A-Trust GmbH
1030 Wien, Landstraßer Hauptstraße 1b, E02

Registrierungshandbuch für Registration Officer

-

Ausstellung von qualifizierten Zertifikaten *xIDENTITY*

Kontakt E-Mail: office@a-trust.at, Telefon: +43 1 713 21 51 0
Konto Oberbank, BIC: OBKLAT2L, IBAN: AT17 1515 0005 0116 4396
Firmenbuch UID: ATU50272100, DVR: 1065181, FN: 195738a, HG Wien

1 Inhalt

2 Grundinformationen

2.1 Zertifikat

Im Laufe des Registrierungsprozesses wird **ein qualifiziertes Zertifikat** erstellt. Die Speicherung des Zertifikates erfolgt im Hochsicherheitsbereich des A-Trust Rechenzentrums, die Verwendung darf ausschließlich der im Zertifikat angeführten Person möglich sein. Die Signaturauslösung erfolgt über eine Zweifaktorauthentifizierung, hierzu muss im Aktivierungsprozess ein Signaturpasswort festgelegt, sowie ein zweiter Faktor zur Besätigung verknüpft werden.

Das qualifizierte Zertifikat ist wesentliche Grundvoraussetzung für die Erstellung einer qualifizierten Signatur, die das rechtliche Erfordernis der Schriftlichkeit im Sinne des § 886 ABGB erfüllt. Im Zertifikat wird der Name der signierenden Person inkl. Titel aufgenommen. Bei minderjährigen Personen zwischen 14 und 18 Jahren ist auch das Geburtsdatum Teil des Zertifikats.

2.2 Durchführung einer Signatur

Im Laufe der Aktivierung wird ein Signaturpasswort festgelegt, das aus sechs bis zwanzig (alpha)numerischen Zeichen (= Ziffern, Buchstaben und Sonderzeichen) bestehen muss. Mit diesem Signaturpasswort wird der private Schlüssel der signierenden Person geschützt. Das Signaturpasswort wird somit für die Erstellung von Signaturen benötigt und gewährleistet dadurch den alleinigen Zugriff durch die im Zertifikat namentlich angeführte Person.

Um eine Signatur mit dem xIDENTITY Zertifikat durchzuführen, muss die dafür vorgesehene Maske in der gewünschten Applikation mit der Handynummer und dem Signaturpasswort befüllt werden. Nur die erfolgreiche Eingabe dieser beiden Werte führt zum nächsten Schritt, der Bestätigung über den zweiten Faktor.

Schritte zur Durchführung einer Signatur:

1. Eingabe des Benutzernamens und des zugehörigen Signaturpassworts
2. Überprüfung durch Anzeige der zu signierenden Daten und/oder Kontrolle der Vergleichswerte
3. Signaturauslösung mittels Bestätigung in der verknüpften App oder über den verbundenen FIDO Token

2.3 Gültigkeit der Zertifikate

xIDENTITY Zertifikate sind fünf Jahre lang gültig. Bis zum Ablauf des Zertifikats kann dieses genutzt werden, um die Ausstellung eines Folgezertifikats anzustoßen (Verlängerung).

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* und *Wissen* 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 (+43 1 715 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

Aktuell 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 alt (wird vom System automatisch abgelehnt)?

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 eines xIDENTITY Zertifikats

Um ein xIDENTITY Zertifikat erfolgreich zu aktivieren, müssen folgende Rahmenbedingungen gegeben sein:

- Besitz eines Mobiltelefons mit Android oder iOS Betriebssystem und installierter A-Trust Signatur App
  ODER
- ein unterstützter FIDO-Token (https://www.a-trust.at/de/fido/)
- der Signator muss das 14. Lebensjahr vollendet haben
- Vorlage eines amtlichen **und gültigen** Lichtbildausweises, der in der Liste in Punkt 2.6 enthalten ist

3.2 Anforderungen an den Arbeitsplatz

Technische Anforderungen

- RO: aktives qualifiziertes Zertifikat (xIDENTITY, ID Austria oder Bürgerkarte) mit bei A-Trust hinterlegten xIDENTITY RO-Rechten. Eine Anforderung der RO-Rechte kann per E-Mail durch den zRO erfolgen.
- Optional: Drucker für den Signaturvertrag

- *Optional (wenn eine Smartcard-Bürgerkarte für die Signatur des RO verwendet wird):*
- Smart Card Reader mit PIN-Pad
- a.sign Bürgerkartensoftware in Kombination mit dem a.sign Client

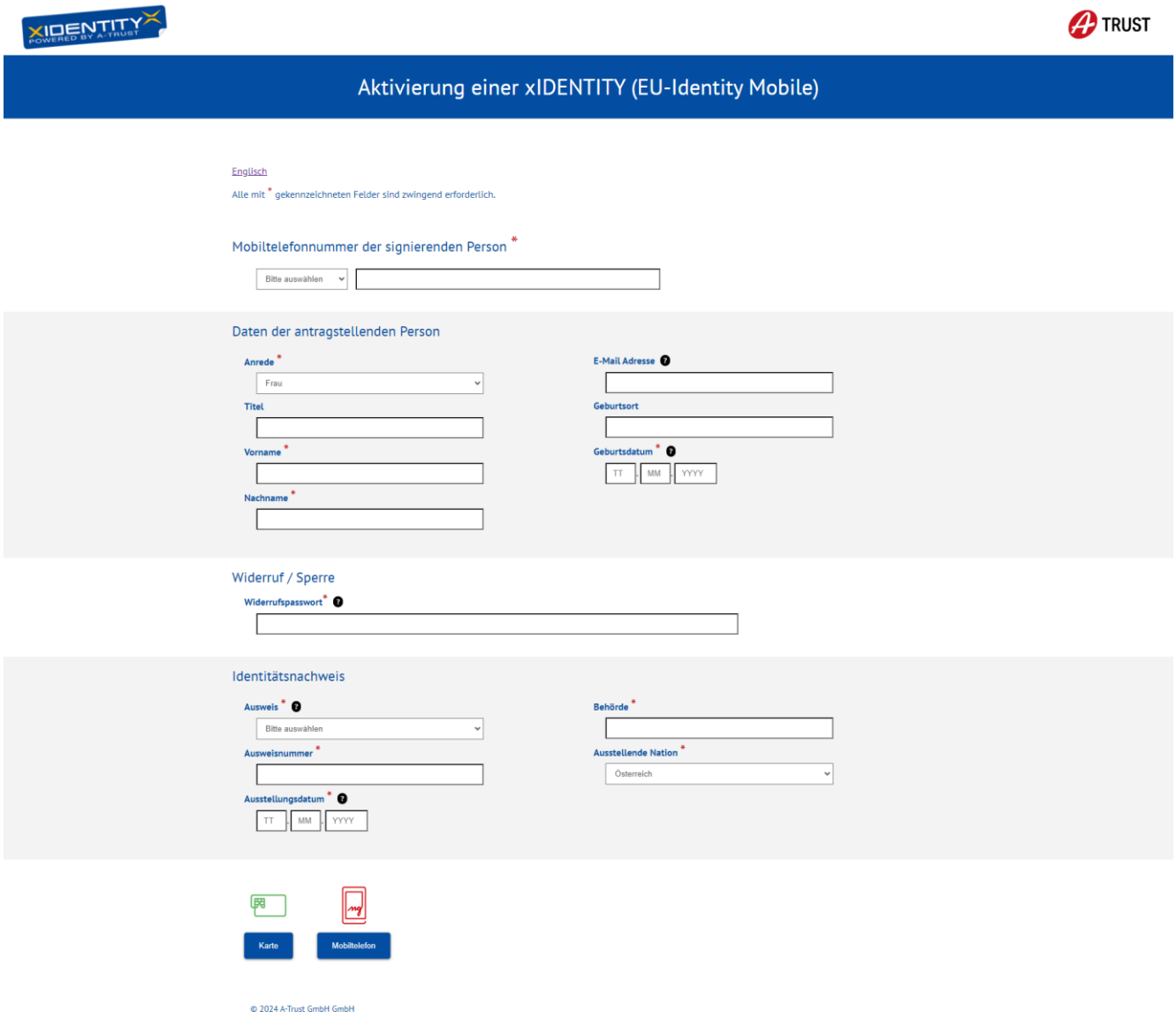
4 Aktivierungsprozess

Das Handbuch bezieht sich auf die Aktivierung von xIDENTITY im Rahmen des RO-Prozesses in einer Registrierungsstelle. Zusätzlich stehen noch andere Identifizierung- und Aktivierungsarten zur Verfügung, die nicht in diesem Handbuch behandelt werden.

Die Aktivierung in der Registrierungsstelle startet unter der URL https://www.a-trust.at/aktivierung/euidentity/ und kann in die zwei Teilbereiche Authentifizierung und Zertifikatsausstellung aufgeteilt werden. Das Formular ist in den Sprachen Deutsch und Englisch verfügbar, eine Umstellung ist am Beginn der Seite möglich.

4.1 Authentifizierung

Im ersten Schritt 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.



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 bestätigt 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 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.

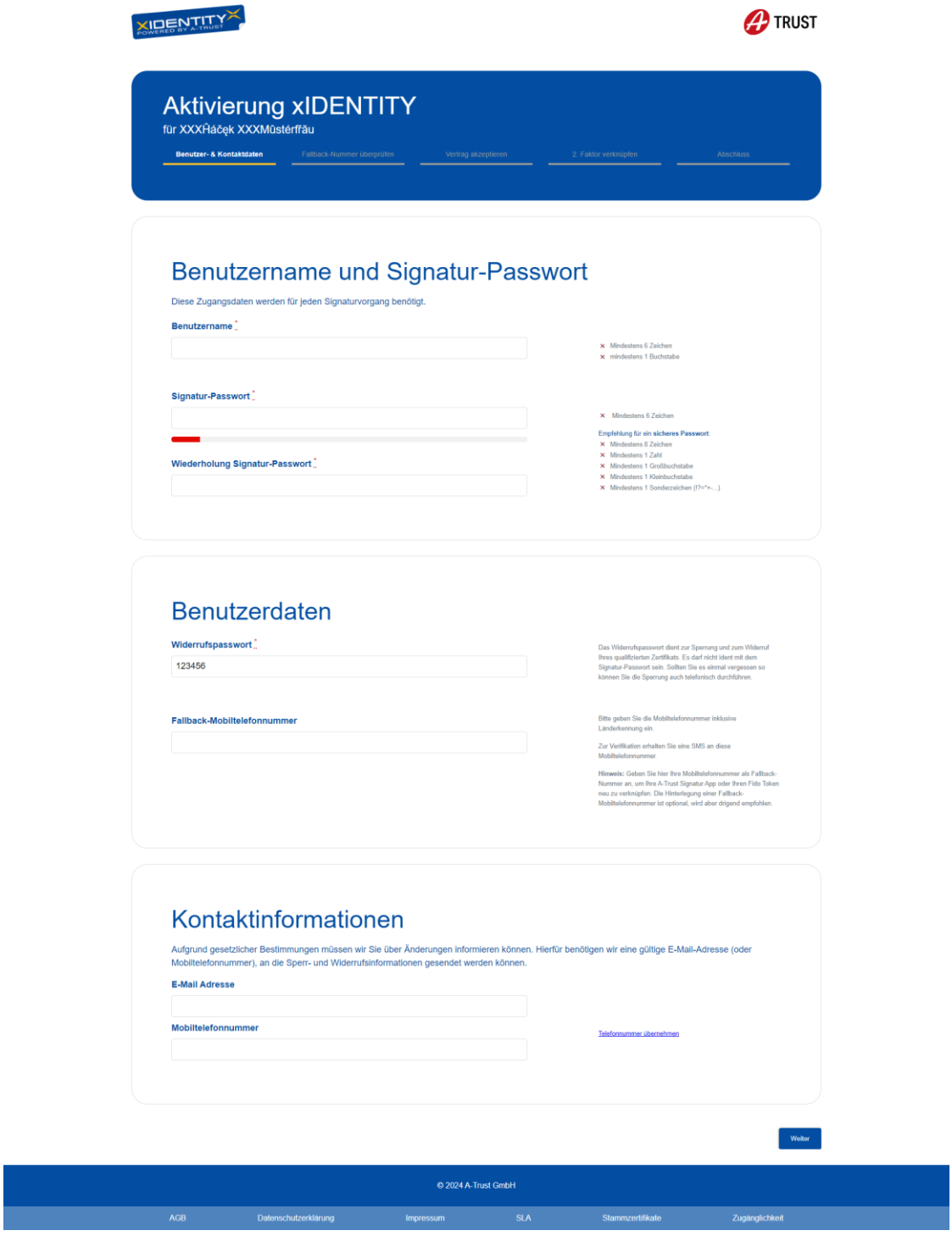
ANMERKUNG: Die E-Mail-Adresse sollte unbedingt erfragt werden. Nur wenn diese im Datensatz vorhanden ist, kann der Signator vor Ablauf seines Zertifikates durch A-Trust erinnert werden, dass eine Verlängerung erforderlich ist.

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 oder mit xIDENTTIY bzw. einer ID Austria durchführen möchte. Der RO muss vorher bereits von A-Trust für die Aktivierung von xIDENTITY Zertiifkaten berechtigt worden sein!

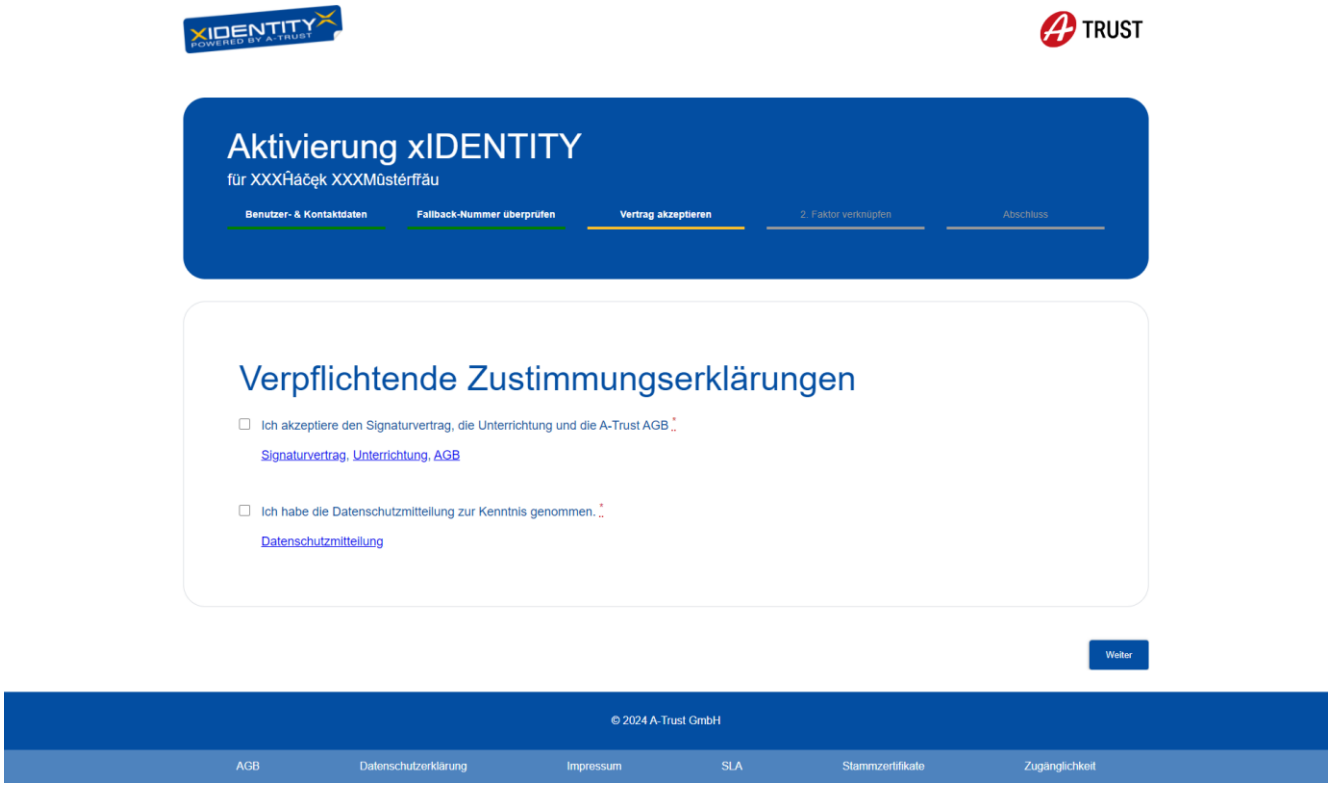
4.2 Zertifikatsausstellung

Nach dem Prozess erscheint nach der Signatur der Signator-Identifikationsdaten durch den RO automatisch die nächste Eingabemaske, in der der Benutzername und das Signaturpasswort festgelegt werden müssen.

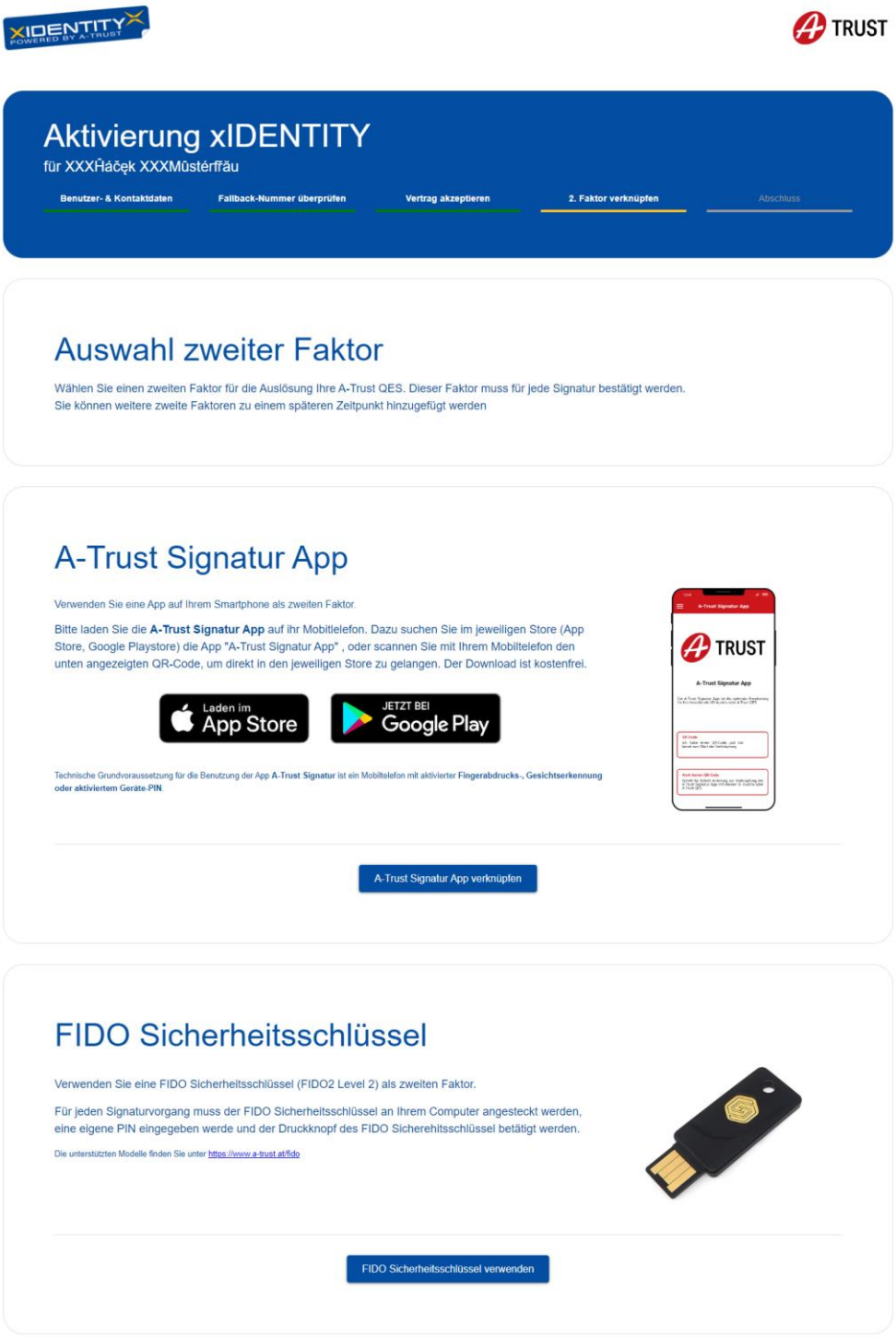
Der Signator wählt hier sein gewünschtes Signaturpasswort, das für jeden Signaturvorgang benötigt wird. Der Prozess wird durch einen Klick auf „weiter“ fortgesetzt.



Im nächsten Schritt können Signaturvertrag und Datenschutzmitteilung angezeigt werden. Diesse müssen mittels Checkbox akzeptiert werden, um den Prozess fortzusetzen.



Nun folgt die Bindung des zweiten Faktors zum Signaturvertrag. Hierfür kann zwischen der A-Trust Signaturapp und einem FIDO Token gewählt werden, Anleitungen zur Bindung selbst sind beim jeweiligen Prozess verfügbar.



Die Aktivierung ist nun erfolgreich abgeschlossen.

5 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 erforderlich
Signaturpasswort	-	Vom Signator festgelegt, wird bei jedem Signaturvorgang benötigt.
RSA / ECC	-	Verschlüsselungsalgorithmen
VDA	Vertrauensdiensteanbieter	z.B. A-Trust