben sein:

- Besitz eines Handys mit SIM-Karte eines österreichischen Mobilfunkproviders
- der Signator muss das 14. Lebensjahr vollendet haben
- bei der RO Aktivierung ist die Vorlage eines amtlichen **und gültigen** Lichtbildausweises notwendig

3.2 Anforderungen an den Arbeitsplatz

Technische Anforderungen

- Internetanschluss (mindestens ISDN)
  - TCP-Port 443 (SSL)
  - TCP-Port 80 (Web)
- Internetbrowser
- Optional: Drucker für den Signaturvertrag
- RO: aktives qualifiziertes Zertifikat (Bürgerkarte oder Handy-Signatur) mit bei A-Trust hinterlegten Handy-Signatur RO-Rechten. Eine Anforderung der RO-Rechte kann durch den zRO per E-Mail angefordert werden.

- *Optional (wenn eine Smartcard-Bürgerkarte für die Signatur des RO verwendet wird):*
- Smart Card Reader mit PIN-Pad z.B.
  - Reiner SCT Cyberjack (pinpad oder e-com)
  - SCM Microsystems Chipdrive Pinpad
- Bürgerkartenumgebung (eine der Optionen)
  - a.sign Bürgerkartensoftware in Kombination mit dem a.sign Client
  - BKUOnline
    - PC/SC 2.0 Treiber für Kartenleser
    - Java ab Version 1.6 (aktuellste Version empfohlen)
    - Für Reiner – Kartenleser: mindestens Treiber Version 6.0
    - für SCM – Kartenleser: mindestens Firmware - Version 5.10

Organisatorische Anforderungen

- aufliegende Dokumente
  - Unterrichtung in größerer Zahl, Übergabe an den Kunden bei Registrierung
  - RO – Handbuch zum Nachschlagen für den RO
  - RO – Mappe
    - Zertifizierungsrichtlinie

- Anwendungsvorgaben
- AGBs
- Blanko-Signaturvertrag

Sicherheitsanforderungen laut Arbeitsplatzanforderungen

- Auf dem Rechner ist nur die für die jeweilige Funktion des Arbeitsplatzes notwendige Software installiert.
- Der Rechner besitzt nur die für die jeweilige Funktion des Arbeitsplatzes notwendigen Kommunikationsschnittstellen. Insbesondere sind die Rechner nur in die für ihre Funktion notwendigen Teilnetzwerke integriert.
- Unnötige Funktionen des Betriebssystems und der installierten Software werden – sofern möglich – deaktiviert.
- Falls Sicherheitsrisiken in der verwendeten Software bekannt werden, ergreifen die Systemadministratoren die vom Hersteller bzw. von unabhängigen Experten empfohlenen Gegenmaßnahmen. Insbesondere werden beim Betriebssystem und der Software stets die aktuellen Patches gegen bekannte Sicherheitslücken eingespielt.
- Der Zugriff auf die Rechner ist auf das für den Betrieb des Arbeitsplatzes notwendige Maß beschränkt. Insbesondere werden die Rechner nur durch die verantwortlichen Systemadministratoren verwaltet.
- Nicht mehr benötigte Daten werden von den Rechnern gelöscht. Die Löschung erfolgt in einer Weise, die eine teilweise oder vollständige Rekonstruktion unmöglich macht.
- Sicherheitskritische Ereignisse auf den Rechnern werden protokolliert.
- Auf den Rechnern dürfen Systeme nur von Viren geprüften Datenträgern verwendet werden.
- Die Sicherheit der Systeme wird von den in der Registrierungsstelle verantwortlichen Administratoren regelmäßig (nach jeder relevanten Modifikation des Systems, mindestens aber halbjährlich) mittels geeigneter Software geprüft. Bei gefundenen Sicherheitslücken werden sofort entsprechende Gegenmaßnahmen eingeleitet.
- Modifikationen der Systeme werden zuerst an Testsystemen erprobt und vor der Anwendung am Produktivsystem die relevanten Systemdaten gesichert.
- Sofern der Zugang in öffentliche Netze nicht oder nicht ausschließlich über LAN möglich ist (z.B. bei mobilen Endgeräten) sollte der Arbeitsplatzrechner über eine Software-Firewall verfügen.

4. Aktivierungsprozess

Prinzipiell wird zwischen zwei Aktivierungsarten unterschieden: der Heimaktivierung durch den Signator sowie der Aktivierung in der Registrierungsstelle. Das aus der Aktivierung resultierende Zertifikat ist in beiden Fällen identisch.

Online Aktivierung	**Registrierungsstelle**
Kunde führt Prozess selbstständig durch Authentifizierung mittels bestehender Bürgerkarte bzw. über externe Plattformen, in welchen der Kunde bereits voridentifiziert ist (z.B. FinanzOnline,…) Dauer: ca. 10 Minuten bei bestehender BK bzw. min. 3 Tage über externe Plattformen (Briefversand)	RO unterstützt Kunden bei der Aktivierung Authentifizierung durch RO Dauer: ca. 10 Minuten
Dauer technischer Ablauf: ca. 3 Minuten	

Um die Authentifizierung durch den RO zu bestätigen, muss dieser die Antragstellerdaten signieren Hierzu kann jedes qualifizierte Zertifikat von A-Trust verwendet werden (a.sign premium Karten, e-cards, Handy-Signatur), welches auch dafür legitimiert (= für die RO-Tätigkeit berechtigt) wurde.

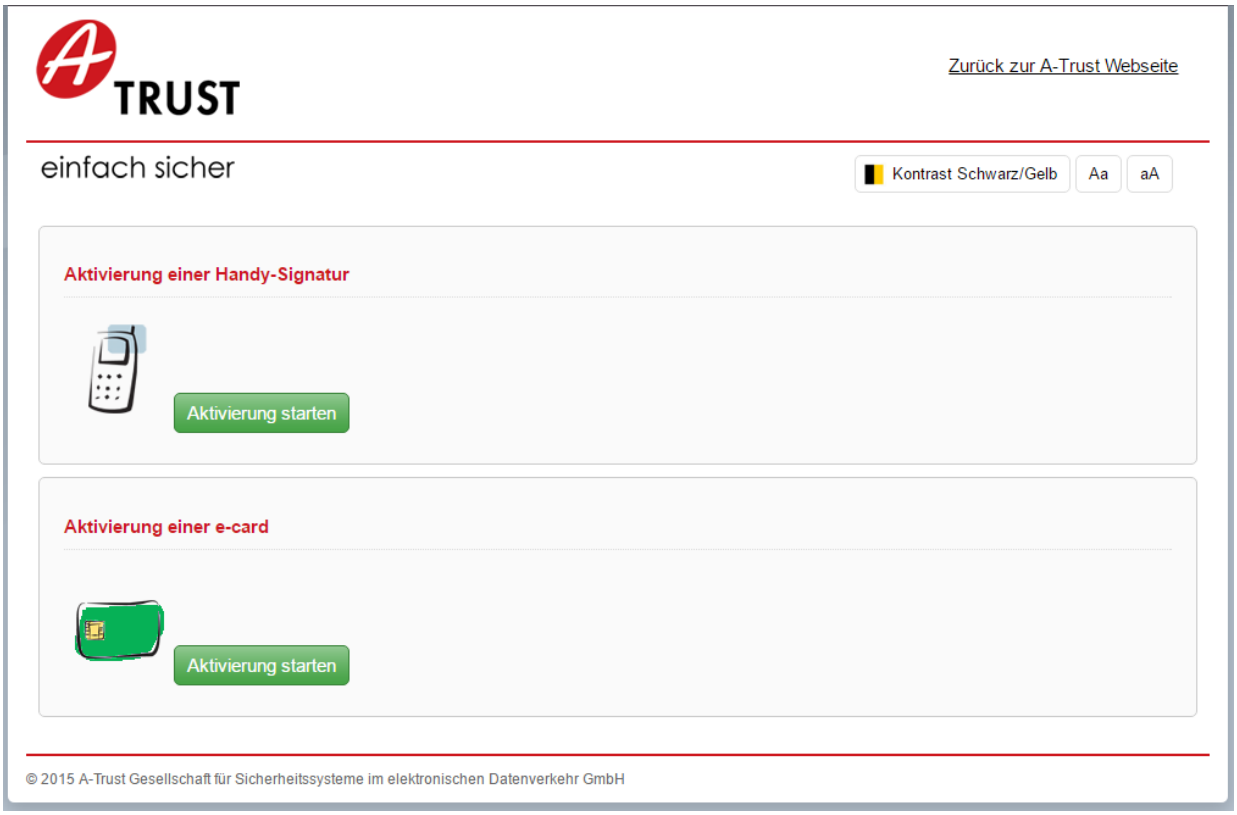
Detaillierte Erklärungen zur Online Aktivierung mittels bestehender Bürgerkarte bzw. über externe Plattformen sind unter https://www.a-trust.at/hsaktivierung zu finden.

4.1 Aktivierung in der Registrierungsstelle

Die Aktivierung in der Registrierungsstelle startet unter der URL https://www.a-trust.at/Aktivierung/ro und kann in die zwei Teilbereiche Authentifizierung und Zertifikatsausstellung aufgeteilt werden. Der zweite Bereich, die Zertifikatsausstellung, ist für alle Prozesse (Online Aktivierung bzw. Aktivierung durch den RO in der Registrierungsstelle) identisch, weshalb der Kunde dies nach der Authentifizierung durch einen RO auch selbstständig durchführen kann.

4.1.1 Authentifizierung (https://www.handy-signatur.at/aktivierung/ro/)

Im ersten Schritt muss das für die Aktivierung gewünschte Trägermedium - in diesem Fall die Handy-Signatur – ausgewählt werden. Der Registrierungsprozess startet nach einem Klick auf „Aktivierung starten“ im Feld der Handy-Signatur.



Danach erscheint die Eingabemaske, die vom RO zu befüllen ist. Felder mit einem roten * sind Pflichtfelder und müssen zwingend ausgefüllt werden. Hilfestellung zu einzelnen Feldern können über die ?-Symbole angezeigt werden. Bevor das Formular abgesendet wird, erfolgt eine Plausibilitätsprüfung der einzelnen Felder. Im Fehlerfall wird das falsch befüllte Feld markiert und am Ende nochmals angeführt.

TRUST

einfach sicher

Zurück zur A-Trust Webseite

Kontrast Schwarz/Gelb | Aa | aA

Aktivierung einer Handy-Signatur

Alle mit * gekennzeichneten Felder sind zwingend erforderlich.

Mobiltelefonnummer des Signators/Kunden *

Bitte auswählen

Antragstellerdaten

Anrede *

Herr

Titel

Vorname *

Nachname *

E-Mail Adresse

Geburtsdatum *

TT . MM . YYYY

Postleitzahl der Meldeadresse

Widerruf / Sperre

Widerrufspasswort *

Identitätsnachweis

Ausweis *

Bitte auswählen

Ausweisnummer *

Ausstellungsdatum *

TT . MM . YYYY

Behörde *

Ausstellende Nation *

Österreich

Karte

Mobiltelefon

Das erste Feld erfordert die Eingabe der Handynummer des Signators – auswählbare Vorwahlen werden mittels Dropdown-Feld angezeigt.

Die Daten für die nächste Gruppe von Feldern werden vom RO aus dem Ausweis des Signators übernommen und in die Maske eingetragen. Näheres zu den akzeptierten Ausweisen finden Sie im entsprechenden Kapitel (siehe Kapitel 2.6). Die Erfassung der Ausweisdaten dient der Identifizierung des Signators. Im nächsten Schritt signiert der RO diese Daten und garantiert somit für deren Korrektheit.

Die Felder Telefonnummer, E-Mail-Adresse und Widerrufspasswort (4 bis 10 Zeichen alphanumerisch – je nach Verwendung case sensitive) müssen vom Kunden erfragt werden. Die Kontaktdaten (Telefonnummer, E-Mail-Adresse) sind hierbei optional, werden sie angegeben so bleiben sie auch im System gespeichert. A-Trust verarbeitet diese Daten ausschließlich zum Zweck der Erbringung von Vertrauensdienstleitungen in Vertragserfüllung.

ANMERKUNG: Die E-Mail-Adresse sollte unbedingt erfragt werden. Nur wenn diese im Datensatz vorhanden ist, kann der Signator vor Ablauf seines Zertifikates durch A-Trust erinnert werden, dass die Handy-Signatur verlängert werden muss.

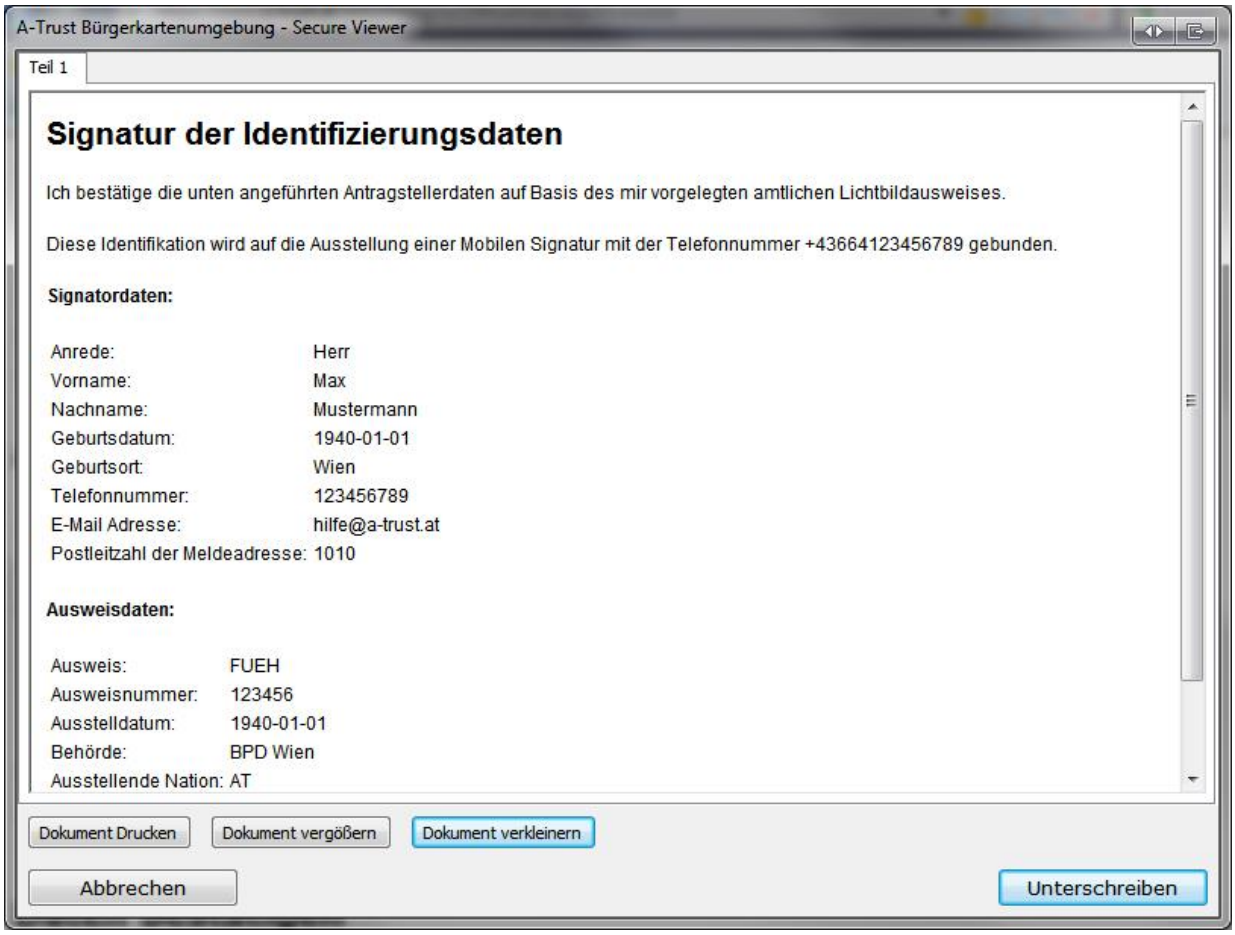
Sind alle Daten eingegeben, wird dies mit einem Klick auf einem der beiden Buttons unter dem Formular bestätigt, wobei der RO hier entscheidet, ob er die Signatur mit einem kartengebundenen Zertifikat (z.B. e-card) oder mittels Handy-Signatur durchführen möchte. Der RO muss vorher bereits von A-Trust für die Aktivierung von Handy-Signaturen berechtigt worden sein!

Option 1: Signatur der Identifizierungsdaten mittels Handy-Signatur:

Wurde der Button „Mobiltelefon“ für die Signatur gewählt, so muss der RO im nächsten Schritt mit Handy-Signatur unterschreiben. Mit dieser Unterschrift bestätigt der RO, dass er den Signator unterrichtet hat (Unterrichtung gemäß Artikel 24 Abs 2 lit d eIDAS-Verordnung) und dass die Übereinstimmung des Signators mit dem vorgelegten Lichtbildausweis überprüft wurde. Hierzu gibt der RO die Daten seiner Handy-Signatur (Mobiltelefonnummer sowie Signaturpasswort) an und bestätigt den Vorgang über „Identifizieren“. Danach startet der Vorgang der Signaturauslösung (z.B. SMS-TAN, QR-Code scannen, Eingabe biometrischer Daten, siehe Kapitel 5).

Über den Link „Signaturdaten anzeigen“ kann der RO die zu signierenden Daten nochmals überprüfen. Nach erfolgter Signatur ist der erste Schritt (**Authentifizierung**) abgeschlossen, es erfolgt eine automatische Weiterleitung zur Zertifikatserstellung.

Option 2: Signatur der Identifizierungsdaten mittels Bürgerkarte und a.sign Bürgerkartensoftware:



Wird die a.sign Bürgerkartensoftware (lokale Bürgerkartenumgebung) ausgewählt, so öffnet sich nach kurzer Wartezeit automatisch ein Fenster, in dem die eingegebenen Daten angezeigt werden. Nach einem Klick auf „Unterschreiben“ wird der RO aufgefordert, den Signatur-PIN (6-stellig) einzugeben, um die Identifizierungsdaten zu signieren.

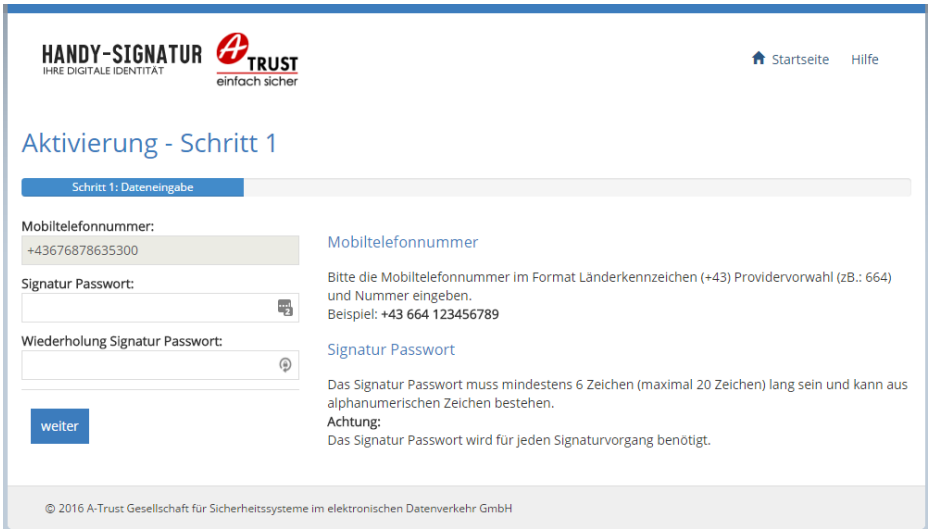
Mit dieser Unterschrift bestätigt der RO, dass er den Signator unterrichtet hat (Unterrichtung gemäß Artikel 24 Abs 2 lit d eIDAS-Verordnung) und dass die Übereinstimmung des Signators mit dem vorgelegten Lichtbildausweis überprüft wurde.

4.1.2 Zertifikatsausstellung

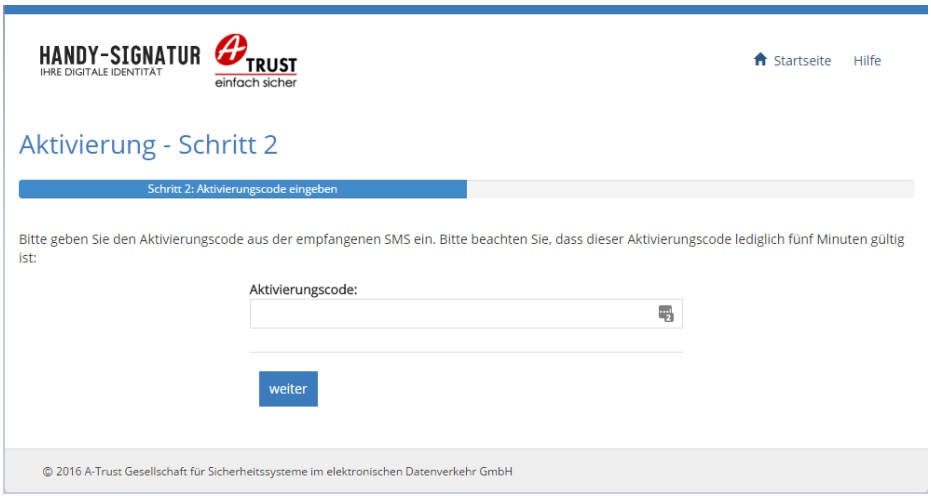
Nach dem Prozess erscheint nach der Signatur der Signator-Identifikationsdaten durch den RO automatisch die nächste Eingabemaske, in der das Signaturpasswort festgelegt werden muss (Aktivierung Schritt 1).

Die Handynummer, die bei der Erfassung der Signator-Daten bereits gespeichert wurde, ist hierbei vorausgefüllt und nicht mehr änderbar! (Bei Tippfehlern muss der Aktivierungsprozess neu begonnen werden)

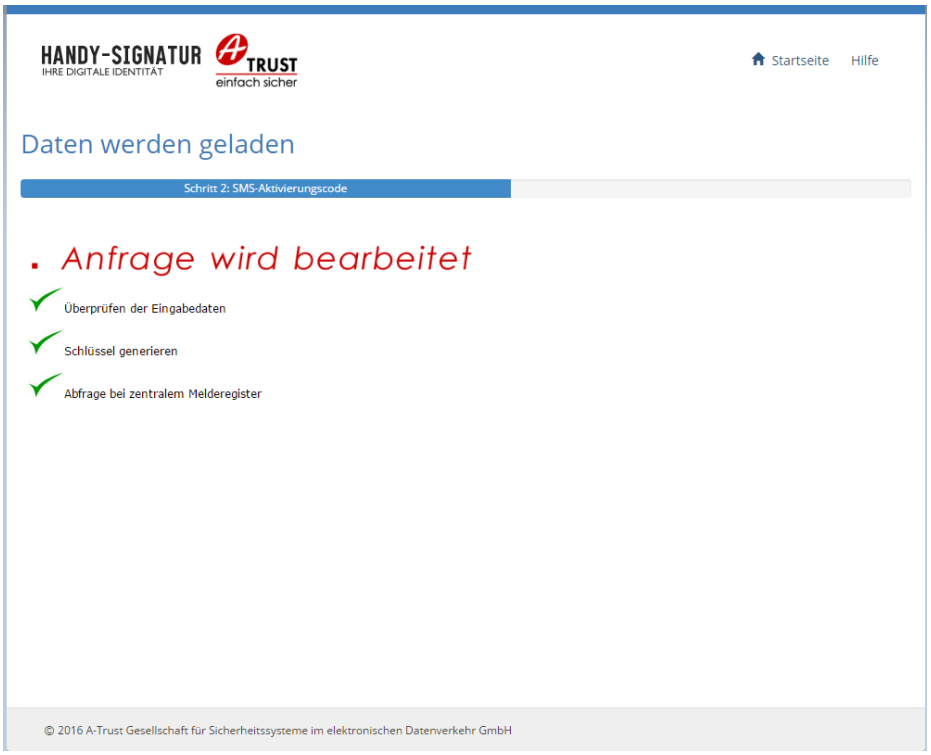
Der Signator wählt hier sein gewünschtes Signaturpasswort (mindestens 6 Zeichen case sensitive; Buchstaben, Sonderzeichen und Ziffern möglich), das für jeden Signaturvorgang benötigt wird. Der Prozess wird durch einen Klick auf „weiter“ fortgesetzt. Dadurch wird eine SMS mit einem Aktivierungscode für die angegebene Handynummer angefordert.



Im nächsten Schritt muss der Aktivierungscode, den der Signator per SMS erhält, eingegeben werden, um die Verknüpfung des Zertifikates mit der Mobilfunknummer zu ermöglichen. Auch hier wird der Vorgang mittels „weiter“-Button fortgesetzt.

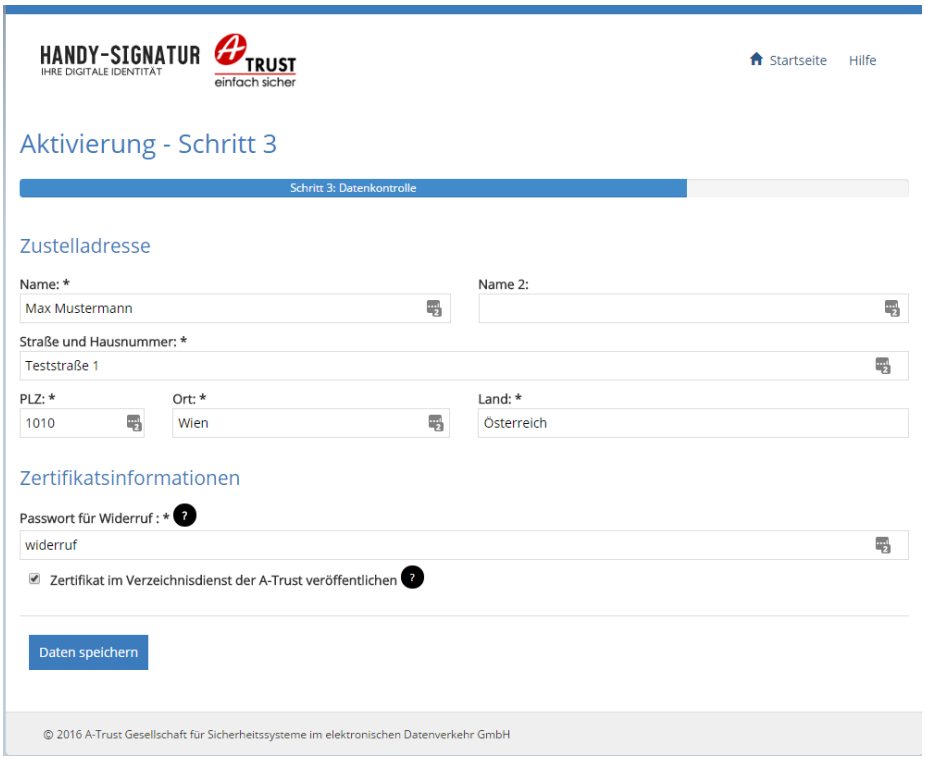


Es folgt die Überprüfung der Daten und die Herstellung der Personenbindung.



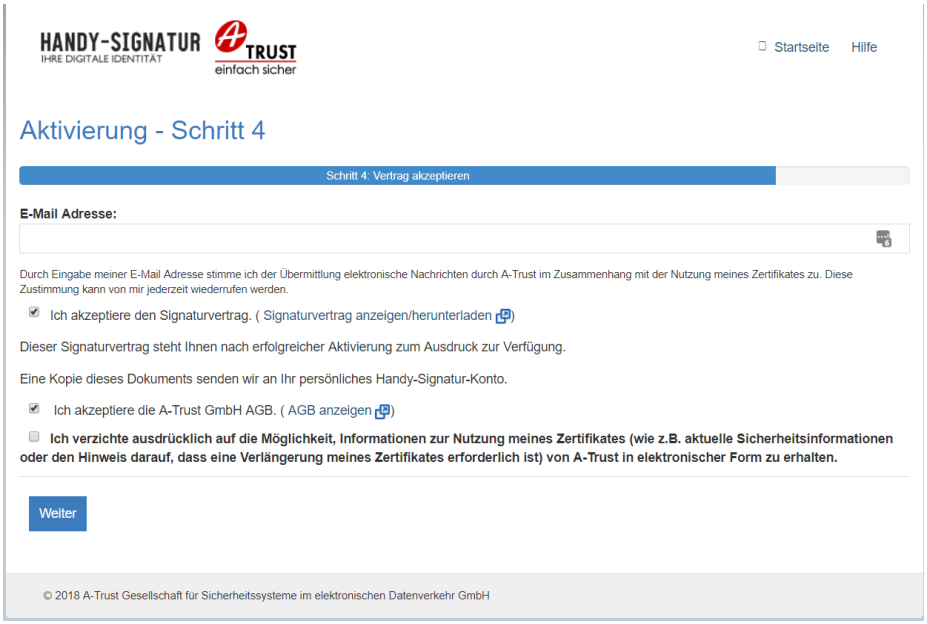
Schritt 3 sieht die Kontrolle der ausgelesenen Daten vor.

Nach einer Kontrolle der hinterlegten Werte und einer optionalen Anpassung der Zustelladresse wird der Schritt über den Button „Daten speichern“ abgeschlossen.

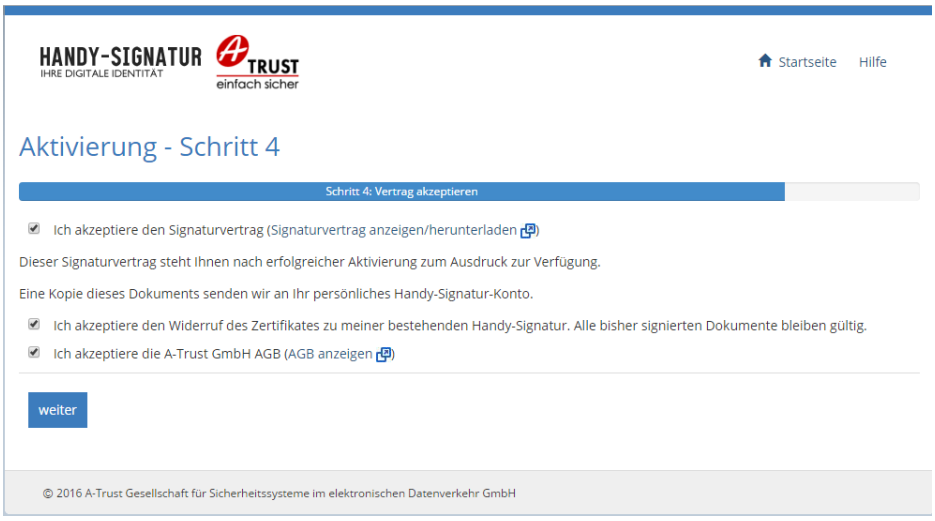


Im vierten Schritt wird durch das Akzeptieren des Signaturvertrags sowie der AGB der Prozess abgeschlossen. Beide Checkboxen müssen aktiviert sein, bevor der „weiter“ Button geklickt wird, um die Zertifikatsausstellung abzuschließen.

Falls keine E-Mail-Adresse angegeben wird, erscheint eine weitere Checkbox. Mit dieser erklärt der Signator, dass er ausdrücklich auf die Bekanntgabe einer E-Mail-Adresse verzichtet und zur Kenntnis nimmt, dass relevante Informationen ggf. nicht elektronisch zugestellt werden können. (A-Trust verarbeitet die Signator-Daten ausschließlich zum Zweck der Erbringung von Vertrauensdienstleitungen in Vertragserfüllung. Weitere Informationen zum Datenschutz: https://www.a-trust.at/sicherheit/datenschutz)



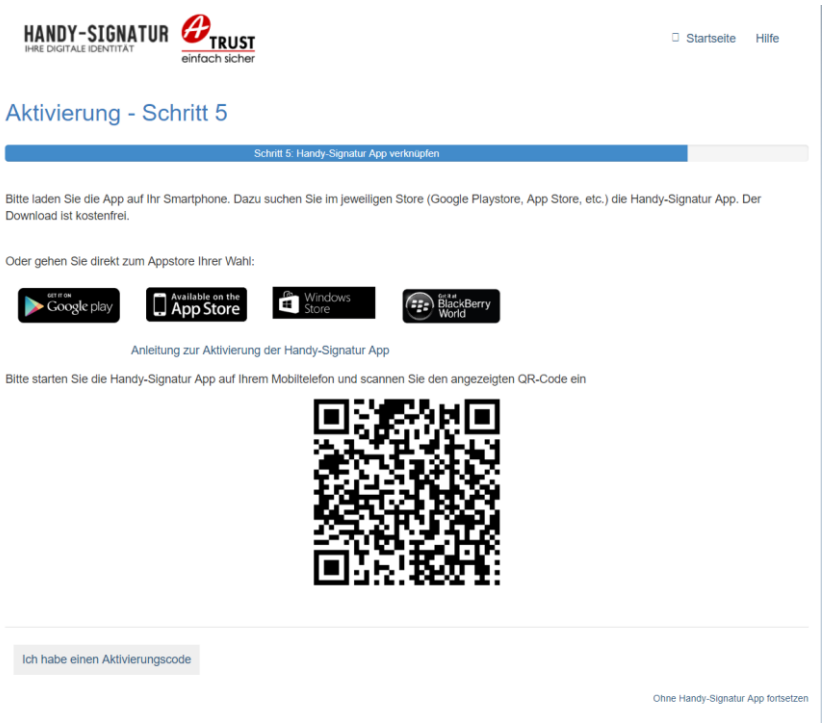
Ist für die zu aktivierende Nummer bereits ein Zertifikat ausgestellt, so erfolgt ein automatischer Widerruf des alten Zertifikats mit der Neuausstellung. In diesem Fall wird an dieser Stelle eine zusätzliche Checkbox angezeigt, über die der Widerruf akzeptiert wird.



Abschließend werden die Zertifikate ausgestellt und somit der Prozess für die Aktivierung der Handy-Signatur beendet. Um die korrekte Funktionsweise zu testen, kann ein Login (z.B. FinanzOnline) durchgeführt werden.

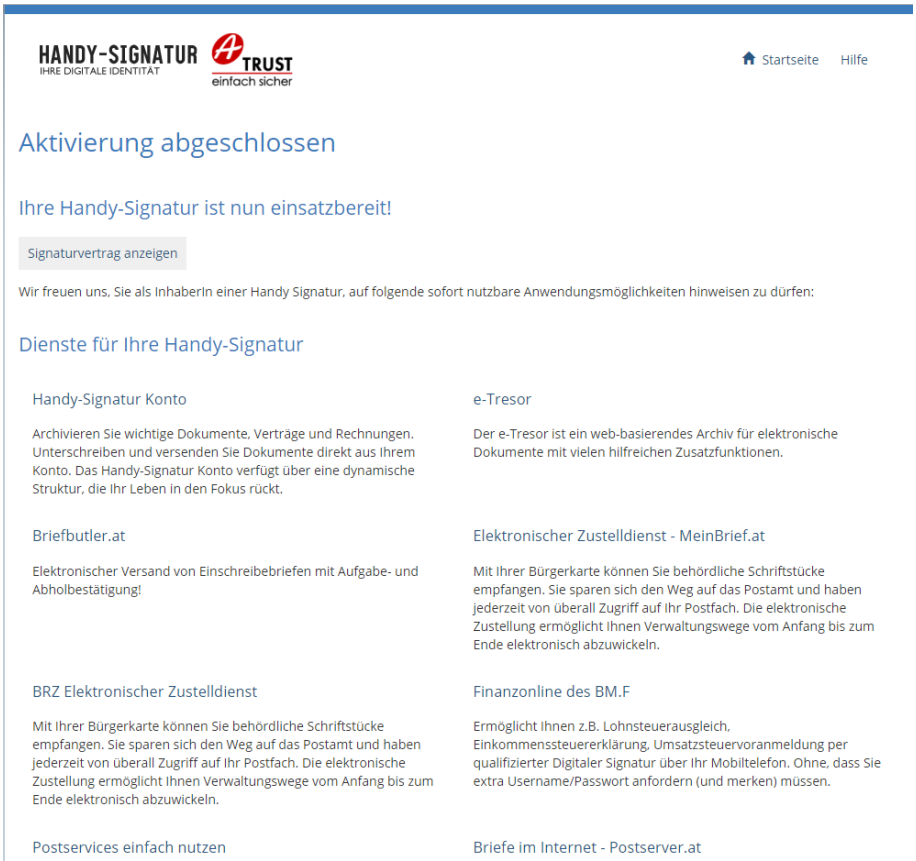
Im nächsten Schritt kann optional die Handy-Signatur App aktiviert werden. Dafür wird eine Verbindung zwischen der Handy-Signatur und der Handy-Signatur App hergestellt. Für die Aktivierung der App muss diese bereits aus dem jeweiligen Store (App Store / Google Play Store) heruntergeladen und auf dem Smartphone installiert sein.

Mithilfe des angezeigten QR-Codes können Sie direkt die bereits am Smartphone installierte App aktivieren. Alternativ kann mittels numerischem Aktivierungscode aktiviert werden (weitere Informationen siehe Kapitel 5). Falls keine App aktiviert werden soll, klicken Sie bitte auf „Ohne Handy-Signatur App fortsetzen“.



Nach Beendigung des Prozesses erhalten Sie eine Bestätigung.

In der Übersicht werden Dienste für die Nutzung mit der Handy-Signatur dargestellt. Nähere Informationen zur Verwendung der Handy-Signatur App erhalten Sie in Kapitel 5.



5 Handy-Signatur App

Ohne Verwendung der Handy-Signatur App wird dem Signator bei jedem Signaturvorgang eine TAN per SMS zugestellt: Nach Eingabe des Handynummer (+43…) und dem zugehörigen Signaturpasswort wird diese SMS versendet. Der Signator muss innerhalb von 5 Minuten die TAN in das Eingabefeld im Browserfenster übertragen (abtippen), um die Signatur durchzuführen.

Die Handy-Signatur App ersetzt das SMS TAN Verfahren und bietet Unterstützung bei der Durchführung von Signaturen. Mithilfe der speed-sign Verfahren kann beispielsweise noch schneller und komfortabel signiert werden: Die Signaturauslösung erfolgt, indem ein QR-Code gescannt oder biometrische Daten eingegeben werden – bequem, einfach und sicher.

Die Verwendung der Handy-Signatur mittels App wird automatisch von allen Diensten unterstützt, welche die Handy-Signatur verwenden. Download und Nutzung der App sind kostenfrei (etwaige Entgelte für die Nutzung mobiler Datendienste sind hierbei ausgenommen).

Die Handy-Signatur App ist für folgende Betriebssysteme verfügbar und kann über die zugehörigen Stores bezogen werden:

- **Android** ab Version 4.1
  https://play.google.com/store/apps/details?id=at.atrust.tanapp

- **iOS** ab Version 9.0
  https://itunes.apple.com/us/app/handy-signatur-app/id1016945247?l=de&ls=1&mt=8

Um die Handy-Signatur App nutzen zu können, muss diese nach Download aus dem jeweiligen App-Store (App Store / Google Play Store) mit der Handy-Signatur verbunden (aktiviert) werden. Nachdem diese Aktivierung der App erfolgreich durchgeführt wurde, können die Funktionen der App, wie etwa die speed-sign Verfahren genutzt werden. Die App ersetzt das SMS TAN Verfahren.

Die Verbindung der App mit der Handy-Signatur (Aktivierung der App) kann **direkt im Anschluss an die Aktivierung der Handy-Signatur** durchgeführt werden. Alternativ kann die App auch zu einem späteren Zeitpunkt heruntergeladen und aktiviert werden, bspw. um nach dem Wechsel des Endgeräts weiterhin die App nutzen zu können.

ANMERKUNG: Eine bestehende Verbindung sollte jedenfalls gelöst werden, bevor das Endgerät dauerhaft an eine andere Person weitergeben wird.

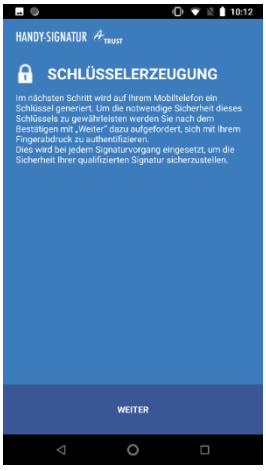
5.1 Handy-Signatur App – Aktivierung mit QR-Code

Direkt nach Abschluss des Aktivierungsprozesses der Handy-Signatur wird im Browserfenster ein QR-Code angezeigt, mit dem der Aktivierungsprozess für die App einfach und rasch gestartet werden kann. Mit diesem Prozess wird die Handy-Signatur mit der App auf dem Smartphone des Signators verbunden. (Gegebenenfalls kann zu einem anderen Zeitpunkt via www.a-trust.at/appaktivierung die Aktivierung gestartet werden.)

Für die Aktivierung muss der Signator die App bereits auf seinem Smartphone installiert haben.
In der App sollte der Status „NICHT VERBUNDEN“ angezeigt werden. Die Aktivierung der App wird mit einem Klick auf „JETZT AKTIVIEREN“ gestartet.

Im nächsten Schritt wird aus Sicherheitsgründen auf dem Mobiltelefon ein Schlüssel generiert, bitte lassen Sie den Signator dies mit „WEITER“ bestätigen. Diese Sicherheitseinstellung verhindert die missbräuchliche Verwendung der Handy-Signatur, wenn das Mobiltelefon unbeaufsichtigt ist. Ohne diesen Zwischenschritt kann die Aktivierung der App nicht abgeschlossen werden.

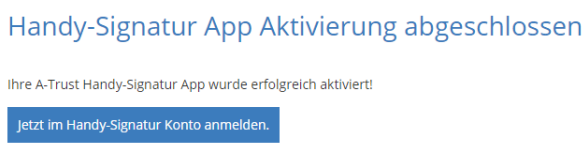
Um die Sicherheit des Schlüssels zu gewährleisten, ist es erforderlich, dass der Signator sich mittels biometrischer Daten (Fingerabdruck oder Gesichtserkennung, sofern vom Gerät/Betriebssystem unterstützt) authentifiziert. Die biometrischen Daten müssen hierfür bereits auf dem Smartphone hinterlegt sein. Falls eine Bestätigung mittels biometrischer Daten nicht möglich ist, kann alternativ eine Sicherheits-PIN festgelegt werden (siehe Kapitel 5.3).



Danach ist es erforderlich der App zu erlauben auf die Smartphone-Kamera zuzugreifen, um den Prozess zu starten. (Falls der Signator keinen Zugriff auf die Kamera erlauben möchten, steht die Aktivierung der App mittels numerischem Aktivierungscode zur Verfügung; siehe Kapitel 5.2.) Sobald die App auf die

Kamera zugreift, kann der im Browser angezeigte QR-Code gescannt und damit die Verbindung zwischen Handy-Signatur und App hergestellt werden.

Nach Beendigung des Prozesses ist die Handy-Signatur erfolgreich mit der App verknüpft.
Im Webbrowser sehen Sie folgende Meldung:



5.2 Handy-Signatur App – Aktivierung mit numerischem Code

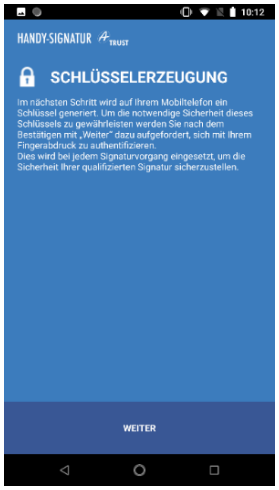
Für die Aktivierung muss der Signator die App bereits auf seinem Smartphone installiert haben.
Falls der Signator der Handy-Signatur App keinen Zugriff auf die Smartphone-Kamera gewähren möchte, kann alternativ auch mithilfe eines numerischen Aktivierungscode die Handy-Signatur App aktiviert werden. (Ohne Zugriff auf die Smartphone-Kamera können die Möglichkeiten der Signaturauslösung, welche auf die Kamera zugreifen, natürlich nicht genutzt werden.)

Direkt nach Abschluss des Aktivierungsprozesses der Handy-Signatur wird im Browserfenster ein QR-Code angezeigt, darunter wird „Ich habe einen Aktivierungscode“ zur Auswahl angeboten – bitten Sie den Signator auf diese Anzeige zu klicken. Anschließend wird ein Eingabefeld für den numerischen Aktivierungscode angezeigt. Der Signator darf anschließend das Browserfenster nicht schließen, und muss die App am Mobiltelefon starten. In der App sollte der Status „NICHT VERBUNDEN“ angezeigt werden. Der Signator muss nun die Aktivierung in der App mit einem Klick auf „JETZT AKTIVIEREN“ starten.

Gegebenenfalls kann der Signator die Aktivierung via www.a-trust.at/appaktivierung zu einem anderen Zeitpunkt starten.

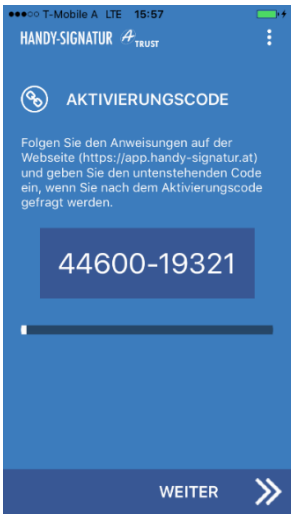
Im nächsten Schritt wird aus Sicherheitsgründen auf dem Mobiltelefon ein Schlüssel generiert, bitte lassen Sie den Signator dies mit „WEITER“ bestätigen. Diese Sicherheitseinstellung verhindert die missbräuchliche Verwendung der Handy-Signatur, wenn das Mobiltelefon unbeaufsichtigt ist. Ohne diesen Zwischenschritt kann die Aktivierung der App nicht abgeschlossen werden.

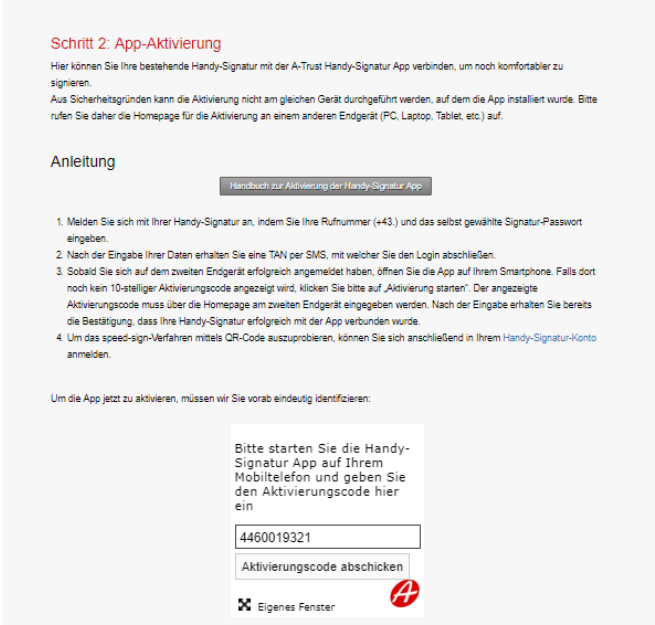
Um die Sicherheit des Schlüssels zu gewährleisten, ist es erforderlich, dass der Signator sich mittels biometrischer Daten (Fingerabdruck oder Gesichtserkennung, sofern vom Gerät/Betriebssystem unterstützt) authentifiziert. Die biometrischen Daten müssen hierfür bereits auf dem Smartphone hinterlegt sein. Falls eine Bestätigung mittels biometrischer Daten nicht möglich ist, kann alternativ eine Sicherheits-PIN festgelegt werden (siehe Kapitel 5.3).



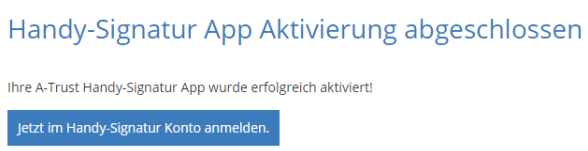
Um den Aktivierungscode einzugeben, kann der App der Zugriff auf die Kamera generell verweigert werden. Alternativ kann in der App bei der Anzeige „AKTIVIERUNGSCODE SCANNEN“ auf die Option „AKTIVIERUNGSCODE EINGEBEN“ unter dem Kamerafenster geklickt werden.

Danach wird in der App ein 10-stelliger numerischer Aktivierungscode angezeigt, welcher in das Eingabefeld im Browser (der Bindestrich ist für die Eingabe nicht erforderlich) übertragen werden muss – damit wird die Verbindung zwischen Handy-Signatur und App bestätigt und der Prozess ist beendet.



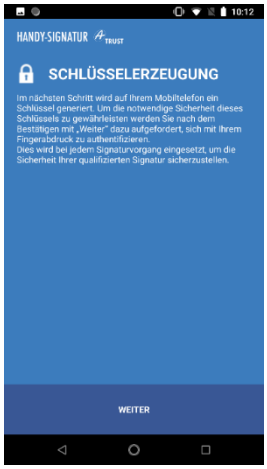


Nach Beendigung des Prozesses ist die Handy-Signatur erfolgreich mit der App verknüpft.
Im Webbrowser sehen Sie folgende Meldung:

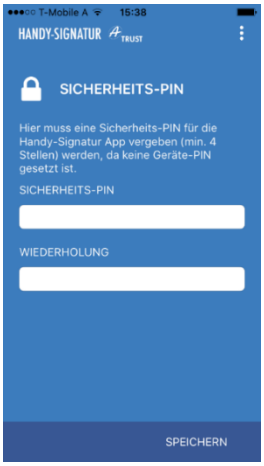


5.3 Handy-Signatur App Aktivierung: Schlüsselerzeugung mit Sicherheits-PIN

Ist die Verwendung von biometrischen Daten zur Sicherung der App auf dem Mobiltelefon nicht möglich, so kann der Signator eine Sicherheits-PIN für die App festlegen. Je nach Sicherheitseinstellungen des Gerätes bzw. je nach verwendetem Betriebssystem kann das Setzen der Sicherheits-PIN auch verpflichtend sein. Um die Schlüsselerzeugung mit Sicherheits-Pin durchzuführen muss diese mit „WEITER“ bestätigt, aber danach die Abfrage der biometrischen Daten abgebrochen werden.



Im nächsten Schritt wird ein Eingabefeld für die Sicherheits-PIN angezeigt. Hier kann der Signator die Sicherheits-PIN festlegen, bzw. den Vorgang durch „Später“ abbrechen. Die Sicherheits-PIN verhindert die missbräuchliche Verwendung der Handy-Signatur, wenn das Mobiltelefon unbeaufsichtigt ist.
Verlangen die Sicherheitseinstellungen des Gerätes bzw. das Betriebssystem das verpflichtende Setzen der Sicherheits-PIN entfällt der „SPÄTER“ Button im Prozess. Die Sicherheits-PIN verhindert die missbräuchliche Verwendung der Handy-Signatur, wenn das Mobiltelefon unbeaufsichtigt ist.



5.4 Handy-Signatur App – Signaturvorgänge durchführen

Nach erfolgter Aktivierung der Handy-Signatur App wird anstelle der gewohnten SMS TAN die App eingesetzt. Bei der Nutzung der Handy-Signatur gibt es keine Änderung zum gewohnten Ablauf, alle Handy-Signatur Dienste sind ohne Einschränkung nutzbar.

Der Signator kann zwischen verschiedenen Formen der Signaturauslösung wählen:

1. Eingabe von biometrischen Daten (Fingerabdruck oder Gesichtserkennung – sofern das Endgerät dies unterstützt),
2. Scannen eines QR-Codes mithilfe der Smartphone-Kamera oder
3. Anzeige der TAN direkt in der App.

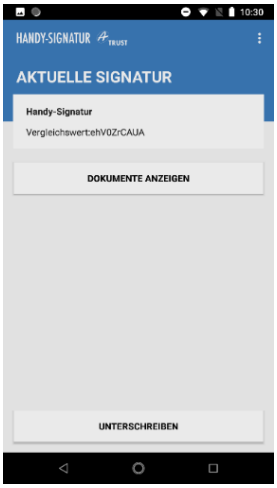
Sollte zum Zeitpunkt der Signatur keine Internetverbindung für das Handy verfügbar sein, so kann bei jedem Signaturvorgang eine TAN per SMS angefordert werden. Dieser Vorgang kann über die Auswahl von „TAN via SMS anfordern“ im Browser gestartet werden. Bei der nächsten durchzuführenden Signatur wird automatisch wieder die Handy-Signatur App verwendet.

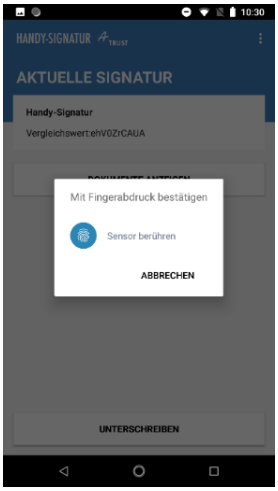
Mit Eingabe der Rufnummer und des Signaturpassworts wird wie gewohnt der Prozess gestartet. Nach erfolgter Eingabe wird der Signaturvorgang in der App fortgesetzt. Je nach Sicherheitseinstellung bzw. Betriebssystem erhält der Signator eine Pop-Up Message der Handy-Signatur App. Falls diese Nachricht nicht erscheint, muss die App manuell gestartet werden.
Nach der optionalen Angabe der Sicherheits-PIN bzw. der hinterlegten biometrischen Daten (Fingerabdruck/Gesichtserkennung), wird die APP geöffnet und dem Signator werden offene Signaturen zur Bestätigung angezeigt. Die Durchführung der Bestätigung hängt von der ausgewählten Form der Signaturauslösung (TAN in der App, QR-Code scannen, Eingabe biometrischer Daten) ab.

Um zu verifizieren, dass die gewünschte Signatur durchgeführt wird, kann der auf der Webseite angezeigte Vergleichswert mit dem in der App angezeigten Wert verglichen werden. Zusätzlich kann sowohl in der App als auch auf der Webseite das zu signierende Dokument angesehen werden.

Variante 1: Biometrische Daten

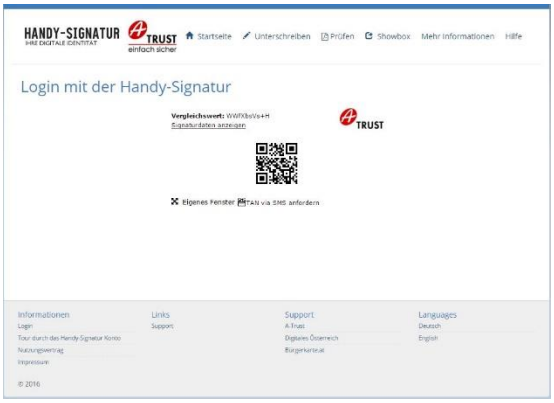
Wenn **biometrische Daten** hinterlegt und diese als Signaturauslösung-Methode ausgewählt sind, kann der Vorgang über den Button „Unterschreiben“ gestartet werden. Nach Bestätigung über den jeweiligen Parameter (Fingerabdruck oder Gesichtserkennung) wird der Signaturprozess beendet.



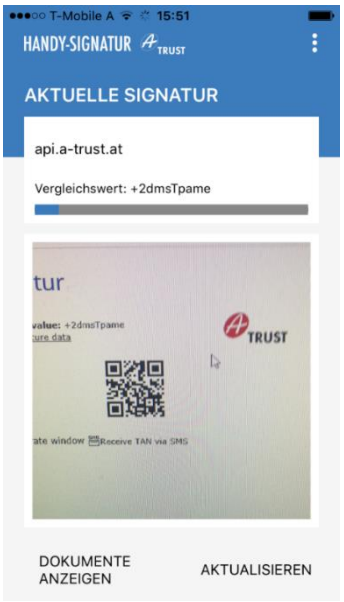


Variante 2: QR-Code scannen

Wenn keine biometrischen Daten für die Freigabe hinterlegt wurden erfolgt die Bestätigung durch das Einscannen eines **QR Codes**, der im Webbrowser angezeigt wird.

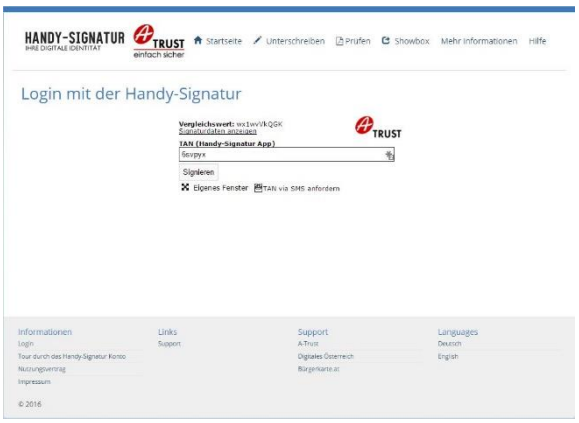


Um die Signatur abzuschließen muss der QR Code mit der Smartphone-Kamera bei geöffneter Handy-Signatur App gescannt werden. Bei erfolgreichem Scan erhalten Sie eine Bestätigung in der App. Wenn die Nutzung der Kamera für die App nicht freigegeben wurde, wird ein TAN in der App angezeigt (siehe Variante 3).



Variante 3: Erhalt der TAN in der App

Statt die TAN per SMS zu erhalten, können auch direkt in der **APP TANs** angezeigt werden. Diese sind dann entsprechend in das Eingabefeld im Browser einzugeben.



I. Glossar

Begriff / Abkürzung	Bedeutung	Beschreibung
RO	Registration Officer	Von A-Trust berechtigte Person, die Zertifikate im Namen von A-Trust ausgibt
zRO	zentraler Registration Officer	Wie RO – zudem Schnittstelle zwischen RO und A-Trust
RA / GS	Registration Authority (Registrierungsstelle) / Geschäftsstelle	Ort an dem Zertifikate ausgestellt werden / Zweigstellen
a.sign Client	-	Gratis – Software von A-Trust zum Zertifikatshandling (nur für Karten benötigt)
BKU	Bürgerkartenumgebung	Anforderung für e-Government mit Bürgerkarten, liest Zertifikate aus. Gratis, z.B. a.sign Bürgerkartenumgebung, Mocca oder TrustDesk Basic
Sperr- und Widerrufspasswort	-	Passwort, das bei der Aktivierung abgefragt wird. Weiters zum telefonischen Widerruf notwendig. 6-10 Stellen, Zeichen und Zahlen.
CA	Certificate Authority	Server, der die Zertifikate ausstellt
Qualifiziertes Zertifikat	-	Zur Signatur bestimmtes Zertifikat, das rechtlichen Grundlagen entspricht – für qualifizierte Signatur notwendig
Einfaches Zertifikat	-	Zertifikat, mit dem eine einfache bzw. fortgeschrittene Signatur durchgeführt werden kann
PIN	Personal Identification Number	Zahlenfolge, deren Eingabe eine Signatur auslöst (Kartenprodukte)
PUK	Personal Unblocking Key	Zahlenfolge, die einen gesperrten PIN (zu viele ungültige Eingaben) entsperren kann (Kartenprodukte) Bei e-card NICHT möglich!
Signaturpasswort	-	Vom Signator festgelegt, wird bei jedem Signaturvorgang benötigt. 6-20 Stellen, Zeichen und Zahlen, case sensitive Nur bei Handy-Signatur vorhanden.
RSA / ECC	-	Verschlüsselungsalgorithmen
SL	Security Layer	siehe BKU
ZMR	Zentrales Melderegister	Meldeverzeichnis aller Österreicher. Wird für die Personenbindung herangezogen.

CMS	Card Management System	System der A-Trust zur Zertifikatsverwaltung
VDA	Vertrauensdiensteanbieter	z.B. A-Trust
LDAP	Lightweight Directory Access Protocol	Protokoll des A-Trust Verzeichnisdienstes

II. Liste der möglichen Fehlermeldungen

Code	Kommentar	Text
1000	Es wurde kein SAMLArtifact vom MOA ID Server geliefert - neue Anmeldung versuchen - sonst beim Servicecenter melden	Fehler bei MOA ID Anmeldung. Bitte starten Sie den Prozess erneut. (Fehler 1000)
1001	Das vom MOA ID Server zurückgelieferte SAML ist Fehlerhaft - neue Anmeldung - an Servicecenter melden	Fehler bei MOA ID Anmeldung. Bitte starten Sie den Prozess erneut. (Fehler 1001)
1002	Zertifikat hat keinen A-Trust Issuer	Dieses Zertifikat ist nicht für die Aktivierung einer mobilen Signatur geeignet. (Fehler 1002)
1003	Datenbank ist nicht da	Datenbank Fehler. (Fehler 1003)
1004	no session	Ihre Session ist abgelaufen - bitte starten Sie den Prozess erneut. (Fehler 1004)
1005	wrong or unknown session	Ihre Session ist abgelaufen - bitte starten Sie den Prozess erneut. (Fehler 1005)
2000	Fehler beim Lesen der Vertragsdaten	Fehler beim Lesen der Vertragsdaten. (Fehler 2000)
2001	Mobiltelefonnummer nicht vollständig	Mobiltelefonnummer nicht vollständig (Fehler 2001)
2002	Passwörter stimmen nicht überein	Passwörter stimmen nicht überein. (Fehler 2002)
2003	Passwort muss mindestens 6 Zeichen lang sein	Passwort muss mindestens 6 Zeichen lang sein
2004	Passwort darf maximal 20 Zeichen lang sein	Passwort darf maximal 20 Zeichen lang sein
2005	Mobiltelefonnummer ist bereits vorhanden	Es konnte kein Zertifikat ausgestellt werden. Sollten Sie schon eine Signatur zu dieser Mobiltelefonnummer besitzen, so widerrufen Sie diese zuerst. (https://www.a-trust.at/widerruf) (Fehler 2005)
2006	Es konnte keine Session am BKU Server gestartet werden	Ein Hintergrundsystem ist nicht verfügbar (Fehler 2006)
2007	Fehler in Session Handling	Fehler in einem Hintergrundsystem (Fehler 2007)
2008	Fehler beim Anlegen der Personendaten	Fehler in einem Hintergrundsystem (Fehler 2008)
2009	Fehler beim Kopieren der Personendaten von Ihrem alten Vertrag	Fehler in einem Hintergrundsystem (Fehler 2009)
2010	Fehler beim OTP versenden	Fehler beim Versenden der Verifikations-SMS (Fehler 2010)
2011	OTP Feld leer	Bitte erst den Wert aus Ihrer SMS eingeben.

2012	Fehler Gen Key	Fehler in einem Hintergrundsystem (Fehler 2012)
2013	Fehler bei Add Contract	Fehler in einem Hintergrundsystem (Fehler 2013)
2014	Fehler bei ZMR Abfrage	Fehler bei Stammzahlenregister-Abfrage (Fehler 2014)
2015	Fehler beim Lesen der Vertragsdaten	Fehler in einem Hintergrundsystem (Fehler 2015)
2016	Fehler beim Speichern des Signaturvertrages	Fehler in einem Hintergrundsystem (Fehler 2016)
2017	Fehler beim Ausstellen des Vertrags	Fehler in einem Hintergrundsystem (Fehler 2017)
2018	Fehler beim Archivieren	Fehler in einem Hintergrundsystem (Fehler 2018)
2019	Fehler beim Contract befüllen	Fehler in einem Hintergrundsystem (Fehler 2019)
2020	Keine Handy Vorwahl ausgewählt	Bitte wählen Sie eine Handyvorwahl aus.
2021	XML Verification Error	Fehler in einem Hintergrundsystem (Fehler 2021)
2022	Fehler beim Finalisieren	Fehler in einem Hintergrundsystem (Fehler 2022)
2023	Eine Ausstellung einer Qualifizierten Handy-Signatur auf Basis Ihrer Karte ist nicht erlaubt.	Eine Ausstellung einer Qualifizierten Handy-Signatur auf Basis Ihrer Karte ist nicht erlaubt. (Fehler 2023)
2024	Der eingegebene TAN ist falsch	Der eingegebene Aktivierungscode ist falsch
2025	Der eingegebene TAN ist falsch, Sie haben keine Versuche mehr	Der eingegebene Aktivierungscode ist falsch, Sie haben keine Versuche mehr
3001	Überprüfen der Eingabedaten	Überprüfen der Eingabedaten
3002	Datensatz anlegen und befüllen	Datensatz anlegen und befüllen
3003	Bestehende Vertragsdaten überprüfen	Bestehende Vertragsdaten überprüfen
3004	Aktivierungscode per SMS an Mobiltelefon verschicken	Aktivierungscode per SMS an Mobiltelefon verschicken
3005	Vorgang Erfolgreich	Vorgang Erfolgreich
3006	Schlüssel generieren	Schlüssel generieren
3007	Vertrag anlegen	Vertrag anlegen
3008	Abfrage bei Zentralem Melderegister	Abfrage bei Zentralem Melderegister
3009	Überprüfen der Eingabedaten bei OTP	Überprüfen der Eingabedaten
3010	Signaturvertrag überprüfen	Signaturvertrag überprüfen
3011	Zertifikate ausstellen	Zertifikate ausstellen
3012	Vertrag und Anmeldedaten archivieren	Vertrag und Anmeldedaten archivieren
3013	Handy-Signatur zur Verwendung vorbereiten	Handy-Signatur zur Verwendung vorbereiten
3014	Finalisieren der qualifizierten Handy-Signatur	Finalisieren der qualifizierten Handy-Signatur

III. Schnellablauf / Checkliste
Registrierung in der Registrierungsstelle

1. Vorbereitung
    a. AGBs und Unterrichtung auflegen
    b. Aktivierte Handy-Signatur (mit RO Rechten) bereit
       ODER
    c. Bürgerkartensoftware (lokal installiert und gestartet)
        i. Kartenleser installiert und einsatzbereit (Test: PIN ändern in verwendeter BKU möglich)
        ii. RO Karte im Kartenleser

2. Aufrufen der Officer-Seite unter https://www.a-trust.at/aktivierung/ro

3. Ausfüllen der Eingabemaske

4. Kontrollieren und Signieren der erfassten Ausweis-Daten und Unterrichtung des Signators

5. Signaturpasswort festlegen

6. Bestätigen des Signaturvertrags

7. eventuell Aushändigen der Unterrichtung (Papier)

8. optional: Aktivierung der App mit Signator durchführen