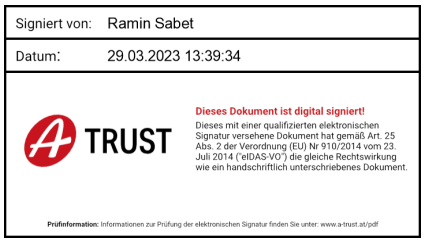
A-Trust GmbH
Landstraßer Hauptstraße 1b E02,
A-1030 Wien
Tel: +43 (1) 713 21 51 - 0
Fax: +43 (1) 713 21 51 - 350
https://www.a-trust.at

A-Trust Anwendungsvorgabe (Certificate Policy) für qualifizierte Zertifikate a.sign premium



Version: 1.4.4
Datum: 27.02.2023

Inhaltsverzeichnis

Rev	Verfasst von	Änderungen
1.3.5	RS	3.3.1 Registrierung des Signators (a-sign business F) 3.2.2 Speicherung der CA-Schlüssel 2.1 Widerrufsbrief bei Neuaktivierung
1.3.6	RS	3.3.2 Fortgeschrittene Signatur für Rezertifizierung 3.2.2 Speicherung der CA-Schlüssel
1.3.7	RS	3.3.1 Widerrufsbrief bei Neuaktivierung präzisiert
1.3.8	RS	Tippfehler
1.4.0	RS, PT	eIDAS Anpassungen
1.4.1	RS	Adresse, Logo
1.4.2	RS	Feedback Auditor
1.4.3	RS, IH	Generation 08, Namensänderung Genderneutrale Sprache, Löschung a.sign business F, eCard
1.4.4	IH	Referenzdokumente, ACOS-ID v2.0

Tabelle 1: Dokumentenhistorie

1 Einführung

1.1 Überblick

Die Anwendungsvorgaben (Certificate Policy) enthalten ein Regelwerk, das den Einsatzbereich eines Zertifikats für eine bestimmte Personengruppe und/oder Anwendungsklasse mit gemeinsamen Sicherheitsanforderungen definiert.

Die Certificate Policy für qualifizierte a.sign premium Zertifikate gilt entsprechend der Verordnung (EU) 910/2014 [eIDAS-VO] und dem österreichischen Signatur- und Vertrauensdienstegesetz [SVG], die an Nutzende ausgestellt werden, auf sicheren Signaturerstellungseinheiten basieren und für die Erstellung qualifizierter Signaturen geeignet sind.

1.2 Dokumentidentifikation

Name der Richtlinie:	A-Trust Anwendungsvorgaben (Certificate Policy) für qualifizierte Zertifikate a.sign premium für qualifizierte Signaturen
Version:	1.4.4 / 27.02.2023
Object Identifier:	1.2.040.0.17 (A-Trust) .1 (CP) .11 (a.sign premium) .1.4.4 (Version) vorliegende Version

Der A-Trust OID 1.2.040.0.17 ist bei ÖNORM registriert.

Die vorliegende Policy ist in Übereinstimmung mit Klasse "qcp-natural-qscd" [Object Identifier: 0.4.0.194112.1.2] (siehe [ETSI 319 411]) und mit RFC3647 [RFC3647].

1.3 Anwendungsbereich

Diese Anwendungsvorgaben gelten für qualifizierte Zertifikate gem. Artikel 28 [eIDAS-VO], welche ausschließlich für natürliche Personen ausgestellt werden.

Der Schlüssel der signierenden Person darf ausschließlich für das Erstellen von Signaturen genutzt werden.

Elektronische Signaturen, die in Übereinstimmung mit diesen Anwendungsvorgaben und unter Verwendung der von A-Trust empfohlenen Komponenten und Verfahren erstellt wurden, sind qualifizierte Signaturen im Sinne von Artikel 3 [eIDAS-VO].

Ausgestellt werden a.sign premium Zertifikate auf folgende geeignete Chipkarten:

- a.sign premium Standardkarten, wobei es eine bei A-Trust bestellte reine Signaturkarte oder eine signaturfähige Karte mit zusätzlichen Funktionen (z. B. Maestrokarte, Mastercard, Mitgliedsausweis etc.) sein kann.

Qualifizierte Signaturen, die auf Basis eines qualifizierten a.sign premium Zertifikats für qualifizierte Signaturen erstellt wurden, sind in ihrer Rechtswirkung gemäß Artikel 25 Abs 2 [eIDAS-VO] einer eigenhändigen Unterschrift grundsätzlich gleichgestellt. Ausnahmen können sich aus vertraglichen Vereinbarungen oder gesetzlichen Bestimmungen ergeben (siehe [SVG]).

Zu den empfohlenen Komponenten und Verfahren gehören:

- ein von A-Trust empfohlenes Hash-Verfahren,
- die sichere Eingabe der Signatur PIN, bei welcher die signierende Person ausschließen kann, dass die PIN anderen Personen zukommt oder über den Signaturvorgang hinaus gespeichert wird,
- die sichere Anzeige der zu signierenden Daten, die alle zu signierenden Daten inhaltlich unverändert darstellen kann.

Nur mit einem qualifizierten Zertifikat, welches auf der von einer Bestätigungsstelle (z.B. A-SIT) bescheinigten sicheren Signaturerstellungseinheit wie in Kapitel 3.2.8 beschrieben basiert, kann eine qualifizierte Signatur erstellt werden.

Die signierende Person ist sich bewusst, dass A-Trust eine Liste mit empfohlenen technischen Komponenten und Verfahren für die Erstellung von qualifizierten Signaturen bereitstellt und dass bei der Verwendung anderer Komponenten und Verfahren A-Trust für Schäden, die durch diese verursacht werden, nicht haftbar gemacht werden kann.

1.4 Übereinstimmung mit der Policy

A-Trust verwendet den Object Identifier aus Kapitel 1.2 nur für die Erstellung von Zertifikaten, anlässlich derer Anwendung die Regelungen der gegenständlichen Policy Beachtung fanden.

2 Verpflichtungen und Haftung

2.1 Verpflichtungen der Zertifizierungsstelle

A-Trust verpflichtet sich, dass alle Anforderungen dieser Anwendungsvorgabe und der Zertifizierungsrichtlinie erfüllt sind, die sich insbesondere auf die folgenden Aspekte erstrecken:

- Die Zertifikate der signierenden Personen werden im Einklang mit dieser Anwendungsvorgabe und der Zertifizierungsrichtlinie erstellt und können ausgesetzt, widerrufen oder verlängert werden.
- Die Zertifizierungsstelle arbeitet im Einklang mit dem der Aufsichtsbehörde vorgelegten Sicherheits- und Zertifizierungskonzept.
- Die Zertifizierungsstelle beschäftigt ausschließlich qualifiziertes Personal.
- Die Zertifizierungsstelle kommt ihrer Informationspflicht gegenüber den signierenden Personen und Aufsichtsbehörden nach.
- Die Zertifizierungsstelle sorgt durch geeignete Maßnahmen (technisch, organisatorisch, infrastrukturell und personell) für den Schutz des privaten Schlüssels der Zertifizierungsstelle.
- Der Einsatz des privaten Schlüssels der Zertifizierungsstelle erfolgt ausschließlich zum Signieren der Zertifikate der signierenden Personen und zum Signieren der Widerrufsinformationen.
- Die Zertifizierungsstelle veröffentlicht alle ausgestellten Zertifikate (sofern dies gewünscht wird). Bei Widerruf und Aussetzung eines Zertifikats wird die betroffene signierende Person benachrichtigt. Ein nicht veröffentlichtes Zertifikat wird bei einer Aussetzung oder einem Widerruf in die Widerrufsliste aufgenommen. Wenn der Widerruf aufgrund einer Neuaktivierung stattfindet, im Zuge derer die signierende Person über den Widerruf des bestehenden Zertifikates informiert wird, kann diese Verständigung ausbleiben.
- A-Trust hat insbesondere die Verpflichtung eine Liste der für eine qualifizierte Signaturerstellung und -prüfung zu verwendenden Komponenten und Verfahren zu erstellen und aktuell zu halten und diese den signierenden Personen und Signaturempfangende jederzeit zugänglich zu machen.

2.2 Verpflichtungen der signierenden Person

Die signierenden Personen haben sich an die Richtlinien dieses Dokuments zu halten. Dies betrifft insbesondere folgende Aspekte:

- Die signierenden Personen verpflichten sich die relevanten Allgemeinen Geschäftsbedingungen [AGB] zusammen mit der a.sign premium Anwendungsvorgabe (Policy), der Zertifizierungsrichtlinie und den Entgeltbestimmungen von A-Trust als Grundlage für den abgeschlossenen Vertrag anzuerkennen.
- Die signierende Person ist für die Richtigkeit der Angaben verantwortlich, die bei der Registrierung gemacht wurden und wirkt gemäß den in der Zertifizierungsrichtlinie angegebenen Verfahren zur Identitätsfeststellung und Authentifikation mit.
- Die signierende Person ist verpflichtet, ihren privaten Schlüssel angemessen zu schützen. Dies umfasst insbesondere keinen Zugriff durch unautorisierte Personen auf die a.sign premium Karte zuzulassen und die Aktivierungsdaten (PIN) des privaten Schlüssels geheim zu halten.
- Falls nötig initiiert die signierende Person unverzüglich die Aussetzung oder den Widerruf ihres Zertifikats. Wird die Aussetzung nicht in einem vorgegebenen Zeitraum aufgehoben, so erfolgt automatisch ein Widerruf des Zertifikats.
- Die signierende Person setzt das Zertifikat nur zu dem im Zertifikat angegebenen Zweck ein. Maßgeblich hierfür sind die zum Zeitpunkt der Ausstellung des Zertifikats gültige Zertifizierungsrichtlinie und die zugehörigen Anwendungsvorgaben (Policy).
- Die signierende Person ist sich bewusst, dass A-Trust eine Liste mit empfohlenen technischen Komponenten und Verfahren für die Erstellung von qualifizierten a.sign premium bereitstellt und dass bei der Verwendung anderer Komponenten und Verfahren A-Trust für Schäden, die durch diese verursacht werden, nicht haftbar gemacht werden kann.
- Es muss weiters dafür Sorge getragen werden, dass auf dem Gerät, mit welchem die qualifizierte Signatur erstellt wird, kein unbefugt eingebrachter Programmcode zur Anwendung kommt. Dazu sollen die folgenden Vorgaben von A-Trust einhalten werden:
  - Die signierende Person muss alle notwendigen technischen und organisatorischen Maßnahmen ergreifen, um unbefugten Zugriff auf ihr Gerät und die darauf befindlichen Programmcodes zu verhindern.
  - A-Trust verpflichtet die signierende Person, sich an die Empfehlungen der herstellenden Unternehmen des verwendeten Betriebssystems sowie der anderen Software-Produkte, die installiert wurden, zu halten.
- Die signierende Person ist verpflichtet die jeweiligen nationalen bzw. europäischen Ausfuhrbestimmungen sowie etwaige nationale Nutzungsbeschränkungen bei einer Verwendung im Ausland zu beachten.

2.3 Verpflichtungen der Signaturempfangenden

Den Signaturempfangenden von a.sign premium Zertifikaten wird empfohlen, vor der Akzeptanz folgende Prüfungen durchzuführen:

- Die digitale Signatur
- Die Gültigkeit des Zertifikats
- Den zweckgemäßigen Einsatz des Zertifikats (d.h. für die Erstellung einer Signatur)

Wenn Signaturempfangende eine qualifizierte Signaturprüfung durchzuführen beabsichtigen, dann wird die Verwendung der für eine qualifizierte Überprüfung einer Signatur vorgesehenen Komponenten und Verfahren empfohlen.

2.4 Haftung

A-Trust haftet als Vertrauensdiensteanbieter gemäß Artikel 13 [eIDAS-VO].

3 Anforderung an die Erbringung von Zertifizierungsdiensten

Diese Policy ist auf die Erbringung von qualifizierten Vertrauensdiensten ausgerichtet. Dies umfasst die Bereitstellung von Registrierungsdiensten, Zertifikatsgenerierung, Zertifikatsausgabe, Aussetzungs- und Widerrufsdiensten und Abfragediensten über den Zertifikatsstatus.

3.1 Zertifizierungsrichtlinie (CPS)

A-Trust hat die nachfolgend aufgelisteten Maßnahmen ergriffen, um die für die Erbringung von Zertifizierungsdiensten nötige Sicherheit und Verlässlichkeit zu gewährleisten:

1. A-Trust hat eine Risikoanalyse erstellt, um die möglichen Risiken abzuschätzen und die sich daraus ergebenden Sicherheitsanforderungen und Umsetzungsmaßnahmen zu bestimmen.
2. A-Trust hat alle nötigen Vorgangsweisen und Prozeduren, um die Anforderungen aus der Anwendungsvorgabe zu erfüllen, in ihrem Sicherheitskonzept dargestellt.
3. Die Zertifizierungsrichtlinie (siehe [CPS]) benennt die Verpflichtungen aller externen Vertragsparteien, die Dienstleistungen für A-Trust unter Beachtung der jeweils anwendbaren Policies und Richtlinien erbringen.
4. A-Trust macht allen signierenden Personen und Signaturempfangenden die Zertifizierungsrichtlinie und jegliche Dokumentation, die die Übereinstimmung mit dieser Anwendungsvorgabe dokumentiert, zugänglich (siehe Kapitel 3.3.4).
5. Die Geschäftsführung der A-Trust stellt das alleinige Entscheidungsgremium dar, das für die Genehmigung der Zertifizierungsrichtlinie für a.sign premium verantwortlich ist.
6. Die Geschäftsführung der A-Trust trägt auch die Verantwortung für die ordnungsgemäße Implementierung der Zertifizierungsrichtlinie für a.sign premium.
7. A-Trust hat einen Revisionsprozess zur Überprüfung der Vorgangsweisen der Zertifizierung aufgesetzt, der auch Maßnahmen zur Wartung der Zertifizierungsrichtlinie für a.sign premium umfasst.
8. A-Trust wird zeitgerecht über beabsichtigte Änderungen informieren, die in der Zertifizierungsrichtlinie vorgenommen werden sollen, und wird nach Genehmigung derselben entsprechend Punkt 5 dieses Absatzes eine überarbeitete Version der Zertifizierungsrichtlinie für a.sign premium entsprechend Kapitel 3.3.4 unverzüglich zugänglich machen.

3.2 Verwaltung der Schlüssel zur Erbringung von Zertifizierungsdiensten

3.2.1 Erzeugung der CA-Schlüssel

Die Generierung der von A-Trust zur Erbringung von Zertifizierungsdiensten verwendeten Schlüssel erfolgt in Übereinstimmung mit den Bestimmungen der Artikel 19, 24 [eIDAS-VO]:

1. Die Erzeugung der Schlüssel wird von dazu autorisiertem Personal (siehe Rollenmodell in Kapitel 3.4.3), mindestens im Vier-Augen-Prinzip in einer physisch abgesicherten Umgebung durchgeführt (siehe 3.4.4).
2. Die Schlüssel werden in einer Signaturerstellungseinheit (Hardware Security Modul) erstellt, die einem Bestätigungsverfahren bei A-SIT unterzogen wurde und zur Erstellung fortgeschrittener Signaturen geeignet ist.
3. Für die Schlüsselgenerierung wird ein Algorithmus verwendet, der für qualifizierte Zertifikate als geeignet angesehen wird.
4. Die Schlüssellänge und der Algorithmus sind für qualifizierte Zertifikate geeignet und entsprechen dem Durchführungsbeschluss zur [eIDAS-VO] (EU) 2015/1506 und den Empfehlungen der Expertsgroup der European Electronic Signature Standardisation Initiative.

3.2.2 Speicherung der CA-Schlüssel

A-Trust stellt sicher, dass die privaten Schlüssel geheim gehalten werden und ihre Integrität bewahrt bleibt.

Die Schlüssel sind in einem Hardware Security Modul gespeichert, welches die Anforderungen aus Art 2 (7) [SVV] erfüllt.

3.2.3 Verteilung der öffentlichen CA-Schlüssel

A-Trust stellt durch die folgenden Maßnahmen sicher, dass die Integrität und Authentizität der öffentlichen Schlüssel anlässlich der Verteilung gewahrt bleibt:

- Ausstellung und Veröffentlichung eines selbst signierten Root-Zertifikates.

Das Zertifikat des CA-Schlüssels zur Signatur von a.sign premium Zertifikaten wird den vertrauenden Beteiligten durch Veröffentlichung im Rahmen des Verzeichnisdienstes zugänglich gemacht. A-Trust gewährleistet die Authentizität dieses Zertifikats.

3.2.4 Schlüsseloffenlegung

Eine Offenlegung der geheimen CA-Schlüssel ist nicht vorgesehen.

3.2.5 Verwendungszweck von CA-Schlüsseln

Der private Schlüssel der Zertifizierungsstelle wird nur für die Erstellung von a.sign premium Zertifikaten und für die Signatur der zugehörigen Widerrufslisten oder Antworten von OCSP Anfragen innerhalb von physisch abgesicherten Räumlichkeiten verwendet.

3.2.6 Ende der Gültigkeitsperiode von CA-Schlüsseln

Die CA-Schlüssel werden verwendet, solange die verwendeten Algorithmen den Sicherheitserwartungen entsprechen. Eine Archivierung der privaten Schlüssel ist nicht vorgesehen.

3.2.7 Erzeugung der Schlüssel für die signierende Person

Bestimmungen entsprechen denen der CA-Schlüssel (siehe 3.2.1).

Die Schlüssel werden im Hochsicherheitsbereich des kartenherstellenden Unternehmens in den a.sign premium Karten erzeugt. Ein Zertifikat für das Signaturschlüsselpaar wird noch nicht erstellt. Dies geschieht erst im Zuge des Registrierungsprozesses, indem die signierende Person zuverlässig identifiziert und authentisiert wird.

3.2.8 Sicherheit der a.sign premium Karte

Die Schlüssel der signierenden Person werden auf einer den Anforderungen entsprechenden Chipkarte, der a.sign premium Karte, gespeichert. Es handelt sich bei der a.sign premium Karte um eine von einer Bestätigungsstelle (wie z.B. A-SIT) nach Artikel 30 [eIDAS-VO] bescheinigte Smartcard, welche eine sichere Signaturerstellungseinheit darstellt und die Erzeugung und Speicherung der Signaturerstellungsdaten ermöglicht (z.B. [**?**], [**?**]). Auf den von A-Trust als a.sign premium Karten eingesetzten Smartcards mit zertifiziertem Chip ist sicher gestellt, dass es durch andere auf der Karte befindliche Applikationen zu keiner Beeinflussung der Signaturfunktion kommen kann.

3.3 Lebenszyklus des Zertifikats

3.3.1 Registrierung der signierenden Person

Die Maßnahmen zur Identifikation und Registrierung der signierenden Person entsprechen den Anforderungen des Artikels 24 [eIDAS-VO] und stellen sicher, dass der Antrag auf Ausstellung eines qualifizierten Zertifikats korrekt, vollständig und autorisiert ist.

Die Angaben der signierenden Person werden in zwei Kategorien eingeteilt. Dies sind zum einen die erforderlichen und zum anderen die optionalen Angaben. Es sind folgende Daten aufzunehmen:

- Name für das a.sign premium Zertifikat: Nachname und Vorname sind erforderlich. Im Falle von Standard a.sign premium Karten kann die signierende Person statt des Namens auch ein Pseudonym wählen. Der korrekte und vollständige Name muss der Registrierungsstelle und Zertifizierungsstelle auch bei Verwendung eines Pseudonyms bekannt sein.
- Die Angabe der postalischen Adresse ist erforderlich.
- Die Angabe der Meldeadresse ist optional.
- Optional können im Namen des Zertifikatswerbers die Attribute `OrganizationName` mit dem Inhalt "Berufsbezeichnung" und `OrganizationalUnit` mit einem eindeutigen Code als Inhalt vergeben werden. Diese Attribute werden nur vergeben, wenn die ausstellende Registrierungsstelle die Korrektheit dieser Angaben sicher stellt.
- Im Falle des Produktes "a.sign Business F" werden folgende zusätzlichen Prüfungen durchgeführt:
  - Nach Prüfung des Firmenbuches, ob die signierende Person für eine bestimmte Firma zeichnungsberechtigt ist, oder ob ein firmenmäßig gezeichneter Antrag auf Zertifikatsausstellung unter Eintragung einer im Antrag spezifizierten Vollmacht für die signierende Person vorliegt, wird der Name dieser juristischen Person in das Zertifikatsfeld `OrganizationName` aufgenommen.
  - Allfällige Hinweise zur Vertretungsvollmacht wie
    * Geschäftsführung
    * Prokura (Einzel- bzw. Gesamtprokura)
    * Handlungsvollmacht

    werden in das Feld `organizationalUnitName` eingetragen.
  - Einschränkungen: als Freitext (zB. "nur zur Signatur elektronischer Rechnungen"). Diese werden bei der Bestellung angegeben und von A-Trust ungeprüft in das Zertifikat aufgenommen (ebenfalls `organizationalUnitName`).

Die Angaben der antragstellenden Person werden bei der Aktivierung der Karte in der Registrierungsstelle durch die Registrierungsstelle überprüft.

Die antragstellende Person beweist ihre Identität durch das Vorlegen eines gültigen, amtlichen Lichtbildausweises. Dabei sind die folgenden Ausweise zulässig:

- ein gültiger amtlicher Lichtbildausweis (eine Liste der in Österreich und Deutschland gültigen amtlichen Lichtbildausweise, die von A-Trust akzeptiert werden, ist auf der Homepage der A-Trust zu finden) oder
- ein international gültiger Reisepass in deutscher und/oder englischer Sprache.

Weiters steht die Möglichkeit zur Verfügung, dass mittels eines RSa Briefs gemäß § 2 Z 2 [SVV] ein für die Ausstellung der Zertifikate notwendiger Aktivierungscode an die Meldeadresse der signierenden Person versendet wird. Im Rahmen der Zustellung des RSa Briefs ist es notwendig, dass die antragstellende Person ihre Identität durch das Vorlegen eines gültigen, amtlichen Lichtbildausweises beweist. Alternativ hierzu kann eine Bestätigung der Identität durch Dritte erfolgen, sofern die initiale Identitätsfeststellung und Ausgabe der Zugangsdaten zu deren Onlineportal den Anforderungen des Art 24 Abs. 1 (1) Lit d [eIDAS-VO] entspricht. Diese Bestätigung wird in elektronischer Form, durch die öffentliche Stelle signiert, vor der Zertifikatsausstellung an A-Trust übermittelt.

Als Antrag wird verstanden, wenn die signierende Person entweder selbst oder durch Dritte freiwillig ihre Personendaten an die A-Trust übermittelt, um in den Besitz einer a.sign premium Karte zu kommen. Es wird ebenfalls die persönliche Kontaktaufnahme mit einer Registrierungsstelle zur Aktivierung eines Zertifikats, wie auch die Nutzung einer entsprechenden Webanwendung zur Aktivierung eines Zertifiats als Antrag verstanden. Die Freiwilligkeit bestätigt die signierende Person mit dem Akzeptieren des zustande kommenden Signaturvertrages.

Qualifizierte Zertifikate, die auf die Namen Max Mustermann, Test Test, Musterfrau Maxine lauten oder deren Namen mit „XXX“ beginnen, werden von der A-Trust GmbH zu Testzwecken ausgestellt. Aus diesem Grund wird bei Ausstellung von qualifizierten Zertifikaten auf die genannten Namen keine Identitätsprüfung durchgeführt.

3.3.2 Erneute Registrierung/Rezertifizierung

Die signierende Person kann nach einem Widerruf ein Ersatzprodukt bestellen und analog der Erstregistrierung aktivieren. Dabei sind allfällige Änderungen in den personenbezogenen Daten anzugeben.

Es ist ebenfalls zulässig, dass ein neues a.sign premium Zertifikat, mittels einer noch gültigen qualifizierten oder fortgeschrittenen Signatur durch die signierende Person selbst aktiviert wird. In diesem Falle ist keine erneute Registrierung / Rezertifizierung erforderlich.

Sollten sich Zertifikatsdaten geändert haben, muss eine erneute Registrierung / Rezertifizierung erfolgen. Werden geänderte Zertifikatsdaten einer signierenden Person von einer öffentlichen Stelle signiert übermittelt, wird der Prozess der Registrierung/Rezertifizierung automatisiert durchgeführt (§ 4 Abs 4 [E-GovG]).

3.3.3 Ausstellung von Zertifikaten

Die mit den Schlüsseln versehene a.sign premium Karte wird entweder an die zuständige Registrierungsstelle weitergeleitet und die signierende Person nimmt sie dort entgegen oder die signierende Person ist bereits im Besitz einer signaturfähigen Karte.

Persönliche Ausstellung:

Für die Ausstellung der Zertifikate der antragstellenden Person wird diese persönlich in einer Registrierungsstelle vorstellig. Die Registrierungsstelle stellt die Zertifikate aus, wenn

- die Identität der antragstellenden Person anhand eines gültigen, amtlichen Lichtbildausweises (zulässige Ausweise siehe Kapitel 3.3.1) überprüft wurde,
- die antragstellende Person unterrichtet wurde und
- die Allgemeinen Geschäftsbedingungen [AGB] akzeptiert wurden.

Online-Ausstellung:

Im Zuge der Online-Ausstellung ist es für die signierende Person notwendig die Identität mittels des Aktivierungscodes (mittels RSa Brief an die signierende Person übermittelt) und des beim Antrag selbst gewählten Widerrufspasswortes zu bestätigen. Alternativ hierzu kann eine Bestätigung der Identität durch Dritte erfolgen, sofern die initiale Identitätsfeststellung und Ausgabe der Zugangsdaten zu deren Onlineportal den Anforderungen des Artikel 24(1) Lit d [eIDAS-VO] entspricht. Diese Bestätigung wird in elektronischer Form, durch diese Dritten signiert, vor der Zertifikatsausstellung an A-Trust übermittelt. Im Rahmen der weitern Schritte können die Personendaten nicht mehr geändert werden. Es wird ausschließlich auf bereits verifizierte Personendaten zur Ausstellung des Zertifikats zurückgegriffen, die von der Karten ausgebenden Stelle an die A-Trust zur Verwendung frei gegeben und übermittelt werden.

Die Webanwendung bietet der signierenden Person noch vor Aktivierung des Zertifikats die Möglichkeit sich die Unterrichtung und die Allgemeinen Geschäftsbedingungen [AGB] anzusehen und auf einem eigenen dauerhaften Datenträger zu speichern.

In den Ausstellungsfällen gilt die Ausstellung als abgeschlossen, wenn der Signaturvertrag der signierenden Person unterschrieben ist und das Zertifikat ausgestellt wurde. A-Trust unterscheidet nicht, ob der unterschriebene Signaturvertrag in physischer (Papier) oder elektronischer Form unterzeichnet vorliegt.

Durch die folgenden Maßnahmen wird sichergestellt, dass Ausstellung, Verlängerung und Neuausstellung von Zertifikaten in sicherer Weise erfolgen und den Anforderungen des [SVG] und des [eIDAS-VO] entsprechen.

1. Die Zertifikate werden gem. den Bestimmungen in Anhang I [eIDAS-VO] als X.509 v3 Zertifikate erstellt. Die in den Zertifikaten enthaltenen Angaben sind insb. die folgenden:
   - Versionsnummer des Zertifikats: es werden Zertifikate der Version 3 (codiert mit dem Wert 2) ausgestellt
   - Seriennummer des Zertifikats
   - Bezeichnung des Zertifikatsausstellers
   - Beginn und Ende der Gültigkeit des Zertifikats
   - Bezeichnung der signierenden Person
   - öffentlicher Schlüssel (mit Angabe des Algorithmus)
   - Angabe des Algorithmus für die Signatur des Zertifikats
   - Signatur über das Zertifikat
   - Zertifikatserweiterungen, wie z.B.:
     - Bezeichnung als qualifiziertes Zertifikat
     - Informationen über die anzuwendende Policy bzw. CPS
     - Zertifikatsverwendung
     - Information zum Auffinden der CRL
     - Geburtsdatum der signierenden Person (optional), verpflichtend bei Minderjährigen
     - Optionales Behördenkennzeichen und ggf. eine optionale Verwaltungsbezeichnung.
2. Das Zertifikat wird bei der Registrierung auf Veranlassung der Registrierungsstelle erzeugt, nachdem die antragstellende Person identifiziert und die Korrektheit aller Daten bestätigt wurden. Das Verfahren ist für Verlängerung und Neuausstellung identisch.
3. Das Signatur-Schlüsselpaar der a.sign premium Karte wurde anlässlich der Initialisierung der Karte erstellt.
4. Für alle a.sign premium Karten gilt:
   - Jeder signierenden Person wird eine innerhalb der A-Trust einmalig vergebene und eindeutige Identifikationsnummer (CIN) zugeordnet. Diese Identifikationsnummer ist Teil des hervorgehobenen Namens und stellt damit Eindeutigkeit sicher.

- Die in der Registrierungsstelle aufgenommenen Daten werden signiert und verschlüsselt an die Zertifizierungsstelle übertragen. Vertraulichkeit und Integrität sämtlicher Daten ist damit sichergestellt.
- Alle RA-Mitarbeitenden weisen sich mit qualifizierten Zertifikaten aus. Die Authentizität der übermittelten Registrierungsdaten wird durch Verifizierung der Signatur überprüft.

3.3.4 Bekanntmachung der Vertragsbedingungen

A-Trust macht den signierenden Personen und überprüfenden Personen von Signaturen die Bedingungen betreffend der Benutzung des qualifizierten Zertifikats durch Veröffentlichung der nachfolgenden Dokumente auf der A-Trust Homepage zugänglich:

- der gegenständlichen Anwendungsvorgabe (Certificate Policy),
- des Zertifizierungsrichtlinie für a.sign premium, siehe [CPS],
- der Allgemeinen Geschäftsbestimmungen [AGB],
- der Belehrungen für die signierende Person,
- der sonstigen Mitteilungen.

Änderungen werden der signierenden Person mittels Bekanntmachung auf der A-Trust Homepage und gegebenenfalls per Mail oder Brief mitgeteilt.

3.3.5 Veröffentlichung der Zertifikate

Von A-Trust ausgestellte Zertifikate werden der signierenden Person und, je nach Vereinbarung mit dieser, den Signaturempfangenden folgendermaßen verfügbar gemacht.

- Anlässlich der Erstellung eines Zertifikats wird dieses am Ende des Registrierungsvorgangs auf die a.sign premium Karte der signierenden Person gespeichert.
- Wenn die signierende Person damit einverstanden ist, wird das Zertifikat im Verzeichnisdienst von A-Trust veröffentlicht.
- Die Bedingungen für die Benutzung eines Zertifikats werden von A-Trust allen Beteiligten zur Kenntnis gebracht (siehe Kapitel 3.3.4).
- Die Identifikation der anzuwendenden Bestimmungen ist durch die eindeutige Zuordnung zum Produktnamen “a.sign premium” einfach herstellbar.

- Der Verzeichnisdienst ist 7 Tage 24 Stunden verfügbar.

  Unterbrechungen von mehr als 30 Minuten werden gemäß § 5 (5) [SVV] als Störfälle dokumentiert.

- Der Verzeichnisdienst ist öffentlich und international zugänglich.

3.3.6 Aussetzung und Widerruf

a.sign premium Zertifikate können vorübergehend ausgesetzt werden. Diese Aussetzung kann auch in einen endgültigen Widerruf umgewandelt werden. Ebenso ist ein sofortiger und permanenter Widerruf des Zertifikats möglich. Die signierende Person wird von einer erfolgten Aussetzung oder einem Widerruf informiert.

Die Vorgangsweisen für das Auslösen von Aussetzung und Widerruf sind in der Zertifizierungsrichtlinie für a.sign premium (siehe [CPS]) dokumentiert, insbesondere:

- wer berechtigt ist einen Widerruf zu beantragen,
- wie ein Widerrufsantrag gestellt werden kann,
- die Umstände unter denen eine Aussetzung möglich ist,
- die Mechanismen für die Bereitstellung von Statusinformationen und
- die maximale Zeitdauer, die zwischen Einlangen eines Widerrufsantrags und der Veröffentlichung des Widerrufs, verstreichen kann.

Eine Aussetzung oder ein Widerruf kann durch die signierende Person vorgenommen werden. Dies kann wie folgt geschehen:

- Die signierende Person wendet sich per Telefon an den Widerrufsdienst.
- Die vertretungsbefugte bzw. die signierende Person veranlasst den Widerruf per Fax.
- Bei Vergessen des Passworts für den Widerruf kann kein Widerruf, sondern nur eine Aussetzung beantragt werden.

Dabei ergeben sich einige Anforderungen an den Ablauf der jeweiligen Alternative. Diese werden nachfolgend aufgeführt.

- Telefonat: Die signierende Person kann rund um die Uhr einen Widerruf per Telefon vornehmen. Die Authentifikation erfolgt nur über das Aussetzungs- und Widerrufs-Passwort, welches die antragstellende Person bei der Bestellung bzw. Registrierung selbst festgelegt hat.
  Die für einen Widerruf benötigten Informationen lassen sich wie folgt zusammenfassen:

  - Persönliche Daten (vollständiger Name, Geburtstag und -ort),
  - Passwort für den Widerruf,
  - Identifikationsnummer der signierenden Person (CIN), Kartennummer oder Seriennummer des Zertifikats.

- Fax: Die signierende Person kann von 0 bis 24 Uhr einen Widerruf per Fax vornehmen. Das Fax muss das Aussetzungs- und Widerrufs-Passwort sowie die vollständige Seriennummer oder die Kartennummer des zu widerrufenden Zertifikats beinhalten.
- Fax: Die vertretungsbefugte bzw. eine bevollmächtigte Person kann von 0 bis 24 Uhr einen Widerruf per Fax vornehmen. Das Fax muss einen Hinweis auf Vertretungsbefugnis sowie die vollständige Seriennummer oder die Kartennummer des zu widerrufenden Zertifikats beinhalten.
- Besuch in einer Registrierungsstelle: Die signierende Person benötigt dazu einen gültigen, amtlichen Lichtbildausweis. Die Registrierungsstelle teilt der signierenden Person die Zertifikatsnummer und das Passwort für den Widerruf mit, womit die signierende Person anschließend den Widerruf beim Widerrufsdienst veranlassen kann.

Ausgesetzte und widerrufene Zertifikate werden in einer Widerrufsliste (CRL) unter Berücksichtigung der nachfolgenden Regelungen veröffentlicht:

- Die aktuelle Update-Frequenz der Widerrufsliste ist im Internet über die Web-Seite der A-Trust abrufbar.
- Jede Widerrufsliste enthält den Zeitpunkt der geplanten Ausgabe der nächsten Liste.
- Falls erforderlich kann eine neue Widerrufsliste auch vorzeitig veröffentlicht werden.
- Jede Widerrufsliste ist mit dem Zertifizierungsschlüssel signiert.

Widerrufslisten werden als X.509 Version 2 CRLs ausgegeben. Die wesentlichen Angaben in den CRLs sind die folgenden:

- Versionsnummer der CRL: Version 2 (codiert mit dem Wert 1)
- Bezeichnung des Ausstellers
- Zeitpunkt der CRL-Ausstellung sowie der nächsten geplanten Ausstellung
- Information über die in der CRL enthaltenen Zertifikate:
  - Seriennummer,

  - Zeitpunkt der Eintragung in die CRL,
  - Eintragungsgrund

- CRL-Erweiterungen
- Angabe des Algorithmus für die Signatur über die CRL
- Signatur über die CRL.

Die Widerrufsdienste sind täglich 24 Stunden verfügbar. Spätestens innerhalb von drei Stunden ab Bekanntwerden des Widerrufsgrundes erfolgt eine Aktualisierung der Widerrufsliste. Widerrufslisten sind täglich 24 Stunden abfragbar. Im Fall von Systemausfällen kommen die in der Zertifizierungsrichtlinie für a.sign premium (siehe [CPS]) genannten Vorkehrungen zum Tragen, um die Auswirkungen möglichst gering zu halten. Statusinformationen über Zertifikate können auch online mittels OCSP abgefragt werden. Die Integrität und Authentizität der OCSP-Antworten sind durch eine Signatur gesichert.

3.4 A-Trust Verwaltung

3.4.1 Sicherheitsmanagement

Es gelten folgenden Bestimmungen:

- A-Trust ist für alle Prozesse im Rahmen der Vertrauensdienste verantwortlich; dies gilt auch für die an Vertragsparteien ausgelagerten Dienste. Die Verantwortlichkeiten der Vertragsparteien sind klar geregelt und Kontrollen zur Überprüfung der ordnungsgemäßen Tätigkeit eingerichtet. Die für die Sicherheit relevanten Vorgehensweisen sind in der Zertifizierungsrichtlinie für a.sign premium veröffentlicht.
- Die Geschäftsführung von A-Trust ist unmittelbar verantwortlich für die Definition der Sicherheitsrichtlinien und deren Kommunikation an die mit sicherheitsrelevanten Vorgängen befassten Mitarbeitenden.
- Die Sicherheitsinfrastruktur von A-Trust wird laufend überprüft und an sich ändernde Anforderungen angepasst. Jegliche Änderungen, die einen Einfluss auf das Ausmaß der erreichten Sicherheit haben, sind von der Geschäftsführung der A-Trust zu genehmigen.
- Alle Sicherheitsmaßnahmen und sicherheitsrelevanten Funktionen zur Bereitstellung der Zertifizierungsdienste werden von A-Trust dokumentiert und entsprechend der Dokumentation implementiert und gewartet.
- Der Betrieb des Rechenzentrums der A-Trust ist ausgelagert. Die Dienstleistenden sind an die Wahrung der Informationssicherheit vertraglich gebunden.

3.4.2 Informationsklassifikation und -verwaltung

A-Trust stellt sicher, dass alle Daten und Informationen in geeigneter Weise abgesichert sind. In der Risiko- und Bedrohungsanalyse sind alle Informationsbestände verzeichnet und gem. ihrer Schutzwürdigkeit klassifiziert.

3.4.3 Personelle Sicherheitsmaßnahmen

Das Personal der A-Trust und deren Beschäftigungsmodalitäten sind geeignet, das Vertrauen in die Abwicklung der Zertifizierungsdienste zu stärken. Insbesondere wird Wert gelegt auf:

- A-Trust beschäftigt ausschließlich Personal, welches gemäß Artikel 24 (2) [eIDAS-VO] über das benötigte Fachwissen, die Qualifikation und Erfahrung für die jeweilige Position verfügt.
- Sicherheitsrelevante Funktionen und Verantwortlichkeiten werden in den jeweiligen Stellenbeschreibungen dokumentiert. Funktionen, von denen die Sicherheit der Zertifizierungsdienste abhängt, sind eindeutig identifiziert.
- Für das gesamte Personal der A-Trust (unabhängig ob in einem temporären oder ständigen Beschäftigungsverhältnis angestellt) sind klare Stellenbeschreibungen ausgearbeitet, in denen die Pflichten, Zugriffsrechte und Minimalkompetenzen dargelegt sind.
- Die Ausübung sowohl der administrativen als auch der Managementfunktionen steht im Einklang mit den Sicherheitsrichtlinien.
- Alle Leitungsfunktionen sind mit Personen besetzt, die über Erfahrung mit der Technologie digitaler Signaturen und mit der Führung von Personal verfügen, das Verantwortung für sicherheitskritische Tätigkeiten trägt.
- Alle Mitarbeitenden, denen vertrauenswürdige Positionen zugeordnet sind, werden von Interessenskonflikten, die einer unvoreingenommenen Erfüllung der Aufgaben entgegenstehen könnten, frei gehalten.
- Alle vertrauenswürdigen Positionen sind in der Zertifizierungsrichtlinie (siehe [CPS]) im Detail beschrieben.
- Die Zuweisung der Positionen erfolgt mit formeller Ernennung durch die Geschäftsführung.
- A-Trust beschäftigt keine Personen, die strafbare Handlungen begangen haben, die sie für eine vertrauenswürdige Position ungeeignet erscheinen lassen. Eine Beschäftigung erfolgt erst nach einer diesbezüglichen Überprüfung.

3.4.4 Physikalische und organisatorische Sicherheitsmaßnahmen

Es ist sichergestellt, dass der Zutritt zu Räumlichkeiten, in denen sicherheitskritische Funktionen ausgeübt werden, abgesichert ist und Risken einer physischen Beschädigung der Vermögenswerte minimiert sind. Insbesondere gilt:

- Der Zutritt zu den Räumlichkeiten, in denen Zertifizierungs- und Widerrufsdienste erbracht und in denen die a.sign premium Karten initialisiert werden, ist auf autorisiertes Personal beschränkt. Die Systeme, die die Zertifikate ausstellen, sind vor Gefährdung durch Umweltkatastrophen geschützt.
- Es werden Maßnahmen ergriffen, um den Verlust, die Beschädigung oder die Kompromittierung von Anlagen und die Unterbrechung des Betriebes zu verhindern.
- Weitere Maßnahmen gewährleisten, dass eine Kompromittierung oder ein Diebstahl von Daten und datenverarbeitenden Anlagen nicht möglich ist.
- Die Systeme für Zertifikatsgenerierung, Kartenbereitstellung und die Widerrufsdienste werden in einer gesicherten Umgebung betrieben, sodass eine Kompromittierung durch unautorisierte Zugriffe nicht möglich ist.
- Die Abgrenzung der Systeme für Zertifikatsgenerierung, Kartenbereitstellung und Widerrufsdienste erfolgt durch klar definierte Sicherheitszonen d.h. durch räumliche Trennung von anderen organisatorischen Einheiten und physischen Zutrittsschutz.
- Die Sicherheitsmaßnahmen inkludieren den Gebäudeschutz, die Computersysteme selbst und alle sonstigen Einrichtungen, die für deren Betrieb unerlässlich sind. Der Schutz der Einrichtungen für die Zertifikatserstellung, Kartenproduktion und Bereitstellung der Widerrufsdienste umfasst physische Zutrittskontrolle, Abwendung von Gefahren durch Naturgewalten, Feuer, Rohrbrüche und Gebäudeeinstürze, Schutz vor Ausfall von Versorgungseinheiten, Diebstahl, Einbruch und Systemausfällen.
- Die unautorisierte Entnahme von Informationen, Datenträgern, Software und Einrichtungsgegenständen, welche zu den Zertifizierungsdiensten gehören, wird durch Kontrollmaßnahmen verhindert.

3.4.5 Betriebsmanagement

A-Trust stellt sicher, dass das Zertifizierungssystem sicher und korrekt betrieben und das Risiko des Versagens minimiert wird. Insbesondere gilt:

- Die Integrität der Computersysteme und Informationen ist gegen Viren und böswillige oder unautorisierte Software geschützt.

- Schaden durch sicherheitskritische Zwischenfälle und Fehlfunktionen wird durch entsprechende Aufzeichnungen und Fehlerbehebungsprozeduren verhindert.
- Datenträger werden vor Beschädigung, Diebstahl und unautorisiertem Zugriff geschützt.
- Für die Ausführung von sicherheitskritischen und administrativen Aufgaben, die sich auf die Erbringung der Zertifizierungsdienste auswirken, sind Verfahrensweisen definiert und in Kraft gesetzt.
- Datenträger werden je nach ihrer Sicherheitsstufe (siehe Kapitel 3.4.2) behandelt und aufbewahrt. Nicht mehr benötigte Datenträger, die vertrauliche Daten beinhalten, werden in sicherer Weise vernichtet.
- Kapazitätserfordernisse werden beobachtet und künftige Entwicklungen prognostiziert, sodass stets die angemessene Prozessorleistung und Speicherplatz zur Verfügung stehen.
- Auf Zwischenfälle wird so rasch wie möglich reagiert, um die sicherheitskritischen Vorkommnisse auf ein Minimum zu begrenzen. Alle Zwischenfälle werden baldmöglichst aufgezeichnet.

Die sicherheitskritischen Funktionen im Rahmen der Zertifizierungs- und Widerrufsdienste werden von den gewöhnlichen Funktionen strikt getrennt.

Sicherheitskritische Funktionen inkludieren:

- Operationale Funktionen und Verantwortungen
- Planung und Abnahme von Sicherheitssystemen
- Schutz vor Schadsoftware
- Allgemeine Wartungstätigkeiten
- Netzwerkadministration
- Aktive Überprüfung von Log-Files und Prüfberichten, Analyse von Zwischenfällen
- Datenträgerverwaltung und –sicherheit
- Daten- und Softwareaustausch

Diese Aufgaben werden von A-Trust-Sicherheitsbeauftragten geregelt, können aber von operativem Personal (unter Beaufsichtigung) gem. Sicherheitskonzept und Stellenbeschreibungen durchgeführt werden.

3.4.6 Zugriffsverwaltung

A-Trust stellt durch die nachfolgenden Maßnahmen sicher, dass der Zugriff auf das Zertifizierungssystem ausschließlich auf ordnungsgemäß autorisierte Personen beschränkt ist.

- Sicherungsmaßnahmen wie z.B. Firewalls bewahren das interne Netzwerk vor Zugriffen durch Dritte.
- Vertrauliche Daten werden geschützt, wenn sie über unsichere Netzwerke ausgetauscht werden, wie z.B. die Registrierungsdaten.
- Eine Benutzer:innen-Verwaltung, die den verschiedenen Funktionen unterschiedliche Zugriffsrechte einräumt, ist eingerichtet; insbesondere werden sicherheitsrelevante von nicht sicherheitskritischen Funktionen sorgfältig getrennt. Änderungen in den Zugriffsrechten werden im System sofort nachgezogen und sind Teil des internen Audits.
- Zugriff auf Informationen und Anwendungen ist auf Grund der vergebenen Zugriffsrechte eingeschränkt. Die dafür geltenden Definitionen sind im Zertifizierungsrichtlinie für a.sign premium (siehe [CPS]) angeführt. Administrative und den laufenden Betrieb betreffende Funktionen sind streng getrennt. Die Verwendung von System-Utility-Programmen ist besonders eingeschränkt.
- Das Personal muss sich vor jedem kritischen Zugriff auf Applikationen, die in Zusammenhang mit dem Zertifikatsmanagement stehen, authentifizieren.
- Die Zugriffe werden in Log-Dateien aufgezeichnet. Das Personal wird für die ausgeführten Tätigkeiten zur Verantwortung gezogen.
- Eine Wiederverwendung von Datenspeichern führt nicht zur Offenlegung von vertraulichen Daten an nicht autorisierte Personen.
- Komponenten des lokalen Netzwerks befinden sich in einer physisch gesicherten Umgebung und die Konfiguration wird periodisch überprüft.
- Die Entdeckung von unautorisierten und/oder außergewöhnlichen Zugriffsversuchen auf die eigentliche Zertifizierungsstelle und die Widerrufsdienste wird durch geeignete Maßnahmen gesichert, sodass ggf. sofort Gegenmaßnahmen ergriffen werden können. Dies geschieht durch die Führung und Auswertung von CA-Logfiles und Firewall-Logfiles.
- Ändernde Zugriffe (Löschungen, Hinzufügungen) auf die Verzeichnis- und Widerrufsdienste werden durch Passworteingabe abgesichert.
- Versuche des unautorisierten Zugriffs auf Verzeichnis- und Widerrufsdienste werden aufgezeichnet.

3.4.7 Entwicklung und Wartung vertrauenswürdiger Systeme

A-Trust verwendet vertrauenswürdige Systeme und Produkte, die gegen Veränderung geschützt sind.

- Eine Analyse der Sicherheitsanforderungen muss im Stadium der Design- und Anforderungsspezifikation im Rahmen jedes Entwicklungsprojekts erfolgen, das von A-Trust oder von Dritten im Auftrag von A-Trust durchgeführt wird.
- Änderungskontrollprozeduren existieren für die Erstellung von geplanten Programmversionen, sonstigen Änderungen und Fehlerbehebungen.

3.4.8 Erhaltung des ungestörten Betriebes und Behandlung von Zwischenfällen

A-Trust wird sich bemühen, nach Katastrophenfällen, inklusive der Kompromittierung eines Zertifizierungsschlüssels, den Betrieb so rasch wie möglich wieder aufzunehmen. Insbesondere ist vorgesehen:

- Der Notfallsplan von A-Trust sieht die (vermutete) Kompromittierung des privaten Zertifizierungsschlüssels als Katastrophenfall vor.
- Sollte dieser Fall eintreten, so hat A-Trust die Aufsichtsstelle gemäß des Artikels 19 (2) [eIDAS-VO], die signierenden Personen, die auf die Sicherheit der Zertifizierungsdienste vertrauenden Personen und ggf. andere Zertifizierungsdiensteanbietende, mit denen Vereinbarungen bestehen, davon zu unterrichten und mitzuteilen, dass die Widerrufs- und Zertifikatsinformationen nicht mehr als zuverlässig anzusehen sind.
- Zertifikate und Widerrufslisten werden als nicht mehr gültig gekennzeichnet.

3.4.9 Einstellung der Tätigkeit

Gemäß Artikel 24 (2) Lit. a [eIDAS-VO] wird A-Trust die Einstellung der Tätigkeit unverzüglich der Aufsichtsstelle anzeigen und sicher stellen, dass eine eventuelle Beeinträchtigung der Dienstleistung gegenüber signierenden Personen und vertrauenden Parteien möglichst gering gehalten wird.

1. Vor Beendigung der Dienstleistung werden
   - alle signierenden Personen, Zertifizierungsdiensteanbietenden und sonstige Parteien, mit denen A-Trust eine geschäftliche Verbindung unterhält, direkt, sowie jene Parteien, die auf die Zuverlässigkeit der Zertifizierungsdienste vertrauen, durch Veröffentlichung von der Einstellung unterrichtet,

- die Verträge mit Subunternehmen (Registrierungsstellen, kartenherstellende Unternehmen etc.) zur Erbringung von Zertifizierungsdiensten beendet,
- Vorkehrungen zur Übernahme der Verzeichnis- und Widerrufsdienste sowie der Aufzeichnungen gemäß Kapitel 3.4.11 durch andere Zertifizierungsdiensteanbietende getroffen,
- die privaten Schlüssel von A-Trust von der Nutzung zurückgezogen und in Entsprechung zu Abschnitt 3.2.6 zerstört.

2. Die Abdeckung der Kosten für o.a. Vorkehrungen sind durch Gesellschaftergarantien abgedeckt.
3. Das Zertifizierungsrichtlinie von A-Trust (siehe [CPS]) benennt die Vorkehrungen, die bei Einstellung der Tätigkeit getroffen werden, insbesondere jene Vorkehrungen
   - für die Benachrichtigung der betroffenen Personen und Organisationen,
   - für die Übertragung der Verpflichtungen auf Drittparteien und
   - wie der Widerrufsstatus von nicht abgelaufenen Zertifikaten gehandhabt wird.

3.4.10 Übereinstimmung mit gesetzlichen Regelungen

A-Trust handelt grundsätzlich in Übereinstimmung mit den gesetzlichen Regelungen und Auflagen gemäß [SVG] und [eIDAS-VO], insbesondere sind nachfolgende Punkte sicher gestellt:

- Wichtige Aufzeichnungen werden vor Verlust, Zerstörung und Verfälschung bewahrt.
- Die Anforderungen des Datenschutzgesetzes [DSGVO] werden befolgt.
- Nötige technische und organisatorische Maßnahmen wurden ergriffen, um persönliche Daten vor unautorisierter und ungesetzlicher Verarbeitung sowie vor versehentlicher Zerstörung oder Beschädigung zu schützen.
- Den signierenden Personen wird versichert, dass die an A-Trust übermittelten Informationen nur mit ihrem Einverständnis, mit gerichtlichem Beschluss oder auf Basis gesetzlicher Regelungen offen gelegt werden.

3.4.11 Aufbewahrung der Informationen zu qualifizierten Zertifikaten

Alle Informationen, die in Zusammenhang mit qualifizierten Zertifikaten stehen, werden entsprechend [SVG] aufbewahrt. Insbesondere gilt:

1. Die Vertraulichkeit und Integrität der aktuellen sowie der archivierten Datensätze ist gewahrt.

2. Die Datensätze zu qualifizierten Zertifikaten werden vollständig und vertraulich in Übereinstimmung mit der veröffentlichten Zertifizierungsrichtlinie (siehe [CPS]) archiviert.

3. Aufzeichnungen bezüglich qualifizierter Zertifikate werden für die Beweisführung der ordnungsgemäßen Zertifizierung im Rahmen gerichtlicher Auseinandersetzungen verfügbar gemacht. Zusätzlich hat die signierende Person zu den Registrierungs- und sonstigen persönlichen Daten, die sie betreffen, Zugang.

4. Die Aufzeichnungen umfassen auch den genauen Zeitpunkt des Eintretens wichtiger Ereignisse, die in Zusammenhang mit der Systemumgebung, dem Schlüssel- und dem Zertifikatsmanagement stehen.

5. Die Dokumentation entsprechend Artikel 24 (2) Lit. h [eIDAS-VO] wird gemäß § 10 (3) [SVG] für 30 Jahre nach Ablauf der Gültigkeit elektronisch aufbewahrt. Das Antragsformular (Signaturvertrag) wird für drei Jahre in der betreffenden Registrierungsstelle im Original aufbewahrt.

6. Alle Aufzeichnungen erfolgen derart, dass sie innerhalb der Aufbewahrungsfrist nicht leicht gelöscht oder zerstört werden können.

7. Die spezifischen Ereignisse und Daten die aufgezeichnet werden, sind in der Zertifizierungsrichtlinie (siehe [CPS]) dokumentiert.

8. Insbesondere werden alle Registrierungsinformationen, inkl. jener, die im Zusammenhang mit der Verlängerung der Gültigkeitsdauer von Zertifikaten stehen, elektronisch aufbewahrt.

9. Die aufzuzeichnenden Registrierungsinformationen beinhalten insbesondere:

   - die Art des Identifikationsdokuments, das anlässlich der Registrierung vorgelegt wurde,
   - die Daten des Identifikationsdokuments,
   - die Aufbewahrungsstelle der elektronischen Kopien der Antragsdokumente inklusive der Archivierung der Ausweisdaten,
   - die Akzeptanz der vertraglichen Vereinbarungen
   - von der signierenden Person gewählte und akzeptierte Zertifikatsinhalte,
   - Angabe der Registrierungsstelle und des zuständigen Personals.

10. Die Vertraulichkeit der Daten der signierenden Personen ist gewährleistet.

11. Es werden alle Ereignisse, die den Lebenszyklus der CA-Schlüssel von A-Trust betreffen, aufgezeichnet.

12. Es werden alle Ereignisse, die den Lebenszyklus der Zertifikate betreffen, aufgezeichnet.

13. Es werden alle Ereignisse, die im Zusammenhang mit der Generierung der Schlüssel der signierenden Personen stehen, aufgezeichnet.

14. Es werden alle Ereignisse, die im Zusammenhang mit der Initialisierung und Personalisierung der a.sign premium Karte stehen aufgezeichnet.

3.5 Organisatorisches

A-Trust ist als Organisation zuverlässig und hält die folgenden Richtlinien strikt ein:

3.5.1 Allgemeines

- Alle Richtlinien und Vorgehensweisen sind nicht-diskriminierend.
- Die Dienstleistungen von A-Trust stehen allen Personen zur Verfügung, die über einen in Österreich ausgestellten amtlichen Lichtbildausweis (die zulässigen Lichtbildausweise sind auf der A-Trust Homepage aufgezählt) oder einen international gültigen Reisepass in deutscher und/oder englischer Sprache verfügen.
- A-Trust ist eine juristische Person (Gesellschaft mit beschränkter Haftung).
- A-Trust verfügt über Systeme zur Qualitätssicherung und Gewährleistung der Informationssicherheit, die den angebotenen Zertifizierungsdiensten angemessen sind.
- Die Haftung, insbesondere diejenige zur Schadenswiedergutmachung, entspricht den Bestimmungen des [SVG] und [eIDAS-VO] (siehe Kapitel 2.4).
- Hinsichtlich der finanziellen Ausstattung befolgt A-Trust die Bestimmungen des Artikels 24 (2) Lit. c [eIDAS-VO].
- Das von A-Trust beschäftigte Personal verfügt entsprechend den Bestimmungen [eIDAS-VO] (siehe auch Kapitel 3.4.3) über die nötige Schulung, Training, technisches Wissen und Erfahrung und ist in ausreichender Zahl vorhanden, um den geplanten Umfang der Zertifizierungsdienste bewerkstelligen zu können.
- Es sind Richtlinien und Vorgehensweisen für die Behandlung von Beschwerden und Streitfällen vorhanden, die von allen Parteien an die A-Trust herangetragen werden und die Erbringung ihrer Dienstleistungen betreffen.
- Die rechtlichen Beziehungen zu Subunternehmen, die Dienstleistungen für A-Trust erbringen, sind vertraglich geregelt und ordnungsgemäß dokumentiert.
- Es gibt keine aktenkundigen Gesetzesverletzungen seitens A-Trust.

3.5.2 Zertifikatserstellungs- und Widerrufsdienste

Die für die Erbringung von Zertifizierungs- und Widerrufsdiensten vorgesehenen organisatorischen Einheiten sind hinsichtlich ihrer Entscheidungen über die Erbringung, Aufrechterhaltung und Beendigung der Dienstleistungen der A-Trust unabhängig von anderen Gesellschaften. Die Geschäftsführung und das Personal, das vertrauliche und leitende Funktionen ausübt, sind frei von kommerziellem, finanziellem und sonstigem Druck, der das Vertrauen in ihre Tätigkeit negativ beeinflussen könnte.

Die für die Zertifizierungs- und Widerrufsdienste bestimmten Einheiten verfügen über eine dokumentierte Struktur, die die Unvoreingenommenheit der Aufgabenausführung gewährleistet.

A Anhang

A.1 Begriffe und Abkürzungen

a.sign premium Karte	Eine Prozessorchipkarte, die geheime Schlüssel der kartenbesitzenden Person enthält und zur Erstellung und Verifizierung digitaler Signaturen dient.
Aktivierungsdaten	Daten, die zur Aktivierung der Schlüssel benötigt werden.
Audit	Von externen Personen durchgeführte Sicherheitsüberprüfung.
CA (Certification Authority), Zertifizierungsdiensteanbieter	Eine Person oder Stelle, die Zertifikate ausstellt oder anderweitige elektronische Signaturdienste öffentlich anbieten darf.
CA-Schlüssel	Schlüssel der CA, die zur Ausstellung von Zertifikaten und dem Unterschreiben von Widerrufslisten (Zertifizierung) verwendet werden.
CA-Zertifikat, Zertifizierungsstellenzertifikat	Zertifikat der Zertifizierungsstelle, das zur Signatur der Zertifikate der signierenden Personen und der zugehörigen CRLs dient
Certification Policy, Policy	Ein Regelwerk, das den Einsatzbereich eines Zertifikates für eine bestimmte Personengruppe und/oder Anwendungsklasse festhält.
Certification Practice Statement, CPS, Zertifizierungsrichtlinie	Aussagen über die bei der Ausstellung von Zertifikaten von Zertifizierungsdiensteanbietenden eingehaltenen Vorgehensweise.
Dienste (CA-Dienste)	Überbegriff für angebotene Dienstleistungen wie Verzeichnisdienst, Statusauskunft und Zeitstempeldienst.
Dienste-Schlüssel	Schlüssel eines Dienstes (z.B. Signaturschlüssel zur Signatur von Statusauskünften).
Digitale Signatur	Elektronische Signatur, die mit Hilfe von Verfahren der asymmetrischen Kryptographie erzeugt wird.
E-Mail	Electronic Mail; Nachrichten, die in digitaler Form über computerbasierte Kommunikationswege versandt oder empfangen werden.
Elektronische Signatur	Eine Signatur in digitaler Form, die in Daten enthalten ist, Daten beigefügt wird oder logisch mit ihnen verknüpft ist und von einer signierenden Person verwendet wird, um zu bestätigen, dass der Inhalt dieser Daten gebilligt wird. Sie ist so mit den Daten verknüpft, dass eine nachträgliche Veränderung der Daten offenkundig wird.
Gültigkeitsmodell	Modell, nach dem die Prüfung der Gültigkeit von Zertifikaten und Signaturen vorgenommen wird.

Hardware Security Modul, HSM	Elektronisches System zur sicheren Speicherung von Schlüsseln und zur Berechnung und Verifizierung von Signaturen.
Integrität (von Daten)	Ein Zustand, in dem Daten weder von Unbefugten verändert noch zerstört wurden.
Kettenmodell	Gültigkeitsmodell, nach dem eine gültige Anwendung des Schlüssels dann erfolgt, wenn zum Zeitpunkt der Anwendung das Zertifikat gültig ist und das übergeordnete Zertifikat zum Zeitpunkt der Erstellung des eingesetzten Zertifikats gültig war.
Kompromittierung	Eine unautorisierte Offenlegung von oder der Verlust der Kontrolle über sicherheitskritische Informationen und geheim zuhaltende Daten.
LDAP	Lightweight Directory Access Protocol ist ein Standard Protokoll für Verzeichnisdienste (LDAP Server) im Internet.
OCSP	Online Certificate Status Protocol, Protokoll für die Statusauskunft
OID	Object Identifier, eine Ganzzahl, durch die ein Objekt (z.B. Policy) eindeutig identifiziert wird.
Öffentlicher Schlüssel	Öffentlicher Teil eines Schlüsselpaares. Er ist Bestandteil eines Zertifikates und wird zur Überprüfung von Digitalen Signaturen bzw. zur Verschlüsselung von Nachrichten/Daten verwendet.
PIN	Personal Identification Number (Aktivierungsdaten).
Privater Schlüssel, geheimer Schlüssel	Geheimer Teil eines Schlüsselpaares, der zum digitalen Signieren sowie zum Entschlüsseln von Nachrichten/Dokumenten erforderlich ist und geheim gehalten werden muss.
Public-Key Infrastructure, PKI	Ein kryptografisches System, das ein Paar von durch einen mathematischen Algorithmus verbundenen Schlüsseln benutzt. Der öffentliche Teil dieses Schlüsselpaars kann jeder Person zugänglich gemacht werden, die Informationen verschlüsseln oder eine digitale Signatur prüfen will. Der geheime (private) Teil wird sicher bewahrt und kann Daten entschlüsseln oder eine digitale Signatur erstellen.
Qualifiziertes Zertifikat	Zertifikat, welches den Bestimmungen des Anhang I [eIDAS-VO] entspricht.
Qualifiziertes Zertifikat für Siegel	Zertifikat, welches den Bestimmungen des Anhang III [eIDAS-VO] entspricht.

Registrierungsstelle, Registration Authority, RA	Eine vertrauenswürdige Einrichtung, welche die Überprüfung der Identität der Zertifikatsbewerbenden im Namen der Zertifizierungsdiensteanbietenden unter Berücksichtigung der Zertifizierungsrichtlinien durchführt und selbst keine Zertifikate ausstellt.
RFC	Request for Comments, Artikel über Standards und Protokolle im Internet. Neue Standards werden zunächst vorgeschlagen und zur Diskussion gestellt (daher "mit der Bitte um Stellungnahme"). Erst nachdem sie ausdiskutiert und für gut befunden worden sind, werden sie unter einer RFC-Nummer veröffentlicht.
Root-CA, Root-Zertifizierungsstelle	Die Root-CA ist die oberste CA in der Zertifizierungshierarchie der A-Trust. Sie stellt die Zertifikate für die nachgeordneten CAs aus.
Root-Zertifikat, Stammzertifikat, Root-CA Zertifikat	Zertifikat des Root-Keys, der zur Signatur der Zertifikate der Zertifizierungsstellen und der zugehörigen CRLs dient
RSA	Signatur- und Verschlüsselungsverfahren; benannt nach Rivest, Shamir und Adleman
Schlüsselpaar	Ein privater Schlüssel und der dazugehörige öffentliche Schlüssel. Abhängig vom verwendeten Algorithmus kann man mit Hilfe des öffentlichen Schlüssels eine digitale Unterschrift, die mit dem dazu gehörigen privaten Schlüssel erstellt wurde, verifizieren bzw. mit dem privaten Schlüssel Daten entschlüsseln, welche mit dem zugehörigen öffentlichen Schlüssel verschlüsselt wurden.
signierende Person	Eine natürliche Person, die eine elektronische Signatur erstellt
Siegelerstellende	Juristische Personen, die ein elektronisches Siegel erstellen
Signaturerstellungsdaten	Signaturerstellungsdaten sind einmalige Daten wie Codes oder private Signaturschlüssel, die von der signierenden Person zur Erstellung einer elektronischen Signatur verwendet werden.
Signaturprüfdaten	Signaturprüfdaten sind Daten wie Codes oder öffentliche Signaturschlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden.
Aussetzung	Eine Aussetzung ist ein zeitlich begrenztes vorübergehendes Aussetzen der Gültigkeit eines a.sign premium Zertifikats.
Statusauskunft	Dienst zur Auskunft, über den aktuellen Status (gültig oder widerrufen) eines Zertifikates

URI	Uniform Resource Identifier, spezifiziert eine bestimmte Datei auf einem bestimmten Server, Oberbegriff für URL (Uniform Resource Locator) und URN (Universal Resource Name).
Verifizierung (einer digitalen Signatur)	Feststellung, dass eine digitale Signatur mit dem privaten Schlüssel, der zu dem in einem gültigen Zertifikat beinhalteten öffentlichen Schlüssel gehört, erstellt wurde und die Nachricht sich nach der Signatur nicht verändert hat.
Verzeichnis (-dienst)	Dienst, bei dem die Zertifikate der CA oder anderer signierenden Personen sowie CRLs abgerufen werden können. Der Zugriff wird über LDAP realisiert.
Widerruf	Der irreversible Vorgang der vorzeitigen Beendigung der Gültigkeit eines Zertifikats ab einem bestimmten Zeitpunkt.
X.509	Der ITU-Standard für Zertifikate. X.509 v3 beschreibt Zertifikate, die mit verschiedenen Zertifikatserweiterungen erstellt werden können
Zeitstempel	Digitale Signatur von digitalen Daten und einem Zeitpunkt. Mit Hilfe eines Zeitstempels kann nachgewiesen werden, dass digitale Dokumente zu einem bestimmten Zeitpunkt existiert haben. Um Manipulationen zu verhindern, soll der Zeitstempel nur von einer vertrauenswürdigen Instanz (z.B. Zertifizierungsstelle) ausgestellt werden.
Signaturempfangende	Person, die Zertifikate über die Schlüssel und Daten anderer nutzt, um Signaturen zu prüfen.
Zertifikats-Widerrufsliste, CRL	Eine digital signierte Datenstruktur, die widerrufene und ausgesetzte Zertifikate anführt, welche von bestimmten Zertifizierungsdiensteanbietenden ausgestellt wurden.

A.2 Referenzdokumente

[AGB] Allgemeine Geschäftsbedingungen (AGB) A-Trust für qualifizierte und fortgeschrittene Zertifikate Version 7.2

[eIDAS-VO] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

[SVG] Bundesgesetz über elektronische Signaturen und Vertrauensdieste für elektronische Transaktionen (Signatur und Vertrauensdienstegesetz - SVG)
StF: BGBl. I Nr. 50/2016 (NR: GP XXV RV 1145 AB 1184 S. 134. BR: 9594 AB 9607 S. 855.)

[SVV] Verordnung über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdiensteverordnung – SVV) StF: BGBl. II Nr. 208/2016

[CPS] A-Trust Zertifizierungsrichtlinie für qualifizierte Zertifikate für sichere Signaturen, in der jeweils aktuellen Version.

[Policy] A-Trust Certificate Policy für qualifizierte a.sign premium Zertifikate für sichere Signaturen

[RFC3647] RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003

[RFC3161] RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol, August 2001

[ETSI 319 411] Policy and security requirements for Trust Service Providers issuing certificates - ETSI EN 319 411-2 v2.2.2 (April 2018)

[ETSI TS 119 495] Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366

[ACOS-ID v2.0] ACOS-IDv2.0 eMRTD (B) EAC/PACE Configuration (Version 2.0 eMRTD (B))

[PSD II-Verordnung] DELEGIERTE VERORDNUNG (EU) 2018/389 DER KOMMISSION vom 27. November 2017

[E-GovG] Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz – E-GovG) StF: BGBl. I Nr. 10/2004 (NR: GP XXII RV 252 AB 382 S. 46. BR: 6959 AB 6961 S. 705.)

[DSGVO] VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)