A-Trust Gesellschaft für Sicherheitssysteme
im elektronischen Datenverkehr 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 Zeitstempel

Version: 1.0.1
Datum: 06.12.2021

Inhaltsverzeichnis

Rev	Autor	Änderungen
1.0.0	IH	Initiale Version
1.0.1	IH	Feedback Auditor

Tabelle 1: Dokumentenhistorie

1 Einführung

1.1 Überblick

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

Die Certificate Policy für qualifizierte Zeitstempel gilt entsprechend der Verordnung (EU) 910/2014 [eIDAS-VO] und dem österreichischen Signatur- und Vertrauensdienstegesetz [SVG], die an Endbenutzer ausgestellt werden, auf sicheren Zeitstempelerstellungseinheiten basieren und für die Erstellung qualifizierter Zeitstempel geeignet sind.

1.2 Dokumentidentifikation

Name der Richtlinie:	A-Trust Anwendungsvorgaben (Certificate Policy) für qualifizierte Zeitstempel
Version:	1.0.1 / 06.12.2021
Object Identifier:	1.2.040.0.17 (A-Trust) .1 (CP) .26 (Zeitstempel) .1.0.1 (Version) vorliegende Version

Der A-Trust OID 1.2.040.0.17 ist bei ÖNORM registriert.

Die vorliegende Policy ist in Übereinstimmung mit ETSI EN 319 421 [Object Identifier: 0.4.0.2023.1.1].

1.3 Anwendungsbereich

Diese Anwendungsvorgaben gelten für die Anwendung des qualifizierten Zeitstempel gem. Artikel 41 und 42 [eIDAS-VO] .

Die Schlüssel der Zeitstempel werden ausschließlich im Rechenzentrum von A-Trust verarbeitet. Der Zeitstempelauslöser erhält Zugangsdaten, welche ausschließlich zum Zweck der Auslösung des Zeitstempels eingesetzt werden dürfen.

1.4 Übereinstimmung mit der Policy

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

2 Verpflichtungen und Haftung

2.1 Verpflichtungen des Zertifizierungsstelle

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

- Die Zeitstempel Zertifikate 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 Zeitstempelauslösern und Aufsichtsbehörden nach.
- Die Zertifizierungsstelle sorgt durch geeignete Maßnahmen (technisch, organisatorisch, infrastrukturell und personell) für den Schutz des privaten Schlüssels der Zertifizierungsstelle.
- Die Zertifizierungsstelle stellt sicher, dass jeder erstellte Zeitstempel in einer Archiv Datenbank gespeichert wird. Dies dient zur Sicherstellung der Eindeutigkeit der ausgestellten Seriennummer.

2.2 Verpflichtungen der Zeitstempelauslöser

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

- Die Zeitstempelauslöser verpflichten sich die relevanten Allgemeinen Geschäftsbedingungen [AGB] zusammen mit der Zeitstempel Anwendungsvorgabe (Policy), der Zertifizierungsrichtlinie und den Entgeltbestimmungen von A-Trust als Grundlage für den abgeschlossenen Vertrag anzuerkennen.
- Der Zeitstempelauslöser setzt Zeitstempel nur zu dem Zweck in der Zertifizierungsrichtlinie und der zugehörigen Anwendungsvorgaben (Policy) ein. Maßgeblich hierfür sind die zum Ausstellungszeitpunkt gültigen Dokumente.
- Der Zeitstempelauslöser ist sich bewusst, dass A-Trust eine Liste mit empfohlenen technischen Komponenten und Verfahren für die Erstellung von qualifizierten

Zeitstempel 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 der qualifizierte Zeitstempel ausgelöst wird, kein unbefugt eingebrachter Programmcode zur Anwendung kommt. Dazu sollen die folgenden Vorgaben von A-Trust einhalten werden:
  - Der Zeitstempelauslöser muss alle notwendigen technischen und organisatorischen Maßnahmen ergreifen, um unbefugten Zugriff auf sein Gerät und die darauf befindlichen Programmcodes zu verhindern.
  - A-Trust verpflichtet den Zeitstempelauslöser, sich an die Empfehlungen des Herstellers des von ihm verwendeten Betriebssystems sowie an die Empfehlungen der Hersteller der anderen Software-Produkte, die er installiert hat, zu halten.
- Der Zeitstempelauslöser ist verpflichtet die jeweiligen nationalen bzw. europäischen Ausfuhrbestimmungen sowie etwaige nationale Nutzungsbeschränkungen bei einer Verwendung im Ausland zu beachten.

2.3 Verpflichtungen der Zertifikatsnutzer

Den Zertifikatsnutzern wird empfohlen, vor der Akzeptanz folgende Prüfungen durchzuführen:

- Der Zertifikatsnutzer prüft den digitalen Zeitstempel.
- Der Zertifikatsnutzer prüft die Gültigkeit des Zertifikats.
- Die Zertifikatsnutzer prüft, ob das Zertifikat zweckgemäß (d.h. für die Erstellung eines Zeitstempel) eingesetzt wurde.

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 Zertifikatsgenerierung 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 für Zeitstempel (siehe [CPS]) benennt die Verpflichtungen aller externen Vertragspartner, die Dienstleistungen für A-Trust unter Beachtung der jeweils anwendbaren Policies und Richtlinien erbringen.
4. A-Trust macht allen Zeitstempelauslösern und Überprüfern von Zeitstempel die Zertifizierungsrichtlinie und jegliche Dokumentation, die die Übereinstimmung mit dieser Anwendungsvorgabe dokumentiert, zugänglich (siehe Kapitel 3.4.3).
5. Die Geschäftsführung der A-Trust stellt das alleinige Entscheidungsgremium dar, das für die Genehmigung der Zertifizierungsrichtlinie für Zeitstempel verantwortlich ist.
6. Die Geschäftsführung der A-Trust trägt auch die Verantwortung für die ordnungsgemäße Implementierung der Zertifizierungsrichtlinie für Zeitstempel.
7. A-Trust hat einen Revisionsprozess zur Überprüfung der Vorgangsweisen der Zertifizierung aufgesetzt, der auch Maßnahmen zur Wartung der Zertifizierungsrichtlinie für Zeitstempel 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 Zeitstempel entsprechend Kapitel 3.4.3 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 3.6.3), mindestens im Vier-Augen-Prinzip in einer physisch abgesicherten Umgebung durchgeführt (siehe 3.6.4).
2. Die Schlüssel werden durch ein Verfahren entsprechend der Anforderungen für fortgeschrittene Zertifikate nach [eIDAS-VO] erstellt.
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 Expertengruppe 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 Zeitstempel 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 Zeitstempel 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.

3.3 Erzeugung des Schlüssel für Zeitstempelzertifikate

Keine Bestimmungen.

3.4 Lebenszyklus des Zertifikats

3.4.1 Registrierung des Zertifikates

Keine Bestimmungen.

3.4.2 Ausstellung von Zertifikaten

Keine Bestimmungen.

3.4.3 Bekanntmachung der Vertragsbedingungen

A-Trust macht den Auslösern und Überprüfern von Zeitstempeln die Bedingungen betreffend der Benutzung des qualifizierten Zeitstempels durch Veröffentlichung der nachfolgenden Dokumente auf der A-Trust Homepage zugänglich:

- der gegenständlichen Anwendungsvorgabe (Certificate Policy),
- des Zertifizierungsrichtlinie für Zeitstempel, siehe [CPS],
- der Allgemeinen Geschäftsbestimmungen [AGB],

- der sonstigen Mitteilungen.

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

3.4.4 Veröffentlichung der Zertifikate

Von A-Trust ausgestellte Zertifikate werden den Überprüfern folgendermaßen verfügbar gemacht.

- 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.

3.4.5 Aussetzung und Widerruf

Keine Bestimmungen

3.5 Zeitstempel

3.5.1 Zeitstempel-Bestimmungen

Jeder ausgegebene Zeitstempel beinhaltet eine eindeutige Identifikationsnummer. Bei Unregelmäßigkeiten in der Zeitrechnung des Zeitstempeldienstleisters werden keine Zeitstempel ausgestellt. Benutzer, die den Zeitstempeldienst nutzen wollen, müssen einen der folgenden Hashalgorithmen verwenden: sha224, sha256, sha384, sha512, sha3-224, sha3-256, sha3-384, sha3-512 oder RIPEMD-256.

3.5.2 Synchronisation der Uhrzeit

Die verwendete Zeit für den Zeitstempel wird regelmäßig gegen mehrere vertrauenswürdige Zeitquellen synchronisiert (u.a. Bundesamt für Eich- und Vermessungswesen) und darf nicht mehr als 1 Sekunde von UTC abweichen. Sollte der Zeitpunkt von diesen Parametern abweichen, wird kein Zeitstempel ausgelöst.

3.6 A-Trust Verwaltung

3.6.1 Sicherheitsmanagement

Es gelten folgenden Bestimmungen:

- A-Trust ist für alle Prozesse im Rahmen der Vertrauensdienste verantwortlich; dies gilt auch für die an Vertragspartner ausgelagerten Dienste. Die Verantwortlichkeiten der Vertragspartner sind klar geregelt und Kontrollen zur Überprüfung der ordnungsgemäßen Tätigkeit eingerichtet. Die für die Sicherheit relevanten Vorgehensweisen sind in der Zertifizierungsrichtlinie für Zeitstempel veröffentlicht.
- Die Geschäftsführung von A-Trust ist unmittelbar verantwortlich für die Definition der Sicherheitsrichtlinien und deren Kommunikation an die mit sicherheitsrelevanten Vorgängen befassten Mitarbeiter.
- 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. Der Dienstleister ist an die Wahrung der Informationssicherheit vertraglich gebunden.

3.6.2 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.

3.6.3 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 alle Mitarbeiter 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 Mitarbeiter, 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.

3.6.4 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 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 und die Widerrufsdienste werden in einer gesicherten Umgebung betrieben, sodass eine Kompromittierung durch unautorisierte Zugriffe nicht möglich ist.
- Die Abgrenzung der Systeme für Zertifikatsgenerierung 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.

3.6.5 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 3.6.2) 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.

3.6.6 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 Benutzerverwaltung, 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. Die Kontrolle der Benutzerverwaltung ist Teil des internen Audits.

- Zugriff auf Informationen und Anwendungen ist auf Grund der vergebenen Zugriffsrechte eingeschränkt. Die dafür geltenden Definitionen sind im Zertifizierungsrichtlinie für Zeitstempel (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.

3.6.7 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.

3.6.8 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 Signatoren, die auf die Sicherheit der Zertifizierungsdienste vertrauenden Personen und ggf. andere Zertifizierungsdiensteanbieter, 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.

3.6.9 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 Signatoren und vertrauenden Parteien möglichst gering gehalten wird.

1. Vor Beendigung der Dienstleistung werden
   - alle Signatoren, Zertifizierungsdiensteanbieter 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 Subunternehmern (Registrierungsstellen, Kartenhersteller etc.) zur Erbringung von Zertifizierungsdiensten beendet,
   - Vorkehrungen zur Übernahme der Verzeichnis- und Widerrufsdienste sowie der Aufzeichnungen gemäß Kapitel 3.6.11 durch einen anderen Zertifizierungsdiensteanbieter 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.

3.6.10 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 Zeitstempelauslöser wird versichert, dass die an A-Trust übermittelten Informationen nur mit ihrem Einverständnis, mit gerichtlichem Beschluss oder auf Basis gesetzlicher Regelungen offen gelegt werden.

3.6.11 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 der Signator zu den Registrierungs- und sonstigen persönlichen Daten, die ihn 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.
6. Alle Aufzeichnung 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 Vertraulichkeit der Daten der Signatoren ist gewährleistet.
10. Es werden alle Ereignisse, die den Lebenszyklus der CA-Schlüssel von A-Trust betreffen, aufgezeichnet.
11. Es werden alle Ereignisse, die den Lebenszyklus der Zertifikate betreffen, aufgezeichnet.
12. Es werden alle Ereignisse, die im Zusammenhang mit der Generierung der Schlüssel der Zeitstempelauslöser stehen, aufgezeichnet.

3.7 Organisatorisches

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

3.7.1 Allgemeines

- Alle Richtlinien und Vorgehensweisen sind nicht-diskriminierend.
- 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 3.6.3) 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 Kunden oder anderen Parteien an die A-Trust herangetragen werden und die Erbringung ihrer Dienstleistungen betreffen.
- Die rechtlichen Beziehungen zu Subunternehmern, die Dienstleistungen für A-Trust erbringen, sind vertraglich geregelt und ordnungsgemäß dokumentiert.
- Es gibt keine aktenkundigen Gesetzesverletzungen seitens A-Trust.

3.7.2 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

UTC	Coordinated Universal Time
Aktivierungsdaten	Daten, die zur Aktivierung der Schlüssel benötigt werden.
Anwender	Person, die die Dienstleistungen der Zertifizierungsstelle der A-Trust nutzt. Anwender sind sowohl Zertifikatsinhaber als auch Zertifikatsnutzer.
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 Signatoren und der zugehörigen CRLs dient
Certification Policy, Policy	Ein Regelwerk, das den Einsatzbereich eines Zertifikates für eine bestimmte Benutzergruppe und/oder Anwendungsklasse festhält.
Certification Practice Statement, CPS, Zertifizierungsrichtlinie	Aussagen über die bei der Ausstellung von Zertifikaten von einem Zertifizierungsdiensteanbieter 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 einem Unterzeichner verwendet wird, um zu bestätigen, dass er den Inhalt dieser Daten billigt. 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 jedermann zugänglich gemacht werden, der Informationen verschlüsseln oder eine digitale Signatur prüfen will, der geheime (private) Teil wird von seinem Besitzer 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 Zertifikatsbewerber im Namen des Zertifizierungsdiensteanbieters 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.
Zeitstempelauslöser	Eine natürliche Person, die einen Zeitstempel auslöst
Aussetzung	Eine Aussetzung ist ein zeitlich begrenztes vorübergehendes Aussetzen der Gültigkeit eines Zeitstempel Zertifikats.
Statusauskunft	Dienst, bei dem die Anwender Auskunft über den aktuellen Status (gültig oder widerrufen) eines Zertifikates abrufen können.
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 Anwender Zertifikate der CA oder anderer Anwender sowie CRLs abrufen 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.
Zertifikatsinhaber	Anwender, dessen Schlüssel und persönliche Daten im Zertifikat der A-Trust festgehalten sind, auch Zeitstempelauslöser genannt.
Zertifikatsnutzer, Signaturempfänger	Anwender, der Zertifikate über die Schlüssel und Daten anderer nutzt, um Zeitstempel zu prüfen.
Zertifikats-Widerrufsliste, CRL	Eine digital signierte Datenstruktur, die widerrufene und ausgesetzte Zertifikate anführt, welche von einem bestimmten Zertifizierungsdiensteanbieter ausgestellt wurden.

A.2 Referenzdokumente

[AGB] Allgemeine Geschäftsbedingungen (AGB) A-Trust für qualifizierte und fortgeschrittene Zertifikate Version 7.0

[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 Zeitstempel Zertifikate für sichere Signaturen, in der jeweils aktuellen Version.

[Policy] A-Trust Certificate Policy für qualifizierte Zeitstempel Zertifikate für sichere Signaturen

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

[SigV] Verordnung zum Signaturgesetz, BGBl II 2000/30, 02. 02. 2000, BGBl. II Nr. 527/2004, 30. 12.2004 und BGBl. II Nr. 3/2008

[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 EN 319 421] Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps, December 2015

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

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

[DSGVO] VERORDNUNG (EU) 2016/679 vom 27. April 2016