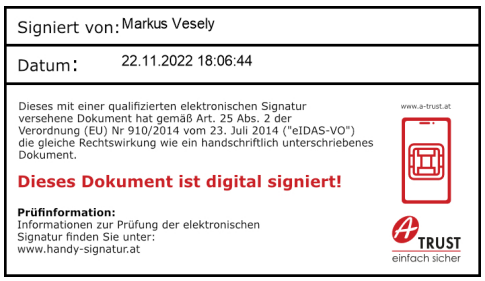
A-Trust Gesellschaft für Sicherheitssysteme
im elektronischen Datenverkehr GmbH
Landstraßer Hauptstraße 1b E02,
A-1030 Wien
Tel: +43 (1) 713 21 51 - 0
Fax: +43 (1) 713 21 51 - 350
https://www.a-trust.at

A-Trust Zertifizierungsrichtlinie (Certificate Practice Statement) für qualifizierte Zeitstempel



Version: 1.0.2

Datum: 29.03.2022

Inhaltsverzeichnis

Rev	Autor	Änderungen
1.0.0	IH	Initiale Version
1.0.1	IH	Feedback Auditor
1.0.2	IH	Feedback Auditor

Tabelle 1: Dokumentenhistorie

Tabellenverzeichnis

Abbildungsverzeichnis

1 Einführung

1.1 Überblick

Das Ziel der vorliegenden Zertifizierungsrichtlinie besteht darin, die Umsetzung der Ausgabe, Administration und Anwendung von Zeitstempel derart festzulegen, dass eine sichere und zuverlässige Durchführung der angebotenen Vertrauensdienstleistungen gewährleistet ist.

Eine Zertifizierungsrichtlinie gibt Auskunft über die Praktiken der Zertifizierungsstellen Sie dient dazu, die Praktiken intern zu fixieren und den Anwendern die Vorgehensweise der Zertifizierungsstelle zu erläutern. Somit können sich die Anwender ein Bild von den vorhandenen Sicherheitsmaßstäben machen.

1.2 Dokumentidentifikation

Name der Richtlinie:	A-Trust Zertifizierungsrichtlinie (Certification Practice Statement) für qualifizierte Zeitstempel
Version:	1.0.2 / 29.03.2022
Object Identifier:	1.2.040.0.17 (A-Trust) .2 (CPS) .21 (Zeitstempel) .1.0.2 (Version) vorliegende Version

Der A-Trust OID 1.2.040.0.17 ist bei ÖNORM registriert.

1.3 Zertifizierungsinfrastruktur und Anwendungsbereich

1.3.1 Zertifizierungsstellen

Es existiert eine zentrale Zertifizierungsstelle, welche die Schlüssel zur Zeitstempelauslösung sowie die Widerrufslisten für Zertifikate signiert. A-Trust stellt qualifizierte Zertifikate (gemäß [eIDAS-VO]) aus.

Die Zertifikate der Root-CA (Stammzertifikat) und der Zertifizierungsstelle (CA-Zertifikat) sind einfache Zertifikate. Die Signaturen, die auf Basis dieser Zertifikate erstellt werden, sind fortgeschrittene Signaturen.

A-Trust erfüllt die Sicherheitsanforderungen gemäß Artikel 19 [eIDAS-VO] und ist in die österreichische Vertrauensliste im Sinne des Artikels 22 [eIDAS-VO] eingetragen.

1.3.2 Anwender

Unter "Anwender" sind die Personen zusammengefasst, die Zeitstempel von A-Trust auslösen (Zeitstempelauslöser), oder welche den Zeitstempel Zertifikatsangaben vertrauen

(vertrauende Beteiligte).

1.3.3 Anwendbarkeit

Dieses Dokument ist relevant für die Zertifizierungsstelle, die angeschlossenen Registrierungsstellen, Dienstleistungen der Zertifizierungs- und Registrierungsstelle und die Anwender. Elektronische Zeitstempel, die in Übereinstimmung mit dieser Zertifizierungsrichtlinie und unter Verwendung der von A-Trust empfohlenen Komponenten und Verfahren erstellt wurden, sind qualifizierte Zeitstempel im Sinne Artikel 42 [eIDAS-VO].

1.3.4 Zertifizierungshierarchie

Abbildung 1 zeigt eine schematische Darstellung der Zertifikatshierarchie.

1.3.5 A-Trust Verzeichnisbaum

Eine schematische Darstellung des Verzeichnisbaums ist in Abbildung 1 zu finden.

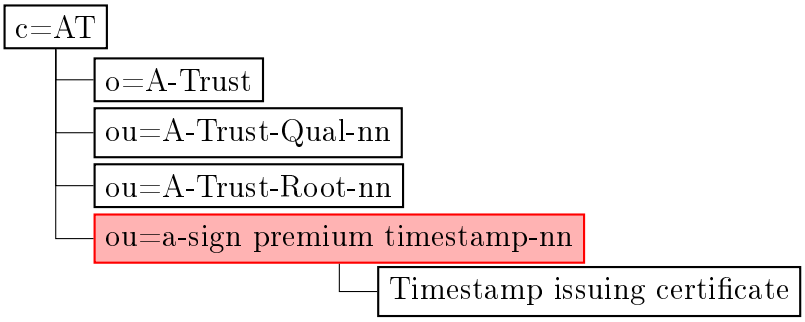


Abbildung 1: A-Trust Verzeichnisbaum

Das Zertifikat des Schlüssels A-Trust-Root-nn ist das A-Trust Stammzertifikat, wobei nn die Version der Root-CA bezeichnet, welche mit dem zugehörigen geheimen Schlüssel digitale Signaturen erstellt. Mit A-Trust-Root-nn werden die CA-Zertifikate und die zugehörigen CRLs signiert. Die Zertifikate der Zertifikatsinhaber von Zeitstempel Zertifikaten und die zugehörigen CRLs werden mit dem CA-Schlüssel a-sign premium timestamp-nn signiert, wobei nn die Version der Zertifizierungsstelle bezeichnet, welche mit dem zugehörigen geheimen Schlüssel digitale Signaturen erstellt.

1.4 Ansprechpartner und Kontaktstellen

1.4.1 Organisation zur Verwaltung dieses Dokuments

A-Trust ist für die Organisation und Verwaltung der Zertifizierungsrichtlinie verantwortlich.

1.4.2 Kontaktinformation

Kontaktinformationen für Zeitstempel Zertifikate erhält man auf folgenden Wegen:

- Auf der Homepage von A-Trust: https://www.a-trust.at
- Bei der Informationshotline des Call Centers: Die Telefonnummer und Erreichbarkeit ist auf der A-Trust Homepage zu finden
- Auf schriftliche Anfrage

Geschäftszeiten A-Trust: 8-18 Uhr

1.4.3 Verantwortlicher für die Anerkennung anderer Anwendungsvorgaben (Policies)

A-Trust übernimmt die Entscheidung über die Anerkennung anderer Anwendungsvorgaben (Policies).

2 Generelle Bestimmungen

2.1 Verpflichtungen

2.1.1 Verpflichtungen des Zertifizierungsdiensteanbieters

Die Zertifizierungsstelle befolgt die Regelungen der Zertifizierungsrichtlinie, die sich insbesondere auf die folgenden Aspekte erstreckt:

- Die Zeitstempel Zertifikate werden im Einklang mit der Anwendungsvorgabe und dieser 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 hinsichtlich Zeitstempelauslöser 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.

2.1.2 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 in der Zertifizierungsrichtlinie und der zugehörigen Anwendungsvorgaben (Policy) angegebenen Zweck 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 eingehalten 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.

2.1.3 Verpflichtungen der Zertifikatsnutzer

Den Zertifikatsnutzern von Zeitstempel (Zeitstempelempfänger) 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 Zeitstempelerstellung) eingesetzt wurde.

2.1.4 Verpflichtungen der Verzeichnisdienste

Der Verzeichnisdienst veröffentlicht in regelmäßigen Abständen die ausgestellten Zertifikate, die zur Veröffentlichung freigegeben sind, sowie Listen der ausgesetzten und widerrufenen Zertifikate.

Der Zertifikatsdienst ist verpflichtet, diese Listen in regelmäßigen Abständen, wie in dieser Zertifizierungsrichtlinie vereinbart, zu aktualisieren und hochverfügbar zu halten.

2.2 Haftung

Die Allgemeinen Geschäftsbedingungen [AGB] bilden zusammen mit der Zertifizierungsrichtlinie, Anwendungsvorgaben (Policy) und den Entgeltbestimmungen der A-Trust in der jeweils gültigen Form die Grundlage für den abgeschlossenen Vertrag.

2.2.1 Haftung der Zertifizierungsstelle

A-Trust haftet gegenüber Dritten, die auf die Richtigkeit des Zertifikats vertraut haben, dass

- die Zeitstempelerstellungsdaten und die ihnen zugeordneten Zeitstempelprüfdaten einander bei der Verwendung der von der A-Trust bereitgestellten oder als geeignet bezeichneten Produkte und Verfahren in komplementärer Weise entsprechen,
- die Anforderungen der [eIDAS-VO] erfüllt und für die Erzeugung und Speicherung von Zeitstempelerstellungsdaten die Anforderungen des Anhangs II [eIDAS-VO] erfüllt werden.
- sie die X.509-Standards einhält,
- die Abläufe, die in der gegenständlichen Zertifizierungsrichtlinie beschrieben sind, einhält.

A-Trust haftet weiters für die Korrektheit eines qualifizierten Zeitstempels, wenn diese unter Einhaltung aller von A-Trust dem Zeitstempelauslöser auferlegten Vorschriften und unter Verwendung der empfohlenen Komponenten und Verfahren erstellt wurde. A-Trust kann in den Zertifikaten eine Haftungsobergrenze (Transaktionslimit) festlegen. Ist ein solches Transaktionslimit im Zertifikat enthalten, haftet A-Trust nur bis zu diesem Betrag. Wenn kein Betrag angegeben ist, liegt keine Haftungsbeschränkung vor.

A-Trust haftet nicht, wenn sie nachweist, dass sie und ihre Mitarbeiter an der Verletzung ihrer Verpflichtungen kein Verschulden trifft (Artikel 13 [eIDAS-VO]).

A-Trust haftet nicht für entgangenen Gewinn, Folgeschäden oder ideellen Schaden des Nutzers.

2.2.2 Haftung der Registrierungsstelle

Keine Bestimmungen.

2.3 Finanzielle Verantwortung

2.3.1 Schadensersatz der beteiligten Parteien

Keine Bestimmungen.

2.3.2 Treuhänderische Beziehungen

Keine Bestimmungen.

2.3.3 Administrative Prozesse

Keine Bestimmungen.

2.4 Auslegung und (gerichtliche) Durchsetzung

2.4.1 Zugrunde liegende Gesetzesbestimmungen

Der zwischen A-Trust und dem Zeitstempelauslöser geschlossene Vertrag unterliegt dem österreichischen Recht und richtet sich nach [eIDAS-VO], [SVG] und [SVV]. Im Verhältnis zu ausländischen Signatoren wird die Anwendung des UN-Kaufrechts ausdrücklich ausgeschlossen.

Qualifizierte Zeitstempel, die in Übereinstimmung mit dieser Zertifizierungsrichtlinie auf Basis eines qualifizierten Zeitstempel Zertifikats erstellt wurden, sind in ihrer Rechtswirkung in Artikel 41 [eIDAS-VO] beschrieben.

2.4.2 Trennbarkeit der Bestimmungen, Fortbestehen von Ansprüchen, Fusion, Kündigung

A-Trust ist berechtigt, Rechte und Pflichten aus dem bestehenden Vertrag auf Dritte zu übertragen. Dem Zeitstempelauslöser entsteht dadurch kein besonderes Kündigungsrecht, solange der Dritte die Rechten und Pflichten des Vertrags erfüllt.

Änderungen der Allgemeinen Geschäftsbedingungen [AGB] wie der Zertifizierungsrichtlinie werden dem Zeitstempelauslöser schriftlich mitgeteilt. Ändert A-Trust die Allgemeinen Geschäftsbedingungen, so hat der Zeitstempelauslöser jederzeit die Möglichkeit zu kündigen. Widerspricht der Zeitstempelauslöser den geänderten Allgemeinen Geschäftsbedingungen nicht binnen eines Monats, so gelten diese als akzeptiert.

2.4.3 Schlichtungsverfahren

Keine Bestimmungen.

2.5 Gebühren

Die aktuell gültige Gebührenregelung findet sich in den Entgeltbestimmungen.

2.5.1 Ausgabe und Erneuerung von Zertifikaten

Die aktuell gültige Regelung findet sich in den Entgeltbestimmungen.

2.5.2 Abrufen von Statusinformationen

Der Zugang zu Widerrufslisten und Statusinformationen ist kostenfrei.

2.5.3 Gebühren für weitere Dienste

Weitere Dienstleistungen können gebührenpflichtig zur Verfügung gestellt werden.

2.5.4 Richtlinien für Gebührenrückerstattung

Der Zeitstempelauslöser hat keinen Anspruch auf Gebührenrückerstattung.

2.6 Bekanntmachung und Verzeichnisdienste

2.6.1 Web-Seiten und Verzeichnisse

A-Trust stellt folgende Web-Seiten und Verzeichnisse bereit:

Bekanntmachungen:	http://www.a-trust.at/
Verzeichnisdienst:	ldap://ldap.a-trust.at/
Widerrufsliste:	ldap://ldap.a-trust.at/
OCSP:	http://ocsp.a-trust.at/ocsp

Tabelle 2: Homepage und Verzeichnisse

Die Liste der empfohlenen Komponenten und Verfahren für die sichere Zeitstempelerstellung und –prüfung stellt A-Trust auf ihrer Homepage unter http://www.a-trust.at/docs/ zur Verfügung.

Die Informationen betreffend den Widerrufsdienst und die Durchführung von Widerrufen stellt A-Trust unter http://www.a-trust.at/widerruf/ zur Verfügung.

2.6.2 A-Trust Stammzertifikat

Das Stammzertifikat ist zu finden unter

- https://www.a-trust.at/certs/A-Trust-Qual-nnx.crt oder
- http://www.a-trust.at/certs/A-Trust-Qual-nnx.crt

Erläuterung: -nn ist die Versionsnummer der Root-CA: erhöht wird bei Generierung eines neuen Schlüssels und Veränderung des Distinguished Name; -x bezeichnet die Version des Zertifikats: erhöht wird bei Ausstellung eines neuen Zertifikats mit unverändertem DN, unabhängig, ob ein neuer Schlüssel generiert wird, bei einer neuen CA-Version wird immer mit –a begonnen; Beispiel: A-Trust-Qual-02a.crt.

Der Download des Stammzertifikats kann auf sichere Weise über https erfolgen. Über den entsprechenden Menüpunkt auf der A-Trust Homepage oder direkt unter dem oben angeführten Link kann der Download des Stammzertifikats erfolgen.

2.6.3 A-Trust CA-Zertifikat

Das benötigte CA-Zertifikat Zertifikate ist unter

- https://www.a-trust.at/certs/a-sign premium timestamp-nnx.crt oder
- http://www.a-trust.at/certs/a-sign premium timestamp-nnx.crt

zu finden (die Bedeutung von -nnx ist in Abschnitt 2.6.2 beschrieben) und kann von hier heruntergeladen werden.

2.6.4 Widerrufsinformationen

Verteilungspunkt für die Widerrufslisten (CRLs) ab der CA-Version 02:

- ldap://ldap.a-trust.at/ou=a-sign premium timestamp-nn,o=A-Trust,c=AT?certificaterevocationlist?base?objectclass=eidcertificationauthority

Sichere Abfrage der CRL über https:

- http://crl.a-trust.at/crl/a-sign premium timestamp-nn

2.6.5 Suche nach einem Zertifikat

Für die Suche nach einem bestimmten Zertifikat (Suchkriterien sind wahlweise CIN oder Seriennummer) und den Download eines gefundenen Zertifikats steht auf der A-Trust Homepage ein Formular zur Verfügung. Sichere Abfrage eines Zertifikats über https:

- https://www.a-trust.at/directory

2.6.6 Veröffentlichung von Informationen der Zertifizierungsstelle

Die Zertifizierungsstelle veröffentlicht:

- die jeweils gültige Zertifizierungsrichtlinie,
- die jeweils gültige Anwendungsvorgabe (Certificate Policy),
- die gültige Entgeltregelung,
- die Ergebnisse der Audits durch die Aufsichtsbehörden,
- interne Auditinformationen, sofern die Sicherheit von A-Trust nicht gefährdet ist,
- das Zertifikat der Zertifizierungsstelle,
- die Allgemeinen Geschäftsbedingungen [AGB],
- die Unterrichtung für den Zeitstempelauslöser,
- die Information über die zu verwendenden Komponenten und Verfahren,
- eine Liste mit Kontaktstellen bzw. Registrierungsstellen,
- auf ihrer Homepage www.a-trust.at.

Diese Informationen werden hochverfügbar gehalten. Ausfallzeiten, die durch Systemfehler anfallen, werden so gering wie möglich gehalten.

Die Zeitstempelauslöser werden zusätzlich informiert über:

- Widerruf des Schlüssels der Zertifizierungsstelle,
- Kompromittierung oder Verdacht auf Kompromittierung des Schlüssels der Zertifizierungsstelle,
- längeren Ausfallzeiten von Diensten (z.B. nach einem Katastrophenfall in der Zertifizierungsstelle),

- wesentliche Änderungen der Zertifizierungsrichtlinie vor der Zertifikatserneuerung und
- Einstellung der Tätigkeit der Zertifizierungsstelle.

A-Trust stellt alle Informationen wie folgt bereit:

- Auf der Web-Seite www.a-trust.at
- Optional: in einem elektronischen Newsletter per E-Mail
- Optional: Briefsendung
- Optional: Printmedien oder TV

Informationen, die nur einzelne Zeitstempelauslöser betreffen, werden diesen direkt zugestellt. Ist eine Vielzahl von Zeitstempelauslöser betroffen, wird eine der o.a. Alternativen ausgewählt. Insbesondere im Notfall bieten sich die Printmedien oder TV zur schnellen Bekanntgabe z.B. einer Kompromittierung eines CA-Schlüssels an.

2.6.7 Frequenz der Aktualisierung

Eine Aktualisierung der Zertifizierungsrichtlinie erfolgt gemäß Kapitel 9.

2.6.8 Zugriffskontrollen

Zugriffskontrollen stellen sicher, dass die Anwender nur lesenden Zugriff auf die Veröffentlichungen von A-Trust haben. Nur autorisierte Mitarbeiter von A-Trust haben die Möglichkeit, Änderungen an den Dokumenten und die Administration der Verzeichnisse für Zertifikate sowie der Widerrufslisten vorzunehmen.

2.6.9 Verzeichnisse

Folgende Verzeichnisse werden von der Zertifizierungsstelle unterhalten:

- Ein öffentlich zugängliches Verzeichnis; es enthält die Zertifikate der Zertifizierungsstellen, die Widerrufslisten und die Zertifikate der Zeitstempelauslöser.
- Eine öffentliche Web-Seite, auf der diese Zertifizierungsrichtlinien abrufbar sind und weitere allgemeine Informationen den Anwendern zugänglich sind.

2.7 Interne Prüfung (Audit)

2.7.1 Häufigkeit des Audits

Das erstmalige Audit zur Akkreditierung der Zertifizierungsstelle erfolgt im Auftrag der Aufsichtsbehörde bei Aufnahme des Betriebs. Danach werden Audits in regelmäßigen Abständen im Auftrag der Aufsichtsbehörde durchgeführt. Darüber hinaus werden jährlich interne, von A-Trust in Auftrag gegebene, Revisionen und Audits durchgeführt. Audits werden stichprobenhaft in allen A-Trust Liegenschaften und Registrierungsstellen durchgeführt.

2.7.2 Identität bzw. Anforderungen an den Auditor

Die Aufsichtsbehörde bestimmt den Auditor für die in ihrem Auftrag durchzuführenden Audits. Interne Audits, die von A-Trust im Rahmen ihrer Qualitätssicherung beauftragt werden, werden im Rahmen der Revision durchgeführt.

2.7.3 Beziehungen zwischen Auditor und zu untersuchender Partei

Die Aufsichtsbehörde bestimmt den Auditor, der in ihrem Auftrag die Überprüfung vornimmt. Von A-Trust beauftragte Audits werden von Personen, welche über die notwendige Qualifikation verfügen, durchgeführt.

2.7.4 Aspekte des Audits

Der Auditor überprüft, ob die Zertifizierungsstelle gemäß der Angaben in der Zertifizierungsrichtlinie und dem Sicherheits- und Zertifizierungskonzept arbeitet. Dies gilt ebenfalls für die zu untersuchenden Liegenschaften. Der Auditor versichert sich des sachgemäßen Einsatzes und der Angemessenheit der kryptografischen Komponenten.

2.7.5 Handlungen nach unzureichendem Ergebnis

Das Audit kann mit einem unzureichenden Ergebnis abgeschlossen werden, das die folgenden Konsequenzen nach sich zieht:

- Widerruf des entsprechenden Zertifikats bzw. Einstellung des Betriebs der überprüften Einheit der Zertifizierungsinfrastruktur,
- der überprüften Einheit der Zertifizierungsinfrastruktur wird eine Frist zur Beseitigung der Schwachstellen eingeräumt.

2.7.6 Bekanntgabe der Ergebnisse

Die Aufsichtsbehörde veröffentlicht die Informationen aus dem Audit. Darüber hinaus wird die A-Trust zusätzliche Informationen – sofern dadurch nicht die Sicherheit gefährdet wird – bereitstellen.

2.8 Vertraulichkeit

2.8.1 Vertraulich eingestufte Informationen

A-Trust verpflichtet sich, die vom Zeitstempelauslöser bekannt gegebenen Daten vertraulich im Sinne des Datenschutzgesetzes bzw. der DSGVO zu behandeln. Die Daten, die bei der Anmeldung angegeben werden, werden ausschließlich für die Dienstleistungen der Zertifizierungsstelle benutzt.

Als vertrauliche Daten werden alle nicht veröffentlichten Zertifikate sowie alle persönlichen Daten angesehen, die nicht Bestandteil des Zertifikats sind.

2.8.2 Nicht vertraulich eingestufte Informationen

Als nicht vertrauliche Daten werden die Informationen in den ausgestellten und veröffentlichten Zertifikaten sowie die Widerrufslisten angesehen.

2.8.3 Offenlegung von Informationen zu Zertifikatswiderruf

Gründe, die zur Aussetzung oder zu einem Widerruf führen, werden im Verzeichnisdienst veröffentlicht.

2.8.4 Offenbarung an Behörden im Rahmen gesetzlicher Pflichten

A-Trust gibt die persönlichen Daten des Zeitstempelauslösers nur auf Verlangen an laut [SVG] berechtigte Gerichte bzw. andere Behörden weiter (gemäß Artikel 24 (2) Lit. h [eIDAS-VO] iVm § 10 [SVG]).

2.8.5 Offenbarung im Rahmen zivilrechtlicher Auskunftspflichten

Wird wie in Abschnitt 2.8.4 behandelt.

2.8.6 Weitere Gründe zur Freigabe von vertraulichen Informationen

Wird wie in Abschnitt 2.8.4 behandelt.

2.9 Urheberrechte und Eigentumsrechte

Die Urheber- und Eigentumsrechte an den folgenden Dokumenten liegen bei A-Trust:

- Sicherheits- und Zertifizierungskonzept
- Zertifizierungsrichtlinie
- Anwendungsvorgabe (Certificate Policy)
- Liste der empfohlenen Komponenten und Verfahren zur Erstellung und Prüfung sicherer elektronischer Signaturen

Die Urheber- und Eigentumsrechte an den folgenden Schlüsseln liegen bei A-Trust:

- Private Schlüssel des Zertifizierungsdiensteanbieters und
- Öffentliche Schlüssel des Zertifizierungsdiensteanbieters.

3 Identifizierung und Authentifikation

Keine Bestimmungen.

4 Betriebliche Anforderungen

4.1 Antrag auf Ausstellung von Zertifikaten

Keine Bestimmungen.

4.2 Ausstellung von Zertifikaten

Keine Bestimmungen.

4.3 Akzeptanz von Zertifikaten

Keine Bestimmungen.

4.4 Aussetzung und Widerrufung von Zertifikaten

Zeitstempel 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. Der Zeitstempelauslöser wird von einer erfolgten Aussetzung oder einem Widerruf informiert, sofern Kontaktdaten angegeben wurden.

4.4.1 Gründe für einen Widerruf

Der Widerruf eines Zeitstempel Zertifikats wird erforderlich, wenn

- Angaben im Zertifikat nicht mehr korrekt sind,
- Verdacht auf eine Kompromittierung besteht bzw. eine Kompromittierung vorliegt,
- die Frist einer Aufhebung einer Aussetzung abläuft,
- die eingesetzten Algorithmen nicht mehr den Sicherheitserwartungen entsprechen und dadurch eine sichere Anwendung der Zeitstempelerstellungsdaten nicht mehr gegeben wäre.
- sonstige im Zertifikat bescheinigter Umstände nicht mehr zutreffen

4.4.2 Wer kann einen Widerruf anordnen

Nur der Zertifikatsinhaber kann einen Widerruf anordnen.

4.4.3 Prozedur für einen Widerrufsantrag

Keine Bestimmungen.

4.4.4 Frist bis zur Bekanntgabe des Widerrufs

Die Aktualisierung der Widerrufsliste erfolgt zumindest alle zwei Stunden. Der Widerrufsdienst ist rund um die Uhr erreichbar.

4.4.5 Gründe für eine Aussetzung

Die Aussetzung ist eine temporäre Aufhebung der Zertifikatsgültigkeit. Sie kann bei Verdacht des Eintritts eines der unter Kapitel 4.4.1 genannten Gründe genutzt werden. Im Gegensatz zu einem Widerruf kann eine Aussetzung innerhalb einer festgelegten Frist auch wieder aufgehoben werden. Nach spätestens zehn Tagen wird eine Aussetzung durch die Zertifizierungsstelle in einen Widerruf umgewandelt.

4.4.6 Wer kann eine Aussetzung anordnen und aufheben

Nur der Zertifikatsinhaber kann einen Widerruf anordnen.

4.4.7 Prozedur für einen Aussetzungsantrag

Keine Bestimmungen.

4.4.8 Aufhebung der Aussetzung

Keine Bestimmungen.

4.4.9 Bekanntgabe der Aussetzung bzw. Aufhebung

Die Aussetzung wird in der Widerrufsliste eingetragen, bei einer Aussetzungsaufhebung ist die betreffende Aussetzung in der nächsten Widerrufsliste, die nach der Aufhebung ausgestellt wird, nicht mehr enthalten.

4.4.10 Grenzen einer Aussetzungsperiode

Keine Bestimmungen.

4.4.11 Aktualisierungsintervalle der Widerrufsliste

Die Intervalle der Aktualisierung der Widerrufsliste sind über die A-Trust Web-Seite in Erfahrung zu bringen.

4.4.12 Anforderungen an die Überprüfung mittels Widerrufslisten

Das Überprüfen der Gültigkeit von Zeitstempel liegt in der Verantwortung der Nutzer. Der Inhalt eines Zeitstempels kann nur dann als authentisch gelten, wenn sich der Nutzer von der Gültigkeit des Zertifikats überzeugt hat.

Für eine positive Gültigkeitsüberprüfung ist es erforderlich, dass

- der Zeitpunkt der Ausstellung im Gültigkeitszeitraum des Ausstellerzertifikats liegt,
- das Zertifikat mit einem gültigen Zertifikat der Zertifizierungsstelle signiert wurde
- sich das Zertifikat nicht in der aktuellen Widerrufsliste befindet.

Ein Zertifikatsnutzer sollte die Authentizität einer Widerrufsliste durch die Prüfung der in der Widerrufsliste enthaltenen Signatur verifizieren.

Ausgehend von der Signatur der Widerrufsliste ist der vollständige Zertifizierungspfad auf Gültigkeit zu prüfen. Die von dem Nutzer lokal gespeicherten Zertifikate sollten vor ihrer Nutzung gegen eine aktuelle Widerrufsliste geprüft werden. Sofern keine erfolgreiche Gültigkeitsprüfung vorgenommen werden kann (beispielsweise aus Internet-Verbindungsprobleme), sollten keine Zertifikate akzeptiert werden. Jede Akzeptanz eines solchen Zertifikats erfolgt auf das Risiko des Zertifikatsnutzers.

4.4.13 Weitere Möglichkeiten zur online Statusabfrage

Es wird ein OCSP-Dienst über das Internet angeboten.

4.4.14 Anforderungen an die online Statusabfrage

Ein Zertifikatsnutzer sollte die Authentizität der Auskunft des Verzeichnisdiensts durch die Prüfung der in der Antwort enthaltenen Signatur verifizieren. Des weiteren ist der in der Auskunft enthaltene Zeitpunkt, auf den sich der Status bezieht, mit dem fraglichen Prüfzeitpunkt zu vergleichen.

Sofern keine erfolgreiche Gültigkeitsprüfung vorgenommen werden kann (beispielsweise aus technischen Gründen), sollte das Zertifikat nicht akzeptiert werden. Jede Akzeptanz eines solchen Zertifikats erfolgt auf Risiko des Zertifikatsnutzers.

4.4.15 Weitere Verfahren zur Bekanntgabe von Widerrufen

Keine Bestimmungen.

4.4.16 Anforderungen an die Überprüfung der weiteren Verfahren zur Bekanntgabe von Widerrufen

Keine Bestimmungen.

4.4.17 Spezielle Verfahren bei Kompromittierung von privaten Schlüsseln

Keine Bestimmungen

4.5 Protokollierung sicherheitsrelevanter Ereignisse

4.5.1 Protokollierte Ereignisse

Zur Protokollierung von Ereignissen werden Datum und Uhrzeit sowie gegebenenfalls der Verantwortliche festgehalten. Dies betrifft:

- Ab- und Anschalten von Systemen,
- Änderungen der Hardwarekonfiguration,
- Einrichtung oder Schließung von Accounts,
- Änderungen bei der Rollenaufteilung,
- Änderung der Softwarekonfiguration (Installation oder Update von Software), Weiterhin werden alle mit den Systemen durchgeführten Transaktionen zusammen mit Transaktionstyp, Zeitpunkt und Informationen darüber, ob die Transaktion abgeschlossen oder abgebrochen wurde und wer die Transaktion veranlasst hat, protokolliert. Folgende Transaktionstypen sind insbesondere aufzuzeichnen:

- Zertifizierungsanträge,
- Schlüsselerzeugungen,
- Zertifikatserstellungen,
- Veröffentlichung von Zertifikaten und Widerrufslisten,
- Aussetzungs- und Widerrufanträge,

- Ausgeführte Aussetzungen und Widerrufe sowie
- Schlüsselwechsel.
- Der exakte Zeitpunkt des Auftretens einer Schaltsekunde
- Zeitliche Abweichungen der gesetzten Parameter

Aus den einzelnen Ablaufprozessen ergeben sich zusätzliche Ereignisse, die an der entsprechenden Stelle protokolliert werden. Dies betrifft:

- Bestätigung der Unterrichtung gem. Art. 24 (2) lit d [eIDAS-VO],
- das Einverständnis des Zeitstempelauslösers mit den Allgemeinen Geschäftsbedingungen und den Entgeltbestimmungen
- Änderungen an bescheinigten Umständen.

4.5.2 Intervalle der Überprüfung der Protokolldateien

Die Protokolle, die im laufenden Rechenzentrumsbetrieb erzeugt werden, sind regelmäßig (routinemäßig einmal pro Woche) vom Rechenzentrumspersonal auf verdächtige Vorkommnisse zu untersuchen.

Es werden die Protokolle, die sich aus den einzelnen Ablaufprozessen ergeben und die für die Sicherheit der Dienstleistungen von A-Trust relevant sind, im Zuge der Revision auf verdächtige Vorkommnisse und Manipulationen untersucht.

4.5.3 Aufbewahrungszeitraum der Protokolldateien

Sicherheitsrelevante Protokolldateien werden 30 Jahre nach Ablauf des Zertifikats aufbewahrt. Protokolldateien, die benötigt werden, um nachträglich Aussagen über die Gültigkeit von Zertifikaten zu treffen, werden archiviert. Dies gilt besonders für Daten zur Veröffentlichung von Zertifikaten und Widerrufslisten sowie Eingang und Bearbeitung von Widerrufsanträgen. Der Zeitraum der Aufbewahrung von archivierten Protokolldateien ist in Abschnitt 4.6.2 festgelegt.

4.5.4 Schutz der Protokolldateien

Die Protokolldateien werden an unterschiedlichen Standorten erstellt und im Rechenzentrum elektronisch aufbewahrt. Sie sind nur autorisiertem Personal zugänglich zu machen. Die Protokolldateien werden mittels digitaler Signatur vor Modifikationen geschützt.

4.5.5 Protokollierungssystem (intern / extern)

Die Protokollierung findet intern durch die Systeme an den Standorten statt.

4.5.6 Benachrichtigung beim Auftreten sicherheitskritischer Ereignisse

Bei einem Verdacht auf das Eintreten eines sicherheitskritischen Ereignisses entscheidet A-Trust über eine Benachrichtigung von betroffenen Anwendern.

4.5.7 Bewertungen zur Angreifbarkeit

Keine Bestimmungen.

4.6 Archivierung

4.6.1 Archivierte Daten

Archiviert werden:

- Zeitstempelantworten
- Zertifizierungsanträge (Antragstellerformular und Vertrag),
- alle von der Zertifizierungsstelle ausgestellten Zertifikate (Zertifikate der Zertifizierungsstelle und Dienste und Zertifikate der Signatoren),
- Aussetzungs- und Widerrufanträge mit Datum und Uhrzeit des Eintreffens (inklusive entsprechender Protokolldateien),
- alle ausgestellten Widerrufslisten,
- Datum und Uhrzeit der Veröffentlichung der Zertifikate und Widerrufslisten (inklusive entsprechender Protokolldateien) und
- Datum und Uhrzeit von Schlüsselwechseln der Zertifizierungsstelle.

Zusätzlich werden die Anträge auf Ausstellung des Zertifikats und die Registrierungsunterlagen für den in Abschnitt 4.6.2 genannten Zeitraum aufbewahrt.

4.6.2 Aufbewahrungszeiten

Die Aufbewahrungszeiten richten sich nach dem [SVG] und betragen 30 Jahre nach Ablauf des Zertifikats. Für die einzelnen Aufbewahrungszeiten sind folgende Aspekte zu berücksichtigen:

- Die Daten müssen mindestens so lange aufbewahrt werden, wie sie im Anwendungszeitraum benötigt werden.
- Zu berücksichtigen ist auch die technische Kompatibilität. Dies gilt insbesondere für Soft- und Hardware, deren Veränderung eine Nachprüfung von Dokumenten nicht mehr möglich macht. Zu diesem Zweck werden ausschließlich technische Formate verwendet, deren zugrunde liegende Spezifikationen öffentlich verfügbar sind.

4.6.3 Schutzvorkehrungen

Das Archiv befindet sich in gesicherten Räumlichkeiten. Der Zugriff ist nur autorisierten Personen gestattet. Die archivierten Protokolldateien sind entsprechend den Richtlinien aus Abschnitt 4.5.4 geschützt.

Elektronische Dokumente sind durch digitale Signaturen vor Modifikationen geschützt.

Systemzugriff auf das Archiv, zu Administrationszwecken, ist ausschließlich im "4-Augen Prinzip" autorisierter Personen möglich.

4.6.4 Anforderungen, die Daten mit Echtzeitangaben zu versehen

Alle Zertifikatsanträge sind mit einer Echtzeitangabe versehen. Dies betrifft insbesondere die Aussetzungs- und Widerrufsanträge sowie die Ausstellung der Widerrufslisten.

4.6.5 System zur Erfassung der Archivierungsdaten (intern / extern)

Das System für das Zertifikatsmanagement ist für die Archivierung aller zu archivierenden Daten verantwortlich. Ausgenommen davon sind die Originalunterlagen, welche in der Registrierungsstelle aufgehoben werden.

4.6.6 Prozeduren zum Abrufen und Überprüfen von Daten

Bei Archivierung von elektronischen Daten über lange Zeiträume ist damit zu rechnen, dass veraltete Datenformate nicht mehr von neuen Systemen unterstützt werden. Die Zertifizierungsstelle hält deshalb auch die Systeme verfügbar, mit denen sich diese Daten auch über den Archivierungszeitraum verarbeiten lassen.

Es werden Regelungen getroffen, dass das Archiv bei Einstellung der Tätigkeit der Zertifizierungsstelle über den festgelegten Archivierungszeitraum bestehen bleibt.

Als Format für die Archivierung werden Formate gewählt, deren Lesbarkeit über die Archivierungsperiode gesichert ist. Text und XML für Logdateien. TIFF/JPG für Bild-Dateien. Zertifikate und Widerrufslisten in DER Kodierung.

4.7 Schlüsselwechsel von CA- und Root-Schlüssel

Ein Schlüsselwechsel erfolgt im Zusammenhang mit dem Ausfall eines Hardware Security Moduls oder wenn die verwendeten Schlüssellängen bzw. Algorithmen nicht mehr den Sicherheitsanforderungen entsprechen sollten oder aber im Falle einer nicht vorhersehbaren Kompromittierung von Schlüsseln. In letzterem Fall ist unbedingt ein Widerruf der betroffenen Zertifikate erforderlich. Die Gründe für den Widerruf von Root- und CA-Zertifikaten sind in Kapitel 4.8.2 aufgelistet. Die Zertifizierungsstellen erneuern außerdem regelmäßig ihre Zertifikate. Dies sollte vor dem Ablauf der im Zertifikat festgelegten Gültigkeitsdauer geschehen. Rechtzeitig vor der Erneuerung wird dies auf der Web-Seite (siehe Abschnitt 2.6.6) angekündigt. Die Gültigkeitsdauer der Zertifikate ist Kapitel 6.3 zu entnehmen.

Der Überprüfer eines Zertifikats erhält das neue Zertifikat über den Verzeichnisdienst. Er kann über die Zertifizierungskette die Gültigkeit des Zertifikats überprüfen.

Um sich von der Authentizität des Zertifikats der Root-CA zu überzeugen hat der Zeitstempelauslöser die Möglichkeit der Abfrage auf der A-Trust Homepage veröffentlichten Fingerprints des öffentlichen Schlüssels.

Mit einem Schlüsselwechsel verliert der alte Schlüssel seine aktive Gültigkeit. D.h. der private Schlüssel wird nicht weiter für die Zertifizierung eingesetzt. Ab diesem Zeitpunkt wird nur noch der neue Schlüssel für das Signieren von Zertifikaten verwendet. Das Zertifikat zu dem alten Schlüssel wird nur, falls erforderlich, widerrufen (Kompromittierung). Wurde der alte Schlüssel nicht widerrufen, kann er bis zum Ablauf der im Zertifikat festgelegten Gültigkeitsdauer zum Nachprüfen von Zertifikaten eingesetzt werden.

Sofern bestehende technische Standards unverändert sind, d.h. der eingesetzte Algorithmus den Sicherheitserwartungen entspricht und auch gesetzliche Vorgaben unverändert sind, wird kein neuer Schlüssel generiert, sondern die Gültigkeitsdauer des Zertifikats in regelmäßigen Abständen erneuert.

Hinsichtlich der Generierung und Aufbewahrung im Hardware Security Modul gibt es keinen Unterschied zwischen dem CA-Schlüssel (Zertifizierungsschlüssel für Zertifikate der Zeitstempelauslöser) und dem Root-CA-Schlüssel (Zertifizierungsschlüssel für Zertifikate der Zertifizierungsstellen).

4.8 Kompromittierung und Notfallplan

4.8.1 Rechner, Software und/oder Daten sind korrumpiert

Regelungen bei Kompromittierung bzw. Verdacht auf Kompromittierung von Schlüsseln sind in Abschnitt 4.8.3 aufgeführt.

Werden innerhalb des Systems fehlerhafte oder manipulierte Rechner, Software oder Daten entdeckt, die Auswirkungen auf die Sicherheit des Systems und dessen Dienste

haben könnten, so werden die entsprechenden Komponenten umgehend aus dem Betrieb genommen.

Bei Zertifikaten sind die betroffenen Zeitstempelauslöser zu informieren. Es erfolgt ein unmittelbarer Widerruf der betroffenen Zertifikate, falls die fehlerhaften Angaben im Zertifikat sind.

Bei Fehlern in einer Widerrufsliste wird umgehend eine korrekte Widerrufsliste ausgestellt. Falls eine sichere, unmittelbare Ausstellung der Widerrufsliste nicht möglich ist und die Fehler sicherheitskritisch sind, werden die Verzeichnisdienste abgeschaltet, die die Widerrufsliste veröffentlichen, um die Publikation unkorrekter Daten zu verhindern. Die Wiederaufnahme des Dienstes ist mit der Veröffentlichung der neuen Widerrufsliste verbunden. In Abhängigkeit der Fehler und der Ausfallzeit der Verzeichnisdienste werden die Anwender informiert.

Sobald die festgestellten Mängel beseitigt sind, werden die eventuell abgeschalteten Komponenten wieder in Betrieb genommen.

4.8.2 Widerruf von Zertifikaten zu Zertifizierungsstellen- und Dienste-Schlüsseln

Zertifikate der Zertifizierungsstelle werden in den folgenden Fällen widerrufen:

- bei Kompromittierung oder Verdacht auf Kompromittierung der entsprechenden Schlüssel,
- wenn die eingesetzten Algorithmen nicht mehr den Sicherheitsanforderungen entsprechen, so dass eine sichere Anwendung nicht gewährleistet werden kann oder
- bei Einstellung der Tätigkeit der Zertifizierungsstelle, wobei die Widerrufsliste oder Dienste zur Statusauskunft nicht weiter gepflegt werden.
- bei Einstellung des jeweiligen Dienstes

Ist der Grund für den Widerruf des Zertifikats Kompromittierung oder der Verdacht auf Kompromittierung des zugehörigen privaten Schlüssels, dann ist insbesondere Abschnitt 4.8.3 zu berücksichtigen. Bei Widerruf des Zertifikats wegen Einstellung der Tätigkeit der Zertifizierungsstelle ist Abschnitt 4.9 zu beachten.

Ist ein Widerruf geplant, so werden die Zeitstempelauslöser rechtzeitig über den bevorstehenden Widerruf informiert. Ein ungeplanter Widerruf erfordert eine umgehende Benachrichtigung der Zeitstempelauslöser. Die Information wird über die Web-Seite bereitgestellt.

Private Schlüssel der Zertifizierungsstelle, deren zugehörige Zertifikate widerrufen wurden, werden nicht weiter durch die Zertifizierungsstelle eingesetzt. Diese privaten Schlüssel werden gelöscht.

4.8.3 Widerruf von Zertifikaten der Dienste

Werden Zertifikate der Dienste der Zertifizierungsstelle (das sind Verzeichnis- und Widerrufsdienst) widerrufen, so werden die Dienste ohne gültigen Schlüssel (CA-Schlüssel zur Signatur von Zertifikaten und CRLs) umgehend aus dem Betrieb genommen. Dadurch wird verhindert, dass die Anwender Dienste nutzen, deren Schlüssel ungültig sind. Die widerrufenen Schlüssel werden durch neue Schlüssel ersetzt. Die Dienste werden erst wieder in Betrieb genommen, wenn die neuen, gültigen Schlüssel installiert wurden.

4.8.4 Widerruf des Zertifikats der Zertifizierungsstelle

Wird ein Zertifikat der Zertifizierungsstelle widerrufen, so müssen dadurch alle unter diesem Zertifikat ausgestellten Zertifikate widerrufen werden. Der Dienst der Statusauskunft wird bei Anfragen zu allen unter der Zertifizierungsstelle bzw. unter deren Untereinheiten ausgestellten Zertifikaten generell mit einem ungültigen Status antworten.

4.8.5 Schlüsselwechsel

Nach dem Widerruf des Zertifikats wird auch der dazugehörige private Schlüssel nicht weiter eingesetzt. Um aber die Zertifizierungsdienstleistungen und Dienste weiter aufrecht zu erhalten, muss die Zertifizierungsstelle einen neuen Schlüssel einsetzen. Verfügt die Zertifizierungsstelle aufgrund eines durchgeführten Schlüsselwechsels bereits über einen solchen neuen Schlüssel, so kann dieser eingesetzt werden. Dies ist aber nur unter der Bedingung möglich, dass der Schlüssel auch weiterhin gültig ist. Sollte dies nicht mehr der Fall sein, so wird ein Schlüsselwechsel nach den Richtlinien aus Abschnitt 4.7 durchgeführt, die sich aber in folgenden Punkten von einem regulären Wechsel unterscheidet:

- Eine rechtzeitige Information der Zeitstempelauslöser über den Schlüsselwechsel ist bei einem unmittelbaren Widerruf nicht möglich. Die Zeitstempelauslöser werden im Zusammenhang mit der Widerrufsinformation auch umgehend über den Schlüsselwechsel informiert.
- Es findet keine Zertifizierung anderer Schlüssel der Zertifizierungsstelle mit dem ungültigen Zertifikat statt. Die Zeitstempelauslöser können die Authentizität der Zertifikate mittels anderer Verfahren überprüfen. Zusätzlich werden bei der Auslieferung neuer Schlüssel auch aktuelle Zertifikate der Zertifizierungsstelle ausgeliefert, mit denen die Authentizität der Zertifikate überprüft werden kann.
- Widerrufene Schlüssel sind ungültig und werden nicht weiter eingesetzt.

4.8.6 Schlüsselkompromittierung bzw. Verdacht auf Schlüsselkompromittierung

Wird in der Zertifizierungsstelle eine Kompromittierung von Schlüsseln der Zertifizierungsstelle bekannt oder besteht ein begründeter Verdacht auf eine Kompromittierung, so wird umgehend der Sicherheitsbeauftragte der Zertifizierungsstelle informiert. Dieser ordnet gegebenenfalls einen Widerruf betroffener Zertifikate an. Wichtige Maßnahmen dazu sind:

- Die Anwender werden umgehend informiert.
- Gegebenenfalls erfolgt das Abschalten des Verzeichnisdiensts und die Einstellungen der Statusauskünfte, um falsche oder ungültige Aussagen durch diese Dienste zu verhindern.
- Verteilung neuer, gültiger Zertifikate und gegebenenfalls neuer Schlüssel an die Anwender.

Der Sicherheitsbeauftragte muss bei jeder festgestellten Kompromittierung oder einem Verdacht darauf genau prüfen, ob davon weitere Schlüssel betroffen sein können und ob die Schlüssel noch als sicher angesehen werden können.

4.8.7 Zeitstempelkompromittierung

Wird eine Kompromittierung des Zeitstempels bekannt oder besteht ein begründeter Verdacht auf eine Kompromittierung, wird umgehend die Aufsichtsstelle informiert.

4.8.8 Sicherheitsvorkehrungen nach Katastrophen

Der Sicherheitsbeauftragte entscheidet, ob durch die Katastrophe eine Gefahr für die Sicherheit der Dienstleistungen besteht und veranlasst gegebenenfalls die notwendigen Aktionen. Wenn, bedingt durch die Auswirkungen der Katastrophe, übliche Verfahren wie Widerruf oder das Anbieten von Informationen über E-Mail oder Web-Seite nicht möglich sind, dann werden verstärkt alternative Verfahren wie der Postweg zur Verbreitung der notwendigen Informationen eingesetzt.

Ist die Sicherheit der Lokalität der Zertifizierungsstelle gefährdet, so werden umgehend Medien, auf denen sich sicherheitskritische Informationen befinden, in eine sichere Umgebung gebracht. Gleiches gilt für Datenträger mit wichtigen Informationen und archivierten Daten. Zusätzlich wird versucht, die Lokalität so weit wie möglich vor dem Zugang Unbefugter zu schützen.

4.9 Einstellung der Tätigkeit der Zertifizierungsstelle

Einstellung der Tätigkeit bedeutet, dass die kompletten Dienstleistungen der Zertifizierungsstelle nicht weiter angeboten werden. Organisatorische Umstellungen oder Wechsel der Schlüssel der Zertifizierungsstelle sind hiervon nicht betroffen.

Die Einstellung der Tätigkeit wird mindestens drei Monate zuvor allen betroffenen Einheiten und Personenkreisen mitgeteilt. Dies gilt insbesondere für die Benachrichtigung der Aufsichtsstelle . Rechtzeitig vor der endgültigen Einstellung der Zertifizierungsstelle werden alle noch gültigen und von der Zertifizierungsstelle ausgestellten Zertifikate widerrufen. Alle von den Widerrufen betroffenen Zertifikatsinhaber werden vom Widerruf ihres Zertifikates informiert.

Alle relevanten Daten der betroffenen Zertifizierungsstelle (Zertifikate, CRLs etc.) werden gesichert. Das Archiv und der Zugriff darauf werden für die festgelegte Archivierungsperiode weiter verfügbar gehalten.

A-Trust trägt dafür Sorge, dass die CRLs der eingestellten Zertifizierungsstelle auch nach der Beendigung den Benutzern öffentlich und authentisch zur Verfügung stehen. Eine darüber hinausgehende Übertragung der Verpflichtung an Drittparteien ist nicht notwendig.

5 Physische, verfahrensorientierte und personelle Sicherheitsvorkehrungen

5.1 Physische Sicherheitsvorkehrungen

5.1.1 Standort und örtliche Gegebenheiten

Die Dienstleistungen der A-Trust werden in den folgenden Örtlichkeiten vorgenommen:

Dienstleistung	**Adresse**
Firmensitz	A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH. Landstraßer Hauptstraße 1b A-1030 Wien
Widerrufsdienst	Den Widerrufsdienst finden Sie auf der Web-Seite der A-Trust https://www.a-trust.at/ veröffentlicht.
Zertifizierung, Brief-Versand (Antragstellerformular, Aussetzungs- und Widerrufsinformation, PUKs, etc.)	Nessus GmbH Fernkorngasse 10 A-1010 Wien Ausfallrechenzentrum: Nessus GmbH Karmarschgasse 23-25 A-1010 Wien

Tabelle 3: Örtlichkeiten

5.1.2 Zugangskontrollen

Der Zugang zu allen technischen Komponenten im Rechenzentrum ist nur durch einen von der A-Trust eingerichteten Berechtigungsmechanismus möglich. Die Zugangskontrollen sind dem angestrebten Sicherheitsniveau für einzelne Bereiche, in denen sich sicherheitskritische Komponenten befinden, angepasst. Der Zutritt in den Hochsicherheitsbereich des Rechenzentrums ist an die Anwesenheit von zwei Personen mit Berechtigungskarten und PIN-Eingabe gebunden. Diese Zutritte werden protokolliert und sind dadurch jederzeit nachvollziehbar. Zusätzlich sind Videoüberwachungssysteme und Einbruchmeldesysteme installiert.

5.1.3 Stromversorgung und Klimaanlage

Die Stromversorgung in den Örtlichkeiten entspricht internationalen Standards und ist - bis auf die Registrierungsstellen überall redundant ausgelegt. Zusätzlich existiert für das Rechenzentrum eine Notstromversorgung.

Die Örtlichkeiten, in denen technische Komponenten der A-Trust untergebracht sind, verfügen alle über eine angemessene Klimaanlage.

5.1.4 Wasserschäden

Die Örtlichkeiten, in denen technische Komponenten der A-Trust untergebracht sind, verfügen alle über einen angemessenen Schutz vor Wasserschäden.

5.1.5 Feuer

Alle Räumlichkeiten, die technische Komponenten beherbergen, verfügen über eine EDV-geeignete Feuermeldeanlage.

Im Hochsicherheitsbereich des Rechenzentrums richtet sich der Brandschutz nach den dort geltenden Richtlinien für den Hochsicherheitsbetrieb.

5.1.6 Datenträger

Als Datenträger werden folgende Medien eingesetzt:

- Papier
- Festplatten
- DVDs
- WORMs

Datenträger mit sensiblen oder sicherheitskritischen Daten werden zugriffsgeschützt in abgeschlossenen Räumen oder Tresoren aufbewahrt.

5.1.7 Müllentsorgung

Die Daten auf den elektronischen Datenträgern werden sachgemäß vernichtet und die Datenträger dann einem spezialisierten Unternehmen zur sachgerechten Entsorgung übergeben. Papierdatenträger werden in vorhandenen Aktenvernichtern entsorgt oder einem spezialisierten Unternehmen zur sachgemäßen Entsorgung übergeben.

5.1.8 Redundante Auslegung

Der gesamte Betrieb im Rechenzentrum ist, soweit technisch möglich, redundant ausgelegt, so dass eine Hochverfügbarkeit (7 x 24 Stunden) des Rechenzentrumsbetriebs erreicht werden kann.

5.2 Verfahrensorientierte Sicherheitsvorkehrungen

In diesem Kapitel werden die bei A-Trust und den Liegenschaften notwendigen Rollen definiert. Die Aufgaben der Rollen werden kurz beschrieben, die Rollen werden nach ihrer sicherheitstechnischen Relevanz eingeordnet.

5.2.1 Funktionen der A-Trust

Rolle	Funktion
Geschäftsführung	Kommerzieller Erfolg des Unternehmens Marketing und Vertrieb Betrieb Schnittstelle zur Aufsichtsbehörde
Vertrieb und Marketing	Vertriebskonzepte und deren Umsetzung
Projektmanagement	Beratung und Durchführung von Kundenprojekten im Zusammenhang mit A-Trust Produkten
Betriebsleitung	störungsfreier Betrieb gemäß Sicherheits- und Zertifizierungskonzept und Betriebskonzept
Produktmarketing	Konzeption marktgerechter Produkte/Produktfamilien
Sicherheitsbeauftragter	Definition und Einhaltung der Sicherheitsbestimmungen Sicherheitsüberprüfung des Personals
Revision	Durchführung der betriebsinternen Audits Darf keine andere Funktion aus dem sicherheitskritischen Bereich durchführen, außer wenn es für die Revision erforderlich ist.
Datenschutz	Überwachung und Einhaltung der Datenschutzbestimmungen
Schulung	Durchführung, Konzeption und Überwachung der Schulungen laut Sicherheits- und Zertifizierungskonzept

Tabelle 4: Funktionen der A-Trust

5.2.2 Sicherheitskritische Funktionen

Rolle	Funktion
Sicherheitsbeauftragter	siehe Tabelle 4
Revision	siehe Tabelle 4
Datenschutz	siehe Tabelle 4
Security Officer (SO)	Zutritt in die Hochsicherheitszone Verantwortlichkeit für die Generierung und Zertifizierung der Schlüssel von A-Trust und Widerruf dieser Zertifikate Verwaltung der Hardware Security Module Vergabe der RO- und RCA-Berechtigung Ansprechpartner für sicherheitsrelevante Fragen Beaufsichtigung der Einhaltung der im CPS festgelegten Vorgehensweisen
Sicherheits-systemadministrator	Zutritt in die Hochsicherheitszone Beaufsichtigung von Systemadministrator und Systemoperator
Revocation Center Agent (RCA), Mitarbeiter im Widerrufsdienst	Ansprechpartner für die Zertifikatsinhaber hinsichtlich der Annahme von Anträgen für Widerruf und Aussetzung
Registration Officer (RO), Mitarbeiter der Registrierungsstelle	Entgegennahme von Zertifikatsanträgen Identifikation von Zertifikatswerbern im Rahmen der Registrierung Belehrung der Zertifikatsinhaber

Tabelle 5: Sicherheitskritische Funktionen

5.2.3 Sonstige (nicht sicherheitskritische) Funktionen

Rolle	Funktion
Systemadministrator	Administration, Installation, Konfiguration und Wartung der Systeme Wird in sicherheitskritischen Bereichen vom Sicherheitssystemadministrator beaufsichtigt.
Systemoperator	Laufende Systembetreuung, Datensicherung und -wiederherstellung für die täglichen Abläufe
Schulung	siehe Tabelle 4

Tabelle 6: Sonstige Funktionen

5.2.4 Anzahl erforderlicher Personen für sicherheitsrelevante Tätigkeiten

Tabelle 7 stellt sicherheitsrelevante Tätigkeiten dar und ordnet diesen die dafür zuständigen Rollen zu. Weiters wird aufgezeigt, ob für diese Tätigkeit das Vieraugenprinzip notwendig ist und ob diese Tätigkeit im Hochsicherheitsbereich des A-Trust Rechenzentrums ausgeübt wird.

Tätigkeit	Personen	Vier-augen-prinzip	Hoch-sicher-heit
Registrierung und Identifizierung von Zertifikatswerbern	RO	Nein	Nein
Widerrufen von Anwenderzertifikaten	RCA, RO	Nein	Nein
Erzeugung der Schlüssel für Root-CA und Zertifizierungsstellen sowie Schlüsselwechsel	SO, SO	Ja	Ja
Aktivierung der Schlüssel für Root-CA und Zertifizierungsstellen	SO, SO	Ja	Ja
Löschen der Schlüssel für Root-CA und Zertifizierungsstellen	SO, SO	Ja	Ja
Zertifizierung für die Root-CA und die Zertifizierungsstellen	SO, SO	Ja	Ja
Widerruf von Zertifikaten der CA	SO, SO	Ja	Ja
Vergabe der Berechtigungen für RO und RCA	SO, SO	Ja	Ja
Inbetriebnahme eines kryptographischen Moduls (Signaturerstellungseinheit der CA)	SO, SO	Ja	Ja
Ab- und Anschalten von Komponenten, insbesondere Verzeichnisdiensten	Sicherheits-systemadministrator	Nein	Nein
Austausch von Hardware-Komponenten	Sicherheits-systemadministrator (2x)	Ja	Ja
Austausch von Software-Komponenten	Sicherheits-systemadministrator (2x)	Ja	Ja
Überprüfung von Protokolldateien auf verdächtige Vorkommnisse	Systemadministrator	Nein	Nein
Überprüfung der Protokolldateien auf Manipulation	Systemadministrator	Nein	Nein

Tätigkeit	Personen	Vier-augen-prinzip	Hoch-sicher-heit
Anfertigung eines Backups der Protokolldateien und Lagerung desselben	Sicherheits-systemadministrator (2x)	Ja	Ja
Qualitätsprüfung der verwendeten Schlüssellängen und Parameter zur Schlüsselerzeugung	SO	Nein	Nein
Wartung oder Austausch eines kryptographischen Moduls	SO, SO	Ja	Ja

Tabelle 7: Anzahl erforderlicher Personen

5.2.5 Identifikation der Rollen

Die Zugangskontrollsysteme beschränken den Zutritt zu Räumlichkeiten mit sicherheitskritischen Komponenten auf Personen, die den zugelassenen Rollen zugewiesen sind.

5.3 Personelle Sicherheitsvorkehrungen

5.3.1 Anforderungen an das Personal

Personal, das A-Trust beschäftigt, erfüllt alle notwendigen Anforderungen hinsichtlich Vertrauenswürdigkeit, Integrität, Zuverlässigkeit und Fachkunde und verfügt über ausreichendes Fachwissen in den Bereichen:

- allgemeine EDV-Ausbildung,
- Sicherheitstechnologie, Kryptographie, elektronische Signatur und Public Key Infrastructure,
- technische Normen, insbesondere Evaluierungsnormen, sowie
- Hard- und Software.

5.3.2 Überprüfung des Personals

Gemäß Art 5 [SVV] dürfen im Rahmen der bereitgestellten Signatur- und Zertifizierungsdienste keine Personen beschäftigt werden, die wegen einer mit Vorsatz begangenen strafbaren Handlung zu einer Freiheitsstrafe von mehr als einem Jahr oder wegen strafbarer Handlungen gegen das Vermögen oder gegen die Zuverlässigkeit von Urkunden

und Beweiszeichen zu einer Freiheitsstrafe von mehr als drei Monaten verurteilt wurden. Verurteilungen, die nach den Bestimmungen des Tilgungsgesetzes 1972 getilgt sind oder der beschränkten Auskunft unterliegen, bleiben außer Betracht.

5.3.3 Anforderungen an die Schulung

Es finden regelmäßige Schulungen durch kompetentes Personal für alle Mitarbeiter statt. Diese Schulungen haben sowohl einen fachlichen als auch einen sicherheitstechnischen Hintergrund. Die Berechtigung, eine Rolle auszuüben, wird erst nach erfolgter Schulung erteilt.

Im Hinblick auf die Qualitätssicherung der A-Trust Dienstleistungen wird auf die Schulung der Mitarbeiter der Registrierungsstelle und des Widerrufsdienstes als primäre Schnittstelle zum Signator besonderer Wert gelegt.

Die Mitarbeiter der Registrierungsstelle müssen einen, vom A-Trust Schulungsbeauftragten abgehaltenen, Kurs absolvieren, der die Grundvoraussetzung für die Ausübung der Rolle des RO darstellt. In jeder RA stehen außerdem speziell geschulte Zentrale Registration Officer zur Verfügung, die die anderen ROs bei Problemen und Fragen unterstützen. Jeder RO hat außerdem Checklisten und Merkblätter zur Verfügung, die ihn in standardisierter Weise durch den Registrierungsprozesses durchführen sollen.

Auch die Mitarbeiter des Widerrufsdienstes (RCA) erhalten eine Einschulung durch den A-Trust Schulungsbeauftragten. Weiters erhalten sie die für ihre Tätigkeit benötigten Unterlagen (Betriebskonzept für den Widerrufsdienst) und ebenfalls eine standardisierte Aufstellung des Ablaufs der Kommunikation mit dem Signator.

5.3.4 Anforderungen und Häufigkeit von Schulungswiederholungen

Die Schulungen finden in regelmäßigen Abständen insbesondere bei der Einführung neuer technischer Systeme, Software oder Sicherheitssysteme statt.

5.3.5 Ablauf und Frequenz der Job Rotation

Keine Bestimmungen.

5.3.6 Sanktionen für unautorisierte Handlungen

Schwerwiegende Verstöße gegen Sicherheitsvorkehrungen werden disziplinarisch geahndet.

5.3.7 Anforderungen an Vertragsvereinbarungen mit dem Personal

Das Personal ist gemäß Datenschutzgesetz zur Geheimhaltung verpflichtet.

5.3.8 An das Personal auszuhändigende Dokumente

An das Personal werden je nach Örtlichkeit und Rolle insbesondere folgende Dokumente ausgehängt:

- Betriebskonzept je nach Örtlichkeit und Rolle,
- Sicherheitskonzept,
- Zertifizierungsrichtlinie und
- Schulungsunterlagen.

6 Technische Sicherheitsvorkehrungen

6.1 Schlüsselgenerierung und Installation

6.1.1 Schlüsselgenerierung

6.1.1.1 Schlüssel für Zeitstempel-Zertifikate

Die Schlüssel werden im Hochsicherheitsbereich der A-Trust generiert.

6.1.1.2 Schlüssel der Zertifizierungsstelle

Die Schlüssel der Zertifizierungsstelle werden im Hardware Security Modul in der Zertifizierungsstelle generiert. Für die geheimen Schlüssel der Zertifizierungsstelle gibt es keine Exportmöglichkeit und auch keine Backups oder wenn ein Backup technisch nicht verhindert werden kann, dann wird sichergestellt, dass das Backup nicht auf einem anderen HSM eingespielt wird. Die Erzeugung von Schlüsseln in der Zertifizierungsstelle erfolgt immer unter der Aufsicht von zwei befugten A-Trust Mitarbeitern und muss von der Geschäftsführung der A-Trust angeordnet werden.

6.1.2 Zurverfügungstellung öffentlicher Schlüssel an Zertifikatsaussteller

Alle Schlüssel der Zertifizierungsstelle werden zentral erzeugt und müssen deshalb nicht an die Zertifizierungsstelle ausgeliefert werden.

6.1.3 Zurverfügungstellung öffentlicher Schlüssel von der Zertifizierungsstelle an die Zeitstempelauslöser

Das Zertifikat des Schlüssels der Root-CA sowie aller Zertifizierungsstellen werden in einem Verzeichnis im Internet veröffentlicht, damit es allgemein zugänglich ist und alle Zertifikatsnutzer Zertifikate dagegen prüfen können. Ein Fingerprint des öffentlichen Schlüssels der Root-CA wird außerdem der Aufsichtsstelle bekanntggeeben.

6.1.4 Schlüssellängen

Die Schlüssel der Root-CA und aller Zertifizierungsstellen, sowie die eingesetzten Hash-Algorithmen sind in folgender Tabelle dargestellt.

CA-Generation: die von der CA A-Trust-Root-05 signierten Zertifikate sind in Tabelle 8 als Generation 5 dargestellt. Siehe auch Kapitel 1.3.5.

Diese Mindestlängen können sich ändern, wenn die eingesetzten Algorithmen nicht mehr den Sicherheitserwartungen entsprechen oder sich die gesetzlichen Vorgaben ändern.

	CA Generation	
	< 5	≥ 5
CA-Schlüssellänge	RSA 2048	RSA 4096
Hash-Algorithmus	SHA-1	SHA-256

Tabelle 8: Schlüssellängen

6.1.5 Parameter zur Schlüsselerzeugung

Für ECC-Schlüssel werden die Anforderungen an die ECC Schlüsselgenerierung lt. ANSI X9.62, The Elliptic Curve Digital Signature Algorithm (ECDSA), Abschnitt 'Key Pair Generation' erfüllt (siehe [ANSI X9.62]).

Die verwendete Kurve ist prime256v1 gem. [ANSI X9.62].

6.1.6 Qualitätsprüfung der Parameter

Der Beauftragte für IT-Sicherheit überwacht die Einhaltung der gesetzlichen Anforderungen für die Parameter zur Signaturschlüsselerzeugung und stellt die korrekte Verwendung des physikalischen Zufallszahlengenerators sicher.

6.1.7 Hardware/Software Schlüsselerzeugung

Die Schlüssel der Root-CA und aller Zertifizierungsstellen werden in einer speziellen Hardware erzeugt und dort auch eingesetzt.

6.1.8 Verwendungszweck der Schlüssel (nach X.509 v3 usage Feld)

Der Verwendungszweck für den zertifizierten Schlüssel wird in den X.509 V3 Zertifikaten in der Extension „keyUsage“ angegeben.

6.1.8.1 Verwendung der Schlüssel der Root-CA

Die Root-CA besitzt ein selbst signiertes Zertifikat, in welchem im Attribut 'keyUsage' die Bits

- keyCertSign (Signieren von Zertifikaten) und
- cRLSign (Signieren von Widerrufslisten)

gesetzt sind.

6.1.8.2 Verwendung der Schlüssel der Zertifizierungsstellen

Die Schlüssel der Zertifizierungsstelle werden ausschließlich zum Signieren von Zertifikaten und Widerrufslisten eingesetzt. Deshalb werden die Bits

- keyCertSign (Signieren von Zertifikaten) und
- cRLSign (Signieren von Widerrufslisten)

gesetzt.

6.1.8.3 Verwendung des Schlüssels zum Zeitstempelauslösen

Der Schlüssel dient zum Auslösen eines Zeitstempels. Deshalb werden die Bits

- nonRepudiation und
- digitalSignature
- id-kp-timeStamping

gesetzt.

6.2 Schutz der privaten Schlüssel

6.2.1 Standards des kryptografischen Moduls

6.2.1.1 Schlüssel der Zertifizierungsstelle

Als kryptografische Module werden Hardware Security Module eingesetzt.

Der private Schlüssel der Root-CA dient zur Signatur der Zertifikate der Zertifizierungsstellen und der zugehörigen Widerrufslisten. Er wird nur in einer gesicherten Umgebung eingesetzt.

Der Schlüssel einer Zertifizierungsstelle dient zur Signatur von Zertifikaten und Widerrufslisten. Er wird nur in einer sicheren Umgebung eingesetzt.

Für die Speicherung und Anwendung des privaten Schlüssels der Root-CA und aller Zertifizierungsstellen werden nur Hardware Security Module eingesetzt, die einen angemessenen physikalischen Zugriffsschutz auf diese Schlüssel bieten.

6.2.1.2 Schlüssel der Zeitstempel-Zertifikate

Der private Schlüssel der Zeitstempel-Zertifikate werden in einem kryptographischen Sicherheitsmodul gem. [ETSI EN 319 421] erzeugt. Der private Schlüssel wird von der Zertifizierungsstelle verwaltet und kann nur angewendet werden, wenn er noch gültig ist.

6.2.2 Aufteilung privater Schlüssel auf mehrere Personen

Private Schlüssel befinden sich in einem Hardware Security Modul (Schlüssel der Zertifizierungsstelle).

Es gilt, dass für die Aktivierung des Schlüssels der Root-CA oder einer Zertifizierungsstelle ein Vieraugenprinzip erforderlich ist. Eine einzelne Person darf nicht über die Mittel verfügen, einen dieser privaten Schlüssel zu nutzen.

Für Ersteller von Zeitstempel ist die alleinige Kontrolle durch den Siegelerstellers erforderlich.

6.2.3 Hinterlegung privater Schlüssel

Private Schlüssel können nicht hinterlegt werden. Dies gilt sowohl für die Schlüssel der Zertifizierungsstelle als auch für Schlüssel zum Auslösen eines Zeitstempelauslöser.

6.2.4 Backup privater Schlüssel

Der private Schlüssel wird in einem kryptographischen Sicherheitsmodul gem. [ETSI EN 319 421] gespeichert.

6.2.5 Archivierung privater Schlüssel

Eine Archivierung privater Schlüssel findet nicht statt.

6.2.6 Einbringung privater Schlüssel in das kryptografische Modul

Die eingesetzte kryptografische Hardware ist so beschaffen, oder es wird organisatorisch sichergestellt, dass die privaten Schlüssel nur innerhalb dieses Mediums generiert werden können.

6.2.6.1 Schlüssel der Zertifizierungsstelle

Die privaten Schlüssel der Zertifizierungsstelle zum Signieren von Zertifikaten und Widerrufslisten werden in einem Hardware Security Modul erzeugt und dort gespeichert. Die Anwendung erfolgt ebenfalls direkt im Hardware Security Modul. Das gilt in gleicher Weise für den Root-Schlüssel wie auch die Schlüssel der Zertifizierungsstelle zur Signatur der qualifizierten Zeitstempelauslöserzertifikate.

6.2.6.2 Schlüssel der Zeitstempel-Zertifikate

Siehe 6.2.1.2.

6.2.7 Methode zur Nutzung privater Schlüssel

Die Nutzung bzw. Aktivierung der privaten Schlüssel der Zertifizierungsstelle ist durch eine Benutzerauthentifikation gesichert. Die Zeitstempel-Zertifikate können erst nach erfolgreicher Entschlüsselung eingesetzt werden.

6.2.8 Methode zur Deaktivierung privater Schlüssel

Wird ein Hardware Security Modul deaktiviert, so führt dies automatisch zur Deaktivierung aller in ihm enthaltenen privaten Schlüssel.

6.2.9 Methode zur Vernichtung privater Schlüssel

Es wird organisatorisch sichergestellt, dass alle Schlüssel bei Bedarf oder Ablauf der Gültigkeit nach den Vorgaben des HSM-Herstellers vernichtet und damit nicht mehr verwendet werden.

6.3 Verwendungszeitraum öffentlicher und privater Schlüssel

Als Gültigkeitsmodell wird das Kettenmodell eingesetzt. Zur Überprüfung der Gültigkeit eines Zertifikats wird dabei die übergeordnete Instanz herangezogen. Dabei muss das übergeordnete Zertifikat nur zum Zeitpunkt der Ausstellung des zu überprüfenden Zertifikats gültig gewesen sein. Ein übergeordnetes Zertifikat kann widerrufen werden, ohne dass die ihm untergeordneten, und vor dem Widerruf ausgestellten, Zertifikate dadurch ihre Gültigkeit verlieren.

Für die Zertifikate gelten die folgenden maximalen Gültigkeitsdauern (Jahre):

Zertifikatstyp	Gültigkeitsdauer
Root-CA	10
Zertifizierungsstellen	10
Zertifikatsinhaber	5

Tabelle 9: Gültigkeitsdauer von Zertifikaten

Eine Verlängerung der Gültigkeitsdauer eines Zertifikats (erneute Zertifizierung des öffentlichen Schlüssels) kann erfolgen, wenn die kryptografische Sicherheit der verwendeten Verfahren über die gesamte neue Gültigkeitsdauer ausreichend sicher gestellt ist und keine Hinweise auf Kompromittierung des zugehörigen privaten Schlüssels bestehen.

6.4 Computer Sicherheitsbestimmungen

6.4.1 Spezifische Sicherheitsanforderungen an die Computer

Keine Bestimmungen.

6.4.2 Bewertung der Computersicherheit

Keine Bestimmungen.

6.5 Life-Cycle der Sicherheitsvorkehrungen

6.5.1 Systementwicklung

Die Vorgaben zur Systementwicklung orientieren sich an den Sicherheitsvorgaben der A-Trust. Die folgenden Richtlinien müssen bei der Entwicklung eingehalten werden:

- Das Entwicklungssystem muss vom Echtsystem getrennt sein
- Die Übernahme der neu entwickelten/geänderten Software in das Echtsystem findet nach erfolgreich abgeschlossenem Test und nach erteilter Freigabe durch die Betriebsleitung statt.

6.5.2 Sicherheitsmanagement

Bestimmte organisatorische Regelungen hinsichtlich der Benutzung von Software müssen eingehalten werden:

- benutzt wird ausschließlich freigegebene Software aus bekannten Quellen,
- die Möglichkeit des unautorisierten Einspielens von Software wird verhindert,
- die Integrität von Standardsoftware wird sicher gestellt,
- Software-Bestände werden regelmäßig überprüft,
- Lizenzverwaltung und Versionskontrolle von Software werden durchgeführt,
- Mitarbeiter werden vor der Programmnutzung auf die Verwendung geschult,
- Handbücher müssen in ausreichender Zahl zur Verfügung stehen,
- Original-Software-Versionen werden sicher aufbewahrt,
- ggf. werden Sicherungskopien von Software angelegt,

- unerlaubte Zugriffe auf Software z.B. zur Erstellung von Raubkopien müssen verhindert werden,
- Regelungen für den Betrieb werden erlassen (Durchführung von Datensicherungen, Wechsel von Passwörtern).

6.5.3 Bewertung

Für die Bewertung von Software sind die folgenden Tätigkeiten durchzuführen:

- Entwicklung eines Testplans für Software,
- Testen der Software,
- Freigabe der Software.

6.6 Vorkehrungen zur Netzwerksicherheit

Die Übertragung von sicherheitskritischen Daten erfolgt durch eine angemessene Absicherung des Kommunikationskanals. Alle sicherheitsrelevanten Komponenten, auf die aus dem Internet zugegriffen werden kann, sind zusätzlich durch Firewalls geschützt.

6.7 Vorkehrungen zur Wartung (Analyse) des kryptografischen Moduls

Wartungsarbeiten finden ausschließlich im Vieraugenprinzip statt und werden gemäß Abschnitt 5.2.4 durchgeführt.

7 Profile von Zertifikaten und Widerrufslisten

Die Zertifikate, die unter dieser Zertifizierungsrichtlinie ausgegeben werden, sind X.509 v3 Zertifikate.

7.1 Zertifikatsprofile

7.1.1 CA-Zertifikate

Attribut	Inhalt	Erläuterung
Version	v3(2)	Die Versionsnummer wird auf '2' gesetzt, um ein X.509 Zertifikat der Version 3 anzuzeigen
Seriennummer	Seriennummer des Zertifikats	Eindeutig innerhalb der A-Trust Zertifizierungsinfrastruktur
Algorithmus	≥ SHA-2	Für die Signatur über das Zertifikat verwendeter Algorithmus
Aussteller des Zertifikats	CN = CommonName OU = OrganizationalUnit O = Organization C = AT	CommonName, OrganizationalUnit: A-Trust-Qual-nn Organization: A-Trust
Gültig von Gültig bis	Beginn und Ende der Gültigkeit des Zertifikats	Der Gültigkeitszeitraum beträgt höchstens 20 Jahre
Zertifikatsinhaber	CN = CommonName OU = OrganizationalUnit O = A-Trust C = AT	CommonName, OrganizationalUnit: a-sign premium timestamp-nn -nn bezeichnet die Generation der CA
Öffentlicher Schlüssel	≥ RSA 4096 Bit	Öffentlicher Schlüssel des Zertifikatsinhabers (der CA)

Tabelle 10: Profil für CA-Zertifikat

7.1.2 Zertifikate des Zeitstempeldienstes

Attribut	Inhalt	Erläuterung
Version	v3(2)	Die Versionsnummer wird auf '2' gesetzt, um ein X.509 Zertifikat der Version 3 anzuzeigen
Seriennummer	Seriennummer des Zertifikats	Eindeutig innerhalb der A-Trust Zertifizierungsinfrastruktur
Algorithmus	$\geq$ SHA-2	Für die Signatur über das Zertifikat verwendeter Algorithmus
Aussteller des Zertifikats	CN = CommonName OU = OrganizationalUnit O = A-Trust C = AT	CommonName, OrganizationalUnit: a-sign premium timestamp-nn -nn bezeichnet die Generation der CA.
Gültig von Gültig bis	Beginn und Ende der Gültigkeit des Zertifikats	Der Gültigkeitszeitraum beträgt höchstens fünf Jahre
Zertifikatsinhaber (subject)	C = CountryName (optional) CN = CommonName	CountryName: AT CommonName: Timestamp issuing certificate
Öffentlicher Schlüssel	$\geq$ ECC 256 Bit bzw. $\geq$ RSA 4096 Bit	Öffentlicher Schlüssel des Zertifikatsinhabers

Tabelle 11: Profil für Zeitstempel Zertifikate

7.1.3 Erweiterungen (certificate extensions)

In den Zertifikaten der CAs werden die folgenden Erweiterungen gemäß X.509 v3 und PKIX verwendet:

Erweiterung	Zertifikatstyp		Klassifikation	
	Root	CA	kritisch	nicht kritisch
Standarderweiterungen				
authorityKeyIdentifier	Nein	Ja		X
subjectKeyIdentifier	Ja	Ja		X
keyUsage	Ja	Ja	X	
subjectAltName	Optional	Optional		X
basicConstraints	Ja	Ja	X	
CRLDistributionPoints	Nein	Ja		X
Private Extensions				
authorityInfoAccess	Nein	Ja		X

Tabelle 12: Erweiterungen (CA-Zertifikate)

Die Verwendung von Erweiterungen in den von der CA ausgestellten Zertifikaten wird in den folgenden Tabellen dargestellt:

Erweiterung	Im Zertifikat vorhanden	Klassifikation	
		kritisch	nicht kritisch
Standarderweiterungen			
authorityKeyIdentifier	Ja		X
subjectKeyIdentifier	Ja		X
keyUsage	Ja	X	
certificatePolicies	Ja		X
basicConstraints	Ja		X
cRLDistributionPoints	Ja		X
subjectAltName	optional		X
id-kp-timeStamping	Ja	X	
esi4-qtstStatement-1	Ja		X
Private Extensions			
authorityInfoAccess	Ja		X

Tabelle 13: Erweiterungen Zeitstempel Zertifikat

Die Codierung der Object Identifier der anzuwendenden Policies ist in Kapitel 7.1.5 beschrieben.

7.1.4 Identifikation der Policy

Hier werden die Policies, die durch diese Zertifizierungsrichtlinie abgedeckt werden, benannt:

Die Erweiterung certificatePolicies im Zertifikat wird mit

- OID 1.2.040.0.17.1.21 gem. [Policy]
  1.2.040.0.17 (A-Trust).1 (Policy).21 (Zeitstempel)

codiert.

7.1.5 Semantik für die Verfahrensweise bei Certificate Policy Extension

Da die Extension certificatePolicies als "nicht-kritisch" markiert ist, sind keine weiteren Bestimmungen diesbezüglich erforderlich.

7.2 Profil der Widerrufsliste

7.2.1 Versionsnummern

Die von der Zertifizierungsstelle ausgegebenen Widerrufslisten sind Widerrufslisten gemäß X.509 v3 in der Version 2.

7.2.2 CRL und CRL Entry Extensions

Für komplette Widerrufslisten werden die nicht kritischen Erweiterungen *authorityKeyIdentifier* und *CRLNumber* verwendet. Delta-Widerrufslisten besitzen zusätzlich noch die kritische deltaCRLIndicator-Erweiterung. Als CRL Entry Extension wird nur der als unkritisch eingestufte *reasonCode* eingesetzt. Nachdem abgelaufene Widerrufenen oder gesperrten Zertifikate nicht von der Sperrliste entfernt werden, ist in der Sperrliste die Erweiterung *ExpiredCertsOnCRL* auf das Erstellungsdatum der CA gesetzt.

8 Nachsignieren

Keine Bestimmungen.

9 Administration dieser Spezifikation

9.1 Prozeduren zur Änderung dieses Dokuments

Änderungen an dieser Zertifizierungsrichtlinie werden ausschließlich durch A-Trust vorgenommen und müssen von der Geschäftsführung genehmigt werden. Änderungen, die sicherheitsrelevante Aspekte betreffen oder die Änderungen der Abläufe seitens der Zertifikatsinhaber erfordern, benötigen eine Anpassung der OID der Certificate Policies und der URI der Zertifizierungsrichtlinie und damit eine generelle Bekanntmachung gegenüber den Zertifikatsinhaber. Dies sind insbesondere Änderungen, die

- Verpflichtungen, Haftung, finanzielle Verantwortung,
- Registrierung,
- Personalisierung,
- Internetadressen und Kontaktinformationen,
- Schlüssel- und Zertifikatsmanagement,
- Verzeichnis- und Widerrufsdienst betreffen und
- Aussetzungen betreffen.

Betreffen die Änderungen an dieser Zertifizierungsrichtlinie keine der o. a. Aspekte, so können diese ohne Bekanntmachung erfolgen. Dies gilt insbesondere für Änderungen bez. Typographie und Layout sowie Adressen oder Geschäftszeiten von Kontaktstellen.

9.2 Verfahren zur Publizierung und Bekanntgabe

Nach einer Änderung können die aktuelle Zertifizierungsrichtlinie und Certificate Policy sowie auch weiterhin alte Versionen abgerufen werden.

9.3 Genehmigung und Eignung einer Zertifizierungsrichtlinie

Diese Zertifizierungsrichtlinie gilt für das Produkt Zeitstempel. A-Trust stellt sicher, dass diese Zertifizierungsrichtlinie für die betroffenen Certificate Policies geeignet ist.

A Anhang

A.1 Begriffe und Abkürzungen

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.
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.
Zeitstempelprüfdaten	Zeitstempelprüfdaten sind Daten wie Codes oder öffentliche Signaturschlüssel, die zur Überprüfung eines elektronischen Zeitstempels verwendet werden.
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 7.3

[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

[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

[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

[ETSI 319 422] Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

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

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