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

A-Trust Zertifikatsrichtlinie (Certificate Policy) für qualifizierte Zertifikate

Version: 1.1
Datum: 03-02-2025

Inhaltsverzeichnis

Tabellenverzeichnis

Rev	Date	Author	Changes
1.0	2024-10-24	IH, RS, CK	Initialversion
1.1	2025-02-03	IH	Bearbeitungszeit eines Zertifikatsantrags, Widerrufsgründe, Schlüsselverwendungszwecke, Namensformen (-ECC)

Tabelle 1: Dokumentenhistorie

1 Einleitung

1.1 Übersicht

Das Ziel des vorliegenden Dokuments besteht darin, die Umsetzung der Ausgabe, Administration und Anwendung von qualifizierten Zertifikaten derart festzulegen, dass eine sichere und zuverlässige Durchführung der angebotenen Zertifizierungsdienstleistungen sowie der Anwendung der ausgegebenen Zertifikate gewährleistet ist.

1.2 Name und Identifikation des Dokuments

Name der Richtlinie A-Trust Zertifikatsrichtlinie (Certificate Policy) für qualifizierte Zertifikate

Version 1.1 / 03-02-2025

Object Identifier 1.2.40.0.17 (A-Trust) .1 (CP) .99 (qualifizierte Zerifikate)

Der A-Trust OID 1.2.040.0.17 ist als ÖNORM registriert.

1.3 PKI Teilnehmende

1.3.1 Zertifizierungsstellen

Es existiert eine zentrale Zertifizierungsstelle, die die Schlüssel der signierenden Personen sowie die Widerrufslisten für Zertifikate signiert. A-Trust stellt qualifizierte Zertifikate (gemäß [eIDAS]) aus, die auf einer sicheren Signaturerstellungseinheit basieren. Darüber hinaus existiert eine Root-Zertifizierungsstelle, welche das Zertifikat und die Widerrufslisten für die Zertifizierungsstellen signiert. Zertifikate der Anwendenden werden von der Root-CA nicht ausgestellt. 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] und ist in die österreichische Vertrauensliste im Sinne des Artikels 22 [eIDAS] eingetragen.

1.3.2 Registrierungsstellen

In den Registrierungsstellen führen Registration Officer die anwenderrelevanten Arbeiten durch. Diese Aufgaben umfassen neben der sicheren Identifizierung auch die Bearbeitung der Daten der Anwendenden und die Weiterleitung von Informationen an die übergeordnete Zertifizierungsstelle. Die Ausstellung des Zertifikats erfolgt auf Veranlassung der Registrierungsstelle.

1.3.3 Anwendende

Unter Anwendenden sind die Personen zusammengefasst, die qualifizierte Zertifikate von A-Trust erhalten (Zertifikatsinhabende bzw. signierende Personen), oder welche qualifizierte Zertifikate nutzen bzw. den Zertifikatsangaben vertrauen (Signaturempfangende).

1.3.4 Vertrauende Stellen

Vertrauende Stellen sind jene, welche Signaturen basierend auf einem qualifizierten A-Trust Zertifikat bzw. die A-Trust Zertifikate prüfen.

1.3.5 Weitere Teilnehmende

Keine Bestimmungen.

1.4 Zertifikatsanwendung

1.4.1 Zulässige Zertifikatsanwendung

Qualifizierte Zertifikate dienen der Zertifizierung von Schlüsseln, die zur Erstellung qualifizierter Signaturen, Siegel sowie zur Auslösung qualifizierter Zeitstempel genutzt werden.

Elektronische Signaturen, die in Übereinstimmung mit dieser Zertifizierungsrichtlinie und unter Verwendung der von A-Trust empfohlenen Komponenten und Verfahren erstellt wurden, sind qualifizierte Signaturen im Sinne von Artikel 3 Z. 12 [eIDAS]. Elektronische Siegel sind qualifizierte Siegel im Sinne von Artikel 3 Z. 27 [eIDAS]. Elektronische Zeitstempel sind qualifizierte Zeitstempel im Sinne von Artikel 3 Z. 34 [eIDAS].

1.4.2 Unzulässige Zertifikatsanwendung

Die Zertifikatsanwendung kann über dem Standard entsprechende Mittel, eingeschränkt werden. Ist eine solche Einschränkung (keyUsage) im Zertifikat hinterlegt, so darf dieses nur für die angeführten Zwecke eingesetzt werden.

1.5 Policy Verwaltung

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

1.5.1 Dokumentverwaltende Organisation

A-Trust GmbH
Landstraßer Hauptstraße 1b
1030 Wien
Österreich

1.5.2 Kontaktinformation

Attn: Produktmanagement
A-Trust GmbH
Landstraßer Hauptstraße 1b
1030 Wien
Österreich

1.5.3 CP Zulassungsverfahren

Die Geschäftsführung der A-Trust ist verantwortlich, jede CP und CPS zu prüfen und freizugeben. Die Freigabe erfolgt mittels qualifizierter Signatur, welche den Zeitpunkt des Inkrafttreten anzeigt.

1.6 Definitionen und Abkürzungen

CA Certification Authority

CP Certificate Policy

CPS Certification Practice Statement

CRL Certificate Revocation List

eIDAS EU regulation [eIDAS]

LDAP Lightweight Directory Access Protocol

OCSP Online Certificate Status Protocol

OID Object Identifier

PIN Personal Identification Number

PKI Public Key Infrastructure

PUK Personal Unblocking Key

RA Registration Authority

RCA Revocation Center Agent

RFC Request for Comments

RO Registration Officer

RSA Encryption Algorithm

SO Security Officer

URI Uniform Resource Identifier

PSD2 DELEGIERTE VERORDNUNG (EU) 2018/389 DER KOMMISSION vom 27. November 2017

QSEE Qualifizierte Signatur- und Siegelerstellungseinheit

WORM Write once read many

2 Verantwortlichkeit für Veröffentlichung und Verzeichnisdienste

2.1 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/ und http://crl.a-trust.at
OCSP:	http://ocsp.a-trust.at/ocsp

Tabelle 2: Homepage und Verzeichnisse

Folgende Verzeichnisse werden von der Zertifizierungsstelle unterhalten:

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

2.2 Veröffentlichung von Zertifikatsinformation

Die Stammzertifikate sind zu finden unter:

- https://www.a-trust.at/certs/A-Trust-Qual-nnx.crt
- https://www.a-trust.at/certs/A-Trust-Root-nn.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 der Stammzertifikate kann auf sichere Weise über den entsprechenden Menüpunkt auf der A-Trust Homepage per https oder http erfolgen.

Die benötigten CA-Zertifikate sind zu finden unter:

- für a.sign premium (Karte):
  - https://www.a-trust.at/certs/a-sign-premium-sig-nnx.crt

- für a.sign premium seal:
  - https://www.a-trust.at/certs/a-sign-premium-seal-nnx.cer
- für a.sign premium mobile:
  - https://www.a-trust.at/certs/a-sign-premium-mobile-nnx.crt
- für EU-Identity Mobile:
  - https://www.a-trust.at/certs/EU-Identity-Mobile-nnx.crt
- für a.sign premium once (Einmalzertifikate):
  - https://www.a-trust.at/certs/a-sign-premium-once-nnx.crt
- für a.sign premium mobile seal:
  - https://www.a-trust.at/certs/a-sign-premium-mobile-seal-nnx.cer
- für a.sign premium timestamping:
  - https://www.a-trust.at/certs/a-sign-premium-timestamping-nnx.crt

2.3 Zeitpunkt oder Häufigkeit der Veröffentlichungen

Die A-Trust Website wird anlassbezogen aktualisiert. Verzeichnisdienst und Widerrufslisten werden gemäß Kapitel 4.9.7 veröffentlicht.

2.4 Zugriffskontrollen auf Verzeichnisse

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

3 Identifizierung und Authentifizierung

3.1 Namensregeln

3.1.1 Arten von Namen

Für Zertifikate natürlicher Personen:

- Nachname und Vorname sind erforderlich. Bei Namensteilen welche die Maximallänge des technischen Zertifikatsstandards überschreiten, können diese entsprechend ihrer Reihenfolge entfallen. Im Falle von Standard a.sign premium mobile können signierende Personen statt des Namens auch ein Pseudonym wählen. Der korrekte und vollständige Name muss der Registrierungsstelle und Zertifizierungsstelle auch bei Verwendung eines Pseudonyms bekannt sein.
- Die Angabe der postalischen oder einer elektronischen Adresse ist erforderlich sofern es sich nicht um Einmalzertifikate (a.sign premium once) handelt.
- Optional können im Namen der Zertifikatswerbenden die Attribute OrganizationName mit dem Inhalt 'Berufsbezeichnung' (z.B. Rechtsanwalt) und OrganizationalUnit mit einem eindeutigen Code (z.B. Rechtsanwaltscode) als Inhalt vergeben werden. Diese Attribute werden nur vergeben, wenn die ausstellende Registrierungsstelle, z.B. Rechtsanwaltskammer, die Korrektheit dieser Angaben sicher stellt. Das Attribut OrganizationName kann auch bei Behördenzertifikaten nach Bekanntgabe der Behörde vergeben werden

Für Zertifikate juristischer Personen:

- Vollständiger Name und ggf. die Registriernummer gemäß der amtlichen Eintragung sind erforderlich.
- Die Angabe der Firmen-Adresse ist optional.
- Im Falle eines Zertifikates im Sinne von Artikel 34 [PSD2] können zusätzlich folgende Attribute aufgenommen werden:
  - Die Rolle des zahlungsdienstleistenden Unternehmens, die eine oder mehrere der folgenden Funktionen umfassen kann:
    - Kontoführung
    - Zahlungsauslösung
    - Kontoinformation
    - Ausstellung kartenbasierter Zahlungsinstrumente
  - Den Namen der zuständigen Behörden, bei denen das zahlungsdienstleistende Unternehmen eingetragen ist.

3.1.2 Aussagekraft der Namen

Der Name der signierenden Person bzw. des besiegelnden Unternehmens muss den bei der Registrierung vorliegenden Identitätsdaten entsprechen. Qualifizierte Zertifikate, die auf die Namen Max Mustermann, Test Zupfer, Test Test, Musterfrau Maxine lauten oder deren Namen mit 'XXX' beginnen, werden von der A-Trust GmbH zu Testzwecken ausgestellt. Aus diesem Grund wird bei Ausstellung von qualifizierten Zertifikaten auf die genannten Namen keine Identitätsprüfung durchgeführt.

3.1.3 Anoymität oder Pseudonymität der Nutzenden

Wird ein Pseudonym verwendet, so muss es wie folgt codiert werden: 'Pseudonym: Pseudonymbezeichnung'.

3.1.4 Regeln zur Auslegung der verschiedenen Namensformen

Keine Bestimmungen.

3.1.5 Einzigartigkeit der Namen

Jede signierende Person erhält eine 12 stellige Nummer (Cardholder Identification Number, abgekürzt CIN). Diese Nummer ist ein Teil des eindeutigen Namens der signierenden Person und ermöglicht die eindeutige und unveränderliche Zuordnung von Signaturerstellungsdaten und -prüfdaten zu einer signierenden Person.

Für Einmalzertifikate wird keine CIN generiert, stattdessen wird ein eindeutiger, zufälliger Wert in das Zertifikat aufgenommen.

3.2 Initiale Überprüfung der Identität

3.2.1 Methode zum Beweis des Besitzes des privaten Schlüssels

Für Zertifikate natürlicher Personen:

Signaturkarte: Die Signaturkarte wird mit einem generierten Schlüsselpaar im Zuge des Ausstellungsprozesses an die signierende Person übergeben. Bei der Zertifikatsausstellung wird durch einen sicheren Kanal zur Signaturkarte der Besitz des privaten Schlüssels sichergestellt.

Mobile Zertifikate: Der private Schlüssel wird im Rahmen der Ausstellung von A-Trust generiert.

Für Zertifikate juristischer Personen:

- Die Siegelkarte wird mit einem generierten Schlüsselpaar im Zuge des Ausstellungsprozesses an die signierende Person übergeben. Bei der Zertifikatsausstellung wird durch einen sicheren Kanal zur Siegelkarte der Besitz des privaten Schlüssels sichergestellt.
- Der private Schlüssel wird bei a.sign seal mobile Zertifikaten im Rahmen der Ausstellung von A-Trust generiert.

3.2.2 Authentifizierung juristischer Personen

Die Identität der antragsstellenden bzw. zeichnungsberechtigten Personen ist analog zu 3.2.3 oder durch eine qualifizierte elektronische Signatur durchzuführen. Die Vertretungsbefugnis der Vertretung der Antragstellenden ist durch Vorlage einer von der gesetzlichen Vertretung der Antragsstellenden gefertigten Vollmacht nachzuweisen.

Als Voraussetzung für die Beantragung eines qualifizierten Zertifikats für ein qualifiziertes elektronisches Siegel, muss die Identität und ggf. die Adresse des Firmensitzes des antragstellenden Unternehmens überprüft werden. Wenn das antragstellende Unternehmen im Österreichischen Firmenbuch oder eines vergleichbaren amtlichen Registers eingetragen ist, erfolgt die Überprüfung der Identität und ggf. der Adresse des Firmensitzes mittels Abfrage. Anderenfalls hat die Vertretung der Antragstellenden die Identität und ggf. die Adresse des Firmensitzes durch Vorlage eines notariell beglaubigten Nachweises zu bestätigen. Eine Ausstellung von Siegel-Zertifikaten ist nur für juristische Personen möglich, deren Firmensitz in der Europäischen Union liegt.

3.2.3 Authentifizierung natürlicher Personen

Die Angaben der Antragstellenden werden bei der Ausstellung des Zertifikates in der Registrierungsstelle durch Registration Officer überprüft. Antragstellende beweisen ihre Identität durch das Vorlegen eines gültigen, amtlichen Lichtbildausweises gemäß den Anforderungen des Artikels 24 (1a) lit d [eIDAS].

Alternativ hierzu kann eine Bestätigung der Identität durch eine öffentliche Einrichtung erfolgen, sofern die initiale Identitätsfeststellung und Ausgabe der Zugangsdaten zu deren Onlineportal den Anforderungen des Artikels 24 (1a) lit a [eIDAS] bzw. 4a [E-GovG] entspricht. Diese Bestätigung wird in elektronischer Form, durch die öffentliche Stelle signiert, vor der Zertifikatsausstellung an A-Trust übermittelt.

Darüber hinaus können alle gemäß Artikel 24 [eIDAS] zulässigen Identifizierungsmethoden eingesetzt werden.

Die spezifische Liste der für die jeweiligen Identifizierungsverfahren zulässigen Ausweistypen ist im Dokument „Für die Ausstellung qualifizierter Zertifikate akzeptierte Ausweisdokumente“ in der jeweils aktuellsten Version festgehalten. Es sind ausschließlich Ausweisdokumente zulässig, die von den jeweiligen Registration Officern aufgrund der Sprache des vorgelegten Ausweises geprüft werden können.

3.2.4 Nicht-verifizierte Nutzendeninformation

Geprüft werden speziell Vorname, Nachname, Geburtsdatum, sowie Organisation.

3.2.5 Validierung einer Behörde

Die Validierung einer Behörde erfolgt in Rücksprache mit der zuständigen Bundesbehörde.

3.2.6 Kriterien in der Interoperation

Keine Bestimmungen.

3.3 Identifizierung und Authentifizierung für Neuverschlüsselungsanfragen

3.3.1 Identifizierung und Authentifizierung für routinemäßige Neuverschlüsselung

Die signierende bzw. siegelerstellende Person kann ein Ersatzprodukt bestellen und analog der Erstregistrierung aktivieren.

3.3.2 Identifizierung und Authentifizierung für Neuverschlüsselungsanfragen nach Widerruf

Die signierende bzw. siegelerstellende Person kann nach einem Widerruf ein Ersatzprodukt bestellen und analog der Erstregistrierung aktivieren.

3.4 Identifizierung und Authentifizierung für Widerrufsanträge

Die signierende Person kann das Zertifikat mittels der unter www.a-trust.at/widerruf angegebenen Methoden aussetzen bzw. widerrufen. Dazu muss die signierende Person zumindest ihren Namen, Daten des betroffenen Zertifikats (Seriennummer) und das Aussetzungs- und Widerrufspasswort (sofern vorhanden) bzw. das Aussetzungsaufhebungspasswort angeben. Sollte das Aussetzung- und Widerrufspasswort nicht bekannt sein, ist eine Aussetzung (kein Widerruf) mit folgenden Angaben möglich:

- Vollständiger Name
- Pseudonym (falls verwendet)
- Geburtstag
- Geburtsort

Eine Aussetzung kann innerhalb von zehn Tagen wieder aufgehoben werden. Wenn das Passwort für einen Widerruf vergessen wurde, kann die signierende Person keinen Widerruf durchführen, sondern nur eine Aussetzung und diese ohne Aufhebung in einen Widerruf übergehen lassen.

Abgelaufene Zertifikate können weder ausgesetzt noch widerrufen werden.

4 Betriebsanforderungen für den Lebenszyklus des Zertifikats

4.1 Zertifikatsantrag

4.1.1 Wer darf ein Zertifikat beantragen?

Jede Person kann ein Zertifikat beantragen. Eine Ausstellung von qualifizierten Siegel-Zertifikaten ist nur für juristische Personen möglich, deren Firmensitz in der Europäischen Union liegt.

4.1.2 Einschreibungsverfahren und Zuständigkeiten

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

Das Verfahren umfasst somit die Registrierung, das Akzeptieren der Bedingungen des Signaturvertrags und jener der darin referenzierten Dokumente, das Zahlen etwaiger Gebühren sowie ggf. die Schlüsselerzeugung.

4.2 Zertifikatsantragsprozess

4.2.1 Ausführen von Identifizierungs- und Authentifizierungsfunktionen

Die Korrektheit der Daten natürlicher Personen wird wie in Kapitel 3.2.3 beschrieben verifiziert. Die Korrektheit der Daten juristischer Personen wird wie in Kapitel 3.2.2 beschrieben verifiziert.

Wenn die Zugehörigkeit zu einer Behörde abgebildet werden soll, so wird von einer autorisierten Behördenvertretung zusätzlich zum Antrag ein Schreiben an die A-Trust Re-

gistrierungsstelle gesandt, das die Rechtmäßigkeit dieser Angabe bestätigt.

4.2.2 Genehmigung oder Ablehnung von Zertifikatsanträgen

Genehmigung oder Ablehnung eines Zertifikatsantrags erfolgt durch A-Trust.

4.2.3 Bearbeitungszeit eines Zertifikatsantrags

Die Zertifikatsausstellung erfolgt zeitnah, nach Übermittlung aller erforderlichen Dokumente und Daten. Die Zertifikatsausstellung kann innerhalb von drei Monaten ab durchgeführter Identifizierung erfolgen.

4.3 Zertifikatsausstellung

4.3.1 CA Maßnahmen während der Zertifikatsausstellung

A-Trust prüft die ordnungsgemäße Signatur und Vollständigkeit jedes Zertifikatsantrags vor der Ausstellung des Zertifikats.

4.3.2 Benachrichtigung der Nutzenden durch die CA über Zertifikatsausstellung

Bei Zertifikaten auf Smartcard-Basis wird die Karte nach erfolgter Zertifikatsausstellung an die signierende Person übergeben. Bei Ausstellungen im Rahmen eines Fernregistrierungsverfahrens kann die nutzende Person nach Abschluss des jeweiligen Vorganges über die erfolgreiche Zertifikatsausstellung informiert werden.

4.4 Zertifikatsannahme

4.4.1 Verhalten, das eine Annahme darstellt

Zertifkate werden durch Übergabe bzw. Festlegung der Zugangsdaten und Abschluss des Fernregistrierungsverfahrens als übermittelt und angenommen erachtet.

Bei Einmalzertifikaten wird der Start des Signaturvorgangs als Annahme erachtet.

4.4.2 Zertifikatsveröffentlichung durch die CA

Ausgestellte Zertifikate werden im Verzeichnisdienst veröffentlicht wobei je nach Zertifikatsprodukt diese Veröffentlichung im Sinne des Grundsatzes der Datenminimierung

entfallen kann. Unabhängig davon kann die signierende Person die Veröffentlichung im bzw. die Entfernung aus dem Verzeichnisdienst schriflich beantragen.

4.4.3 Benachrichtigung weiterer Stellen durch die CA über Zertifikatsausstellung

Eine Benachrichtigung weiterer Stellen ist nicht vorgesehen.

4.5 Schlüsselpaar- und Zertifikatsnutzung

4.5.1 Privater Schlüssel und Zertifikatsnutzung der Nutzenden

Die nutzende Person ist dazu verpflichtet, die in den im Signaturvertrag aufgezählten relevanten Dokumenten (u. a. AGB, CP, CPS, Unterrichtung) sowie einschlägigen Rechtsquellen definierten Pflichten einzuhalten. Zu diesen Pflichten gehören unter anderem aber nicht auschließlich die sichere Aufbewahrung und Verwendung des privaten Schlüssels bzw. der Zugangsdaten zur Auslösung einer Signatur, die Unterlassung der Weitergabe dieser sowie die Widerrufspflicht im Falle der Kompromittierung.

4.5.2 Öffentlicher Schlüssel und Zertifikatsnutzung vertrauender Stellen

Vertrauende Beteiligte (Kapitel 1.3), die eine Signaturprüfung vornehmen müssen die Vorgaben der CPS und CP beachten, hierfür geeignete Komponenten und Verfahren einsetzen, sowie den Status des Signaturzertifikats zum Signaturzeitpunkt überprüfen. Hierfür kann die im Zertifikat angeführte Sperrliste (CRL) oder eine OCSP Abfrage herangezogen werden.

4.6 Zertifikatsverlängerung

4.6.1 Umstände für eine Zertifikatsverlängerung

Zertifikate für natürliche Personen können verlängert werden, wenn das zu verlängernde Zertifikat noch gültig (nicht abgelaufen und nicht gesperrt/widerrufen) ist, der private Schlüssel nicht kompromittiert wurde und der Zertifikatsinhalt weiterhin korrekt ist. Hierbei wird der private Schlüssel weiterhin verwendet, das neu ausgestellte Zertifikat beinhaltet daher denselben öffentlichen Schlüssel.

Für Zertifikate für juristische Personen und Einmalzertifikate ist keine Zertifikatsverlängerung möglich, hier muss eine neuerliche Bestellung vorgenommen werden.

4.6.2 Wer kann eine Zertifikatsverlängerung beantragen?

Die Verlängerung erfolgt ausschließlich auf Antrag der nutzenden Person. Je nach Zertifikatsprodukt kann bereits im Zuge der Ausstellung eine automatische Zertifikatsverlängerung beantragt werden.

4.6.3 Bearbeitung von Zertifikatsverlängerungsanträgen

Zertifikate werden nach Beantragung ausgestellt und bereitgestellt.

4.6.4 Benachrichtigung der Nutzenden über Zertifikatsverlängerung

Nutzende werden per Mail über die Bereitstellung des Verlängerungszertifikats informiert wenn dieses nicht im Rahmen des Antragsprozesses unmittelbar ausgestellt wird.

4.6.5 Verhalten, das eine Annahme einer Zertifikatsverlängerung darstellt

Bei Zertifikaten auf Smartcard-Basis ist die Aufbringung des neuen Zertifikats auf der Smart Card erforderlich. Die nutzende Person kann diesen Vorgang über eine von A-Trust bereitgestellte Applikation durchführen, dieser Vorgang stellt die Annahme dar. Bei Zertifikaten zur Fernsignatur erfolgt die Verlängerung und Verknüpfung der bestehenden Zugangsdaten in einem zusammenhängenden Prozess, die Signatur durch die nutzende Person stellt die Annahme dar.

4.6.6 Veröffentlichung der Zertifikatsverlängerung durch die CA

Ausgestellte Zertifikate werden im Verzeichnisdienst veröffentlicht wobei je nach Zertifikatsprodukt diese Veröffentlichung im Sinne des Grundsatzes der Datenminimierung entfallen kann. Unabhängig davon kann die signierende Person die Veröffentlichung im bzw. die Entfernung aus dem Verzeichnisdienst schriflich beantragen.

4.6.7 Benachrichtigung weiterer Stellen durch die CA über Zertifikatsverlängerung

Eine Benachrichtigung weiterer Stellen ist nicht vorgesehen.

4.7 Zertifikatserneuerung mit Schlüsselerneuerung

Eine Zertifikatserneuerung mit Schlüsselerneuerung ist nicht vorgesehen und wird wie eine Zertifikatsneuausstellung (vgl. Kapitel 4.1) gehandhabt.

4.7.1 Umstände für eine Zertifikatserneuerung mit Schlüsselerneuerung

Nicht zutreffend.

4.7.2 Wer kann eine Zertifizierung eines neuen öffentlichen Schlüssels beantragen?

Nicht zutreffend.

4.7.3 Bearbeitung von Anträgen zur Zertifikatserneuerung mit Schlüsselerneuerung

Nicht zutreffend.

4.7.4 Benachrichtigung der Nutzenden über neue Zertifikatsausstellung

Nicht zutreffend.

4.7.5 Verhalten, das eine Annahme einer Zertifikatserneuerung mit Schlüsselerneuerung darstellt

Nicht zutreffend.

4.7.6 Veröffentlichung der Zertifikatserneuerung mit Schlüsselerneuerung durch die CA

Nicht zutreffend.

4.7.7 Benachrichtigung weiterer Stellen durch die CA über Zertifikatserneuerung

Nicht zutreffend.

4.8 Zertifikatsänderungen

Eine Zertifikatsänderug ist nicht vorgesehen und wird wie eine Zertifikatsneuausstellung (vgl. Kapitel 4.1) gehandhabt.

4.8.1 Umstände für Zertifikatsänderungen

Nicht zutreffend.

4.8.2 Wer kann eine Zertifikatsänderung beantragen?

Nicht zutreffend.

4.8.3 Bearbeitung von Zertifikatsänderungsanträgen

Nicht zutreffend.

4.8.4 Benachrichtigung der Nutzenden über Ausstellung des geänderten Zertifikats

Nicht zutreffend.

4.8.5 Verhalten, das eine Annahme eines geänderten Zertifikats darstellt

Nicht zutreffend.

4.8.6 Veröffentlichung des veränderten Zertifikats durch die CA

Nicht zutreffend.

4.8.7 Benachrichtigung weiterer Stellen durch die CA über Zertifikatsänderungen

Nicht zutreffend.

4.9 Zertifikatswiderruf und -aussetzung

4.9.1 Umstände für einen Widerruf

Der Widerruf eines Zertifikats wird erforderlich, wenn

- Angaben im Zertifikat nicht mehr korrekt sind
- die signierende Person nicht mehr im alleinigen Besitz der Signaturauslösedaten bzw. der für die Verifikation genutzten Methode ist

- Verdacht auf eine Kompromittierung besteht bzw. eine Kompromittierung vorliegt
- der Zertifizierungsstelle ein wesentlicher Verstoß der signierenden Person gegen diese Richtlinien oder die Allgemeinen Geschäftsbedingungen bekannt wird
- die Frist einer Aufhebung einer Aussetzung abläuft
- das Vertragsverhältnis beendet wird
- die eingesetzten Algorithmen und Verfahren nicht mehr den Sicherheitserwartungen entsprechen und dadurch eine sichere Anwendung der Signaturerstellungsdaten nicht mehr gegeben wäre.
- Ablauf der Bescheinigung der eingesetzten Siegel- oder Signaturerstellungseinheit

4.9.2 Wer kann einen Widerruf beantragen?

Ein Widerruf eines Zertifikats kann angeordnet werden durch:

- die betreffende signierende Person oder eine andere Person, die das Passwort für den Widerruf kennt
- bei Verwendung eines Organisationsnamens eine vertretungsbefugte Person der Organisation
- die Zertifizierungsstelle selbst

4.9.3 Verfahren für Widerrufsanträge

Ein Widerruf kann durch die signierende Person sowie im Fall des Firmensiegels der zeichnungsberechtigten Person (sowie Vertretungsbefugte) vorgenommen werden. Dies kann wie folgt geschehen:

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

- Personendaten der signierenden Person
- Passwort für den Widerruf
- Identifikationsnummer der signierenden Person (CIN), Kartennummer oder Seriennummer des Zertifikats

Elektronisch Die elektronische Übermittlung des Widerrufs muss das Aussetzungs- und Widerrufs-Passwort sowie die vollständige Seriennummer oder die Vertragsnummer des zu widerrufenden Zertifikats beinhalten.

Besuch in einer Registrierungsstelle Die signierende Person benötigt dazu einen gültigen, amtlichen Lichtbildausweis. Die Registrierungsstelle teilt der signierenden Person die Zertifikatsnummer und das Passwort für den Widerruf mit, womit die signierende Person anschließend den Widerruf beim Widerrufsdienst veranlassen kann.

4.9.4 Beantragungsfrist für Widerrufsanträge

Die signierende Person hat die Pflicht, unmittelbar nach Bekanntwerden eines Widerrufsgrundes (siehe 4.9.1) den Widerruf zu beantragen.

4.9.5 Bearbeitungszeit der CA für einen Widerrufsantrag

Telefonisch Die Aktualisierung der Widerrufsinformationen erfolgt innerhalb von längstens drei Stunden.

Elektronisch An Werktagen (Montag bis Freitag) von 8:00 bis 17:00 innerhalb von längstens sechs Stunden.

4.9.6 Widerrufsprüfungspflichten vertrauender Stellen

Das Überprüfen der Gültigkeit von Zertifikaten liegt in der Verantwortung der vertrauenden Stelle. Der Inhalt eines Zertifikats kann nur dann als authentisch gelten, wenn sich die vertrauende Stelle 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

Vertrauende Stellen sollten 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 den Nutzenden lokal gespeicherten Zertifikate sollten vor ihrer Nutzung gegen eine aktuelle Widerrufsliste geprüft werden. Sofern keine erfolgreiche Gültigkeitsprüfung vorgenommen werden kann (beispielsweise aus technischen Gründen), sollten keine Zertifikate akzeptiert werden. Jede Akzeptanz eines solchen Zertifikats erfolgt auf das Risiko der vertrauenden Stellen.

4.9.7 Häufigkeit der CRL Veröffentlichung

Die Aktualisierung der Widerrufsliste erfolgt in regelmäßigen Abständen. Die Intervalle der Aktualisierung sind der jeweils gültigen Widerrufsliste zu entnehmen.

4.9.8 Maximale Latenzzeit für CRLs

A-Trust setzt Maßnahmen, um die maximale Latenzzeit des Abrufs der CRL so gering als möglich zu halten.

4.9.9 Verfügbarkeit von online Widerrufs-/Statusprüfungen

Es wird ein OCSP-Dienst über das Internet angeboten.

4.9.10 Anforderungen für online Widerrufsprüfungen

Vertrauende Stellen sollten 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 Internet-Verbindungsproblemen), sollte das Zertifikat nicht akzeptiert werden. Jede Akzeptanz eines solchen Zertifikats erfolgt auf Risiko der vertrauenden Stellen.

4.9.11 Andere verfügbare Formen der Widerrufsanzeige

Keine Bestimmungen.

4.9.12 Besondere Anforderungen bei kompromitierter Schlüsselerneuerung

Keine Bestimmungen.

4.9.13 Umstände für eine Aussetzung

Die Aussetzung ist eine temporäre Aufhebung der Zertifikatsgültigkeit. Sie kann bei Verdacht des Eintritts eines der unter Kapitel 4.9.1 genannten Gründe genutzt werden. Im Gegensatz zu einem Widerruf kann eine Aussetzung innerhalb einer festgelegten Frist auch wieder aufgehoben werden.

4.9.14 Wer kann eine Aussetzung beantragen?

Die befugten Personen für eine Aussetzung sind:

- die betreffende signierende Person oder eine andere Person, die das Passwort für den Widerruf kennt
- bei Verwendung eines Organisationsnamens eine vertretungsbefugte Person der Organisation
- die Zertifizierungsstelle
- die Aufsichtsstelle

Die Aufhebung einer Aussetzung ist jener Person möglich, die das anlässlich der Aussetzung vereinbarte Aussetzungsaufhebungspasswort bzw. das Widerrufspasswort kennt.

4.9.15 Verfahren für Aussetzungsanträge

Die Aussetzung erfolgt wie ein Widerruf mit der Ausnahme, dass ein Antrag nicht elektronisch eingebracht werden kann. Im Rahmen einer Aussetzung muss ein mindestens vierstelliges Passwort festgelegt werden, mit dem die Aussetzung wieder aufgehoben werden kann. Der Widerrufsdienst trägt dieses Aussetzungsaufhebungspasswort in eine Datenbank ein. Das Aussetzungsaufhebungspasswort unterscheidet sich vom Aussetzungs- und Widerrufspasswort und dient zur Berechtigungsprüfung für die Aufhebung der Aussetzung. Wenn die Aussetzung aufgehoben wurde und die Zertifikate dieser Karte zu einem späteren Zeitpunkt nochmals ausgesetzt werden, ist anlässlich der neuerlichen Aussetzung auch ein neues Aussetzungsaufhebungspasswort zu wählen.

Innerhalb der Aussetzungsfrist kann die Aussetzung des Zertifikats wieder aufgehoben werden. Dazu muss die Aufhebung der Aussetzung beim Widerrufsdienst beantragt werden. Für die Authentifizierung muss das Aussetzungsaufhebungspasswort, das anlässlich der Bekanntgabe der Aussetzung gewählt und dem Widerrufsdienst mitgeteilt wurde, oder das Widerrufspasswort angegeben werden. Sollten diese Passwörter nicht bekannt sein, so kann die Aussetzung nicht aufgehoben werden. Weitere benötigte Daten sind die Zertifikats- bzw. Kartennummer oder die Signaturvertragsnummer.

4.9.16 Begrenzung der Aussetzungsdauer

Nach spätestens zehn Tagen wird eine Aussetzung durch die Zertifizierungsstelle in einen Widerruf umgewandelt. Die Aussetzung kann bis 23:00 Uhr des neunten auf den Tag der Aussetzung folgenden Tages wieder aufgehoben werden, sonst wird sie durch A-Trust in einen Widerruf umgewandelt.

4.10 Zertifikatsstatusdienstleistungen

4.10.1 Betriebliche Merkmale

Zertifikatsstatusinformationen können über CRL und OCSP abgerufen werden. Abgelaufene Zertifikate bleiben in der CRL mit der Erweiterung ExpiredCertsOnCRL.

4.10.2 Verfügbarkeit der Dienste

A-Trust setzt Maßnahmen, um die Verfügbarkeit der Dienste so hoch als möglich zu halten.

4.10.3 Optionale Merkmale

Keine Bestimmungen.

4.11 Vertragsende

Das Vertragsende eines Signaturvertrags erfolgt durch Widerruf oder Ablauf der Zertifikatslaufzeit.

4.12 Schlüsselhinterlegung und -wiederherstellung

4.12.1 Schlüsselhinterlegung und -wiederherstellung Richtlinien und Praktiken

Nicht zutreffend.

4.12.2 Session key encapsulation und -wiederherstellung Richtlinien und Praktiken

Nicht zutreffend.

5 Management, betriebliche und physische Kontrollen

5.1 Physische Sicherheitskontrollen

5.1.1 Lage und Standortaufbau

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

Dienstleistung	**Adresse**
Firmensitz	A-Trust GmbH Landstrasser Hauptstrasse 1b A-1030 Wien
Registrierung, Widerrufsdienst	Die Registrierungsstellen und der Widerrufsdienst sind auf der Web-Seite der A-Trust GmbH veröffentlicht.
Hochsicherheits- rechenzentren	Nessus GmbH Fernkorngasse 10/2/1 A-1100 Wien Ausfallsrechenzentrum: Nessus GmbH Karmarschgasse 23-25 A-1100 Wien

Tabelle 3: Örtlichkeiten

5.1.2 Zutrittsmanagement

Der Zugang zu allen technischen Komponenten im Rechenzentrum ist nur durch einen von der A-Trust eingerichteten Berechtigungsmechanismus möglich. Die Zugangskontrollen sind dem 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 Strom und Klimatisierung

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 Brandschutz

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 Aufbewahrung von Datenträgern

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 Abfallentsorgung

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 Ausfallsicherheit

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 Verfahrenskontrollen

5.2.1 Rollen

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
Sicherheitsbeauftragte	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

Rolle	Funktion
Sicherheitsbeauftragte	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 Ansprechperson für sicherheitsrelevante Fragen Beaufsichtigung der Einhaltung der im CPS festgelegten Vorgehensweisen
Sicherheits-systemadministration	Zutritt in die Hochsicherheitszone Beaufsichtigung von Systemadministration und Systemoperation
Revocation Center Agent (RCA), Mitarbeitende im Widerrufsdienst	Ansprechperson für die Zertifikatsinhabenden hinsichtlich der Annahme von Anträgen für Widerruf und Aussetzung
Registration Officer (RO), Mitarbeitende der Registrierungsstelle	Entgegennahme von Zertifikatsanträgen Identifikation von Zertifikatswerbenden im Rahmen der Registrierung Belehrung der Zertifikatsinhabenden

Tabelle 5: Sicherheitskritische Funktionen

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

Tabelle 6: Sonstige Funktionen

5.2.2 Anzahl an Personen pro Aufgabe

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 Zertifikatswerbenden	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-systemadministration	Nein	Nein
Austausch von Hardware-Komponenten	Sicherheits-systemadministration (2x)	Ja	Ja
Austausch von Software-Komponenten	Sicherheits-systemadministration (2x)	Ja	Ja
Überprüfung von Protokolldateien auf verdächtige Vorkommnisse	Systemadministration	Nein	Nein
Überprüfung der Protokolldateien auf Manipulation	Systemadministration	Nein	Nein
Anfertigung eines Backups der Protokolldateien und Lagerung desselben	Sicherheits-systemadministration (2x)	Ja	Ja
Qualitätsprüfung der verwendeten Schlüssellängen und Parameter zur Schlüsselerzeugung	SO	Nein	Nein

Tätigkeit	Personen	Vier-augen-prinzip	Hoch-sicher-heit
Wartung oder Austausch eines kryptographischen Moduls	SO, SO	Ja	Ja

Tabelle 7: Anzahl erforderlicher Personen

5.2.3 Identifikation und Authentikation pro Rolle

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

5.2.4 Rollentrennung

Beauftragte für Interne Revision sowie Beauftragte für Datenschutz dürfen keine weitere sicherheitsrelevante Rolle innehaben.

5.3 Personalkontrollen

Die genauen Bestimmungen für Personalkontrollen (Qualifikationen, Schulungen, Jobrotationshäufigkeit etc.) befinden sich in dem zugehörigen CPS.

5.4 Audit Protokollierungsverfahren

5.4.1 Arten zu protokollierender Ereignisse

Zur Protokollierung von Ereignissen werden Datum und Uhrzeit sowie gegebenenfalls die verantwortliche Person 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)
- 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

Folgende Transaktionstypen sind insbesondere aufzuzeichnen:

- Zertifizierungsanträge
- Schlüsselerzeugungen
- Zertifikatserstellungen
- Veröffentlichung von Zertifikaten und Widerrufslisten
- Aussetzungs- und Widerrufanträge
- Ausgeführte Aussetzungen und Widerrufe
- Schlüsselwechsel

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

- Bestätigung des Kartenerhalts durch die signierende Person
- Bestätigung der Unterrichtung gem. Art. 24 (2) lit d [eIDAS]
- das Einverständnis der signierenden Person mit den Allgemeinen Geschäftsbedingungen und den Entgeltbestimmungen
- Änderungen an bescheinigten Umständen

5.4.2 Häufigkeit der Protokollbearbeitung

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.

5.4.3 Aufbewahrungsfrist des Auditprotokolls

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.

5.4.4 Schutz des Auditprotokolls

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.

5.4.5 Verfahren zur Auditprotokollsicherung

A-Trust erstellt stündlich Backups der Audit-Protokolle und täglich vollständige Backups. Die Backups werden in das jeweils andere Rechenzentrum übertragen.

5.4.6 Schwachstellenanalyse

Keine Bestimmungen.

5.5 Schlüsselwechsel

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 **??** 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 angekündigt. Die Gültigkeitsdauer der Zertifikate ist Kapitel 6.3.2 zu entnehmen.

Die Signaturempfangenden erhalten das neue Zertifikat über den Verzeichnisdienst. Sie können über die Zertifizierungskette die Gültigkeit des Zertifikats überprüfen. Um sich von der Authentizität des Zertifikats der Root-CA zu überzeugen hat die signierende Person die Möglichkeit der Abfrage auf der A-Trust Homepage veröffentlichten Fingerprints des öffentlichen Schlüssels.

Mit einem Schlüsselwechsel verliert der alte Schlüssel seine aktive Gültigkeit. Das heißt 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

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 oben genannten Richtlinien durchgeführt, die sich aber in folgenden Punkten von einem regulären Wechsel unterscheidet:

- Eine rechtzeitige Information der signierenden Personen über den Schlüsselwechsel ist bei einem unmittelbaren Widerruf nicht möglich. Die signierenden Personen 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 signierenden Personen 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.

6 Technische Sicherheitskontrollen

6.1 Generierung und Installation von Schlüsselpaaren

6.1.1 Erzeugung von Schlüsselpaaren

- Für mobile Zertifikate:

  Die Schlüssel werden in einer sicheren Signatur- und Siegelerstellungseinheit erzeugt und nur in verschlüsselter Form gespeichert. Die Signatur- und Siegelerstellungseinheit wurde gemäß Artikel 30 bzw. Artikel 39 [eIDAS] von einer Konformitätsbewertungsstelle zertifiziert.

- Für kartenbasierte Signaturzertifikate:

  Die Schlüssel werden im Hochsicherheitsbereich des kartenherstellenden Unternehmens aufgebracht. Ein Zertifikat für das Signaturschlüsselpaar wird noch nicht erstellt. Dies geschieht erst im Zuge des Registrierungsprozesses, indem die signierende Person zuverlässig identifiziert und authentifiziert wird.

6.1.2 Übergabe des privaten Schlüssels an Nutzende

- Für mobile Zerifikate:

  Der private Signaturschlüssel verläßt die sichere Signaturerstellungseinheit im Rechenzentrum des Zertifizierungsdiensteanbieters nie.

- Für kartenbasierte Signaturzertifikate:

  Der private Signaturschlüssel wird in der Signaturkarte der signierenden Person zur Verfügung gestellt. Ein Auslesen des privaten Signaturschlüssels aus der Chipkarte ist nicht möglich.

6.1.3 Übergabe des öffentlichen Schlüssels an die Zertifikatsausstellenden

Nicht zutreffend.

6.1.4 Übergabe des öffentlichen Schlüssels der CA an vertrauende Stellen

Die Zertifikate der Root-CAs und Intermediate-CAs werden in einem Verzeichnis im Internet, sowie auf der A-Trust Website veröffentlicht.

6.1.5 Schlüssellängen

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

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

Tabelle 8: CA-Schlüssellängen

Nutzenden-Schlüssellänge	$\geq$ RSA 4096
Nutzenden-Schlüssellänge	$\geq$ NIST P-256
Hash-Algorithmus	$\geq$ SHA-256

Tabelle 9: Nutzenden-Schlüssellängen

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

6.1.6 Erzeugung von Parametern für öffentliche Schlüssel und Qualitätsprüfung

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 für prime256v1 gem. [ANSI X9.62].

Die beauftragte Person 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 Schlüsselverwendungszwecke (gemäß X.509 v3 key usage field)

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

Die Root-CA besitzt ein selbst signiertes Zertifikat, in welchem im Attribut 'keyUsage' folgende Bits gesetzt sind:

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

Folgende Bits werden für die Verwendung der Intermediate Schlüssel gesetzt:

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

Folgende Bits werden für den Schlüssel der signierenden Person gesetzt:

- nonRepudiation
- digitalSignature

6.2 Schutz privater Schlüssel und technische Kontrollen kryptographischer Module

6.2.1 Normen und Kontrollen kryptographischer Module

Als kryptografische Module werden gemäß [eIDAS] bescheinigte QSEEs eingesetzt.

6.2.2 Privater Schlüssel (n aus m) Mehrpersonenkontrolle

Es gilt, dass für die Aktivierung des Schlüssels der Root-CA oder einer Intermediate-CA ein Mehrpersonenprinzip (siehe 5.2.1) erforderlich ist. Eine einzelne Person darf nicht über die Mittel verfügen, einen dieser privaten Schlüssel zu nutzen.

6.2.3 Privater Schlüsselhinterlegung

Private Schlüssel können nicht hinterlegt werden. Dies gilt sowohl für die Schlüssel der Intermediate-CAs als auch für Signaturschlüssel von signierende Personen.

6.2.4 Sicherung des privaten Schlüssels

Sicherungen privater Schlüssel werden nicht angefertigt bis auf die in Kapitel 6.2.6 angeführte Vorgangsweise.

6.2.5 Archivierung des privaten Schlüssels

Eine Archivierung privater Schlüssel findet nicht statt.

6.2.6 Übertragung des privaten Schlüssels von oder in ein kryptographisches Modul

Private Schlüssel können in ein anderes kryptographisches Modul exportiert werden. Hierbei wird sichergestellt, dass der private Schlüssel außerhalb des kryptographischen Moduls nur in verschlüsselter Form existiert.

6.2.7 Speicherung des privaten Schlüssels in einem kryptographischen Modul

Die privaten Schlüssel der Root-CAs sowie der Intermediate-CAs 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.

Schlüssel der Endnutzenden:

- Für kartenbasierte Zertifikate:

  Die Schlüssel der signierenden Personen werden auf einer von einer Konformitätsbewertungsstelle nach Art 30 [eIDAS] bescheinigten Smartcard, welche eine sichere Signaturerstellungseinheit darstellt und die Erzeugung und Speicherung der Signaturerstellungsdaten ermöglicht.

- Für mobile Zertifikate:

  Die Schlüssel der signierenden Personen werden auf einer von einer Konformitätsbewertungsstelle nach Art 30 [eIDAS] bescheinigten QSEE welche die Erzeugung und Speicherung der Signaturerstellungsdaten ermöglicht.

- Für a.sign premium timestamping (Zeitstempel):

  Der private Schlüssel der Zeitstempel-Zertifikate wird in einem kryptographischen Sicherheitsmodul gem. [ETSI 319 421] erzeugt. Der private Schlüssel wird von der Zertifizierungsstelle verwaltet.

6.2.8 Aktivierungsverfahren des privaten Schlüssels

Die Nutzung bzw. Aktivierung der privaten Schlüssel der Root-CAs sowie Intermediate-CAs ist durch eine Multifaktor-Authentifikation des Sicherheitspersonals gesichert.

6.2.9 Deaktivierungsverfahren des privaten Schlüssels

Wird ein Hardware Security Modul deaktiviert, so führt dies automatisch zur Deaktivierung aller in ihm enthaltenen privaten Schlüssel. Die privaten Schlüssel der signierenden Personen werden deaktiviert, wenn die vorgegebene Anzahl von Fehlversuchen bei der Signaturauslösung (mobile Zertifikate) bzw. der PIN Eingabe (Karten) überschritten wird und bei der Kartenlösung keine Deblockierung (mehr) durch einen PUK erfolgen kann.

6.2.10 Verfahren zum Zerstören des privaten Schlüssels

Zum Zerstören der privaten Schlüssel der CAs ist ausschließlich Sicherheitspersonal (siehe 5.2.1) befugt. Die Durchführung erfolgt gemäß den Vorgaben des QSEE Herstellers.

6.2.11 Bewertung des kryptographischen Moduls

Siehe Kapitel 6.2.1

6.3 Sonstige Askpekte der Schlüsselpaarverwaltung

6.3.1 Archivierung öffentlicher Schlüssel

Die öffentlichen Schlüssel werden gemäß **??** archiviert.

6.3.2 Zertifikats- und Schlüsselpaar Nutzungszeiträume

Für die Zertifikate gelten die folgenden maximalen Gültigkeitsdauern:

Zertifikatstyp	Gültigkeitsdauer
Root-CA	20 Jahre
Zertifizierungsstellen	20 Jahre
Zertifikatsinhabende	5 Jahre

Tabelle 10: 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 Aktivierungsdaten

Die genauen Bestimmungen zu Aktivierungsdaten (Erzeugung, Installation, Schutz etc.) befinden sich in dem zugehörigen CPS

6.5 Computer-Sicherheitskontrollen

6.5.1 Spezifische technische Anforderungen an die Computersicherheit

A-Trust verschlüsselt die gesamte Kommunikation zwischen den CAs, den Clients und Systemen. Die gesamte Hardware ist gemäß der Best Practices der Branche geschützt, einschließlich Benutzerauthentifizierung, Virenschutz, lokaler Firewall und regelmäßiger Sicherheitsupdates. Der gesamte Zugriff auf die für die Zertifikatsausstellung verwendete Client-Software wird durch eine Multi-Faktor-Authentifizierung über eine Smartcard beschränkt.

6.5.2 Bewertung der Computersicherheit

Keine Bestimmungen.

6.6 Lebenszyklus technischer Kontrollen

6.6.1 Systementwicklungskontrollen

Die Systementwicklung erfolgt ausschließlich intern und unter Verwendung sicherer Coding Guidelines, die auf bewährten Industriestandards beruhen. Bevor das System im Rechenzentrum eingesetzt wird, werden strenge Tests am Testsystem durchgeführt.

6.6.2 Sicherheitsmanagementkontrollen

Die Sicherheitsmanagementkontrollen sind auf die A-Trust Sicherheitsvorschriften abgestimmt. Im Einklang mit den Vorschriften für das Sicherheitsmanagement, aber nicht darauf beschränkt, dürfen Updates für die CA-Systeme nur von zwei Sicherheitsbeauftragten durchgeführt werden.

6.6.3 Lebenszyklus der Sicherheitskontrollen

Keine Bestimmungen.

6.7 Network Security Kontrollen

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.

Alle HSMs auf welchen private Schlüssel gespeichert sind, werden in einem separaten Netzwerksegment betrieben, auf welches nur über eine Firewall zugegriffen werden kann. Firewalls werden nach dem deny all Prinzip betrieben, dies bedeutet, dass nur benötigte Ports geöffnet werden.

6.8 Zeitstempel

Zeitstempel werden verwendet, um die genaue Zeit in Zertifikaten, Sperrlisten und Protokolldateien anzugeben. Die Serverzeit wird mindestens einmal pro Stunde mit Hilfe des Network Time Protocol aktualisiert, wobei vertrauenswürdige Zeitserver verwendet werden, darunter die offizielle Zeit des österreichischen Bundesamts für Eich- und Vermessungswesen.

7 Zertifikats-, CRL- und OCSP Profile

7.1 Zertifikatsprofile

A-Trust verwendet nicht-sequentielle Zertifikatsseriennummern mit zumindest 64 Bit Entropie. Die Zertifikatsseriennummer ist somit eindeutig innerhalb der A-Trust Zertifikatsinfrastruktur.

7.1.1 Versionsnummer(n)

v3(2): Die Versionsnummer wird auf '2' gesetzt,um ein X.509 Zertifikat der Version 3 anzuzeigen

7.1.2 Zertifikatserweiterungen

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

Erweiterung	**Zertifikatstyp**		**Klassifikation**	
	Root	**Interm.**	**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
extkeyUsage	Nein	Ja		X
Private Erweiterungen				
authorityInfoAccess	Nein	Ja		X

Tabelle 11: Erweiterungen (CA-Zertifikate)

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

Erweiterung	Im Zertifikat vorhanden	Klassifikation	
		kritisch	nicht kritisch
Standarderweiterung			
authorityKeyIdentifier	Ja		X
subjectKeyIdentifier	Ja		X
keyUsage	Ja	X	
extkeyUsage	optional		X
certificatePolicies	Ja		X
basicConstraints	Ja		X
CRLDistributionPoints	Ja (*nicht bei Einmalzertifikaten*)		X
subjectAltName	optional		X
id-kp-timeStamping	nur bei a.sign premium timestamping	X	
esi4-qtstStatement-1	nur bei a.sign premium timestamping		X
Private Erweiterung			
authorityInfoAccess	Ja		X
qc-Statement	Ja (*nicht bei a.sign premium timestamping*)		X
1.2.40.0.10.1.1.1	optional (*nicht bei a.sign premium timestamping*)		X

Tabelle 12: Erweiterungen Endnutzendenzertifikate

Erweiterung subjectDirectoryAttributes enthält bei a.sign premium sowie a.sign premium mobile und EU-Identity Zertifikaten optional das Geburtsdatum der signierenden Person, verpflichtend bei Minderjährigen.

Optional können a.sign premium sowie a.sign premium mobile Zertifikate eine Zertifikatserweiterung enthalten, welche die signierende Person als Personal einer Behörde ausweist (Behördenkennzeichen - OID 1.2.40.0.10.1.1.1). In dieser Erweiterung kann weiters optional auch ein Verwaltungsbezeichner enthalten sein, der die Zugehörigkeit zu einer Organisationseinheit der öffentlichen Verwaltung angibt.

7.1.3 Algorithmus object identifiers

CA Zertifikate : SHA-256RSA

Zertifikate der Zertifikatsinhabenden : SHA-256RSA oder ecdsa-with-SHA256

SHA-256RSA wird wie folgt codiert: [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11]

ecdsa-with-SHA256 wird wie folgt codiert: [iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2]

RSASSA-PSS wird wie folgt codiert: [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsassa-pss(10)]

7.1.4 Namensformen

Folgende Abkürzungen werden in den Namensformen erwähnt:

- CN (CommonName)
- OU (OrganizationalUnit)
- O (Organization)
- C (Country)
- -nn bezeichnet die Generation der Zertifikate

Für CA Root Zertifikate:

- CN = A-Trust-Root-nn (optional -ECC)
- O = A-Trust GmbH
- C = AT

Für CA Intermediate Zertifikate:

In das Feld C wird stets AT geschrieben. Das Feld O enthält immer A-Trust GmbH. Das Feld CN ist immer gleich und enthält den Namen des Dienstes, welcher wie folgt ist:

a.sign premium a-sign-premium-sig-nn

a.sign premium seal a-sign-premium-seal-nn

a.sign premium mobile a-sign-premium-mobile-nn

EU-Identity Mobile EU-Identity-Mobile-nn

a.sign premium mobile seal a-sign-premium-mobile-seal-nn

a.sign premium timestamping a-sign-premium-timestamping-nn

a.sign premium once a-sign-premium-once-nn

Für Zertifikatsinhabende:

Nachfolgend die Erläuterungen zu den im Zertifikat enthaltenen Informationen

1. a.sign premium, a.sign premium mobile und EU-Identity Mobile, a.sign premium once:
   - C = CountryName (Ländercode jenes Landes, welches die Verifikationsdaten ausgestellt hat)
   - T = Title (geprüfter Titel)
   - SN = SurName (geprüfter Zuname)
   - G = GivenName (geprüfter Vorname)
   - CN = CommonName (entweder Vorname + Zuname oder Pseudonym)
     - Titel, Zuname, Vorname entfallen bei Verwendung eines Pseudonyms
   - SERIALNUMBER = SerialNumber (Seriennummer)
   - O = OrganizationName
   - OU = OrganizationalUnit-Name
   - optional: Berufskennung für Ziviltechniker
2. a.sign premium seal, a.sign premium mobile seal
   - C = CountryName (Ländercode jenes Landes, des Firmensitzes gemäß des europäischen Unternehmensregisters)
   - O = OrganizationName (Firmenname laut Firmenbuch)
   - CN = CommonName (Firmenname laut Firmenbuch)
   - SERIALNUMBER = SerialNumber (Seriennummer)
   - organizationIdentifier (eindeutig zuordenbare Organisationsnummer, z.B. aus dem europäischen Firmenbuch)
3. a.sign premium timestamping (Zeitstempelzertifikat)
   - C = CountryName (optional)
   - CN = CommonName (Timestamp issuing certificate)

7.1.5 Namenseinschränkungen

Keine Bestimmungen.

7.1.6 Certificate policy object identifier

- a.sign premium:
  - OID 0.4.0.194112.1.2 gem. [ETSI 319 411]
    itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policyidentifiers(1) qcp-natural-qscd (2)
  - OID 1.2.040.0.17.1.20 gem. gültiger Certificate Policy
    1.2.040.0.17 (A-Trust).1 (Policy).99 (a.sign premium qualified)
    vormals: 1.2.040.0.17 (A-Trust).1 (Policy).11 (a.sign premium)
- a.sign premium seal:
  - OID 0.4.0.194112.1.3 gem. [ETSI 319 411]
    itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal-qscd (3)
  - OID 1.2.040.0.17.1.11.1 gem. gültiger Certificate Policy
    1.2.040.0.17 (A-Trust).1 (Policy).99 (a.sign premium qualified)
    vormals: 1.2.040.0.17 (A-Trust).1 (Policy).11.1 (a.sign premium seal)
- a.sign premium mobile:
  - OID 0.4.0.194112.1.2 gem. [ETSI 319 411]
    itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policyidentifiers(1) qcp-natural-qscd (2)
  - OID 1.2.040.0.17.1.11 gem. gültiger Certificate Policy
    1.2.040.0.17 (A-Trust).1 (Policy).99 (a.sign premium qualified)
    vormals: 1.2.040.0.17 (A-Trust).1 (Policy).20 (a.sign premium mobile)
- EU-Idenitity mobile:
  - OID 0.4.0.194112.1.2 gem. [ETSI 319 411]
    itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policyidentifiers(1) qcp-natural-qscd (2)
  - OID 1.2.040.0.17.1.23 gem. gültiger Certificate Policy
    1.2.040.0.17 (A-Trust).1 (Policy).99 (a.sign premium qualified)
    vormals: 1.2.040.0.17 (A-Trust).1 (Policy).23 (EU-Identity mobile)
- a.sign premium mobile seal:
  - OID 0.4.0.194112.1.3 gem. [ETSI 319 411]
    itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal-qscd (3)

  - OID 1.2.040.0.17.1.11 gem. gültiger Certificate Policy
    1.2.040.0.17 (A-Trust).1 (Policy).99 (a.sign premium qualified)
    vormals: 1.2.040.0.17 (A-Trust).1 (Policy).20 (a.sign premium mobile)

- a.sign premium timestamping:
  - OID 1.2.040.0.17.1.21 gem. gültiger Certificate Policy
    1.2.040.0.17 (A-Trust).1 (Policy).99 (a.sign premium qualified)
    vormals: 1.2.040.0.17 (A-Trust).1 (Policy).21 (a.sign premium timestamping)

- a.sign premium once:
  - OID 0.4.0.194112.1.2 gem. [ETSI 319 411]
    itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policyidentifiers(1) qcp-natural-qscd (2)
  - OID 1.2.040.0.17.1.XX gem. gültiger Certificate Policy
    1.2.040.0.17 (A-Trust).1 (Policy).99 (a.sign premium qualified)

7.1.7 Anwendung der Policy Constraints extension

Keine Bestimmungen.

7.1.8 Policy-qualifier Syntax und Semantik

Keine Bestimmungen.

7.1.9 Semantik für die Verfahrensweise bei kritischen Certificate Policy Extension

Keine Bestimmungen.

7.2 CRL Profile

7.2.1 Versionsnummer(n)

v2(1): Wert '1' entspricht einer X.509, Version 2 Sperrliste.

Sperrlisten sind mit dem Algorithmus SHA-256RSA:[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11] signiert.

7.2.2 CRL und CRL Entry Erweiterungen

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, widerrufene oder gesperrte Zertifikate nicht von der Sperrliste entfernt werden, ist in der Sperrliste die Erweiterung ExpiredCertsOnCRL auf das Erstellungsdatum der CA gesetzt.

Die CRL Erweiterung CRLDistributionPoints wird verwendet, da A-Trust Partitioned CRLs verwendet.

7.3 OCSP Profile

7.3.1 Versionsnummer(n)

Die OCSP responder sind mit der Version 1 des RFC 6960 [RFC6960] konform.

7.3.2 OCSP Erweiterungen

Es wird die OCSP Erweiterung id-pkix-ocsp-nocheck geführt.

8 Compliance und Audits

8.1 Häufigkeit und Umstände der Audits

Externe Audits werden mindestens einmal im Jahr von einer unabhängigen Stelle durchgeführt. Darüber hinaus werden jährlich interne Revisionen und Audits durchgeführt. Audits werden stichprobenhaft in allen A-Trust Liegenschaften und Registrierungsstellen durchgeführt.

8.2 Identität der auditierenden Person

Die Konformitätsbewertungsstelle bestimmt die auditierende Person 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. Die für interne Revision zuständige Person ist entsprechend des internen Rollenkonzepts auszuwählen.

8.3 Beziehung zwischen auditierender Person und zu untersuchender Partei

Auditierende Personen handeln immer weisungsungebunden sowie unabhängig.

8.4 Auditierte Bereiche

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

Die Audits werden nach dem folgenden Schema durchgeführt:
ETSI EN 319 411-1 v1.2.2 [ETSI 319 411].

Die internen Audits umfassen Stichproben von mindestens drei Prozent aller seit dem letzten Audit ausgestellten Zertifikate. Sie werden mit Schwerpunkt auf die Integrität des Prozesses überprüft. Dieses Audit wird dokumentiert.

8.5 Handlungen bei unzureichendem Ergebnis

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

- Der gemeldete Mangel wird analysiert
- Ein Plan zur Behebung des Mangels wird ausgearbeitet
- Der Plan wird gemeinsam mit den auditierenden Personen überprüft
- Dieser Plan wird Schritt für Schritt befolgt, was Folgendes beinhalten kann:
  - Kontaktaufnahme mit den betroffenen Stellen
  - Widerruf der betroffenen Zertifikate

8.6 Bekanntgabe der Ergebnisse

A-Trust veröffentlicht die Ergebnisse externer Prüfungen. Interne Audits werden ausschließlich für befugte externe Prüfende und die österreichische Regulierungsbehörde für Rundfunk und Telekommunikation zur Verfügung gestellt.

9 Sonstige finanzielle und rechtliche Regelungen

9.1 Änderungen

9.1.1 Verfahren zur Änderung

Das CPS bzw. CP wird einmal im Jahr überprüft. Änderungen werden durch die Veröffentlichung der neuesten Version im Online-Repository wirksam. Aktualisierungen ersetzen alle angegebenen oder widersprüchlichen Bestimmungen der referenzierten Version des CP bzw. des CPS.

9.1.2 Benachrichtigungsmechanismus und -frist

Überarbeitungen des CP bzw. CPS werden auf der A-Trust Website veröffentlicht.

9.1.3 Umstände, unter denen die OID geändert werden müssen

A-Trust ist allein verantwortlich für die Entscheidung, ob eine Änderung des CP bzw. des CPS eine OID-Änderung zur Folge hat.

A Appendix

A.1 Referenzierte Dokumente

Literatur

[AGB] Allgemeine Geschäftsbedingungen (AGB) A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH (A-Trust) für qualifizierte und fortgeschrittene Zertifikate Version 7.3

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

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

[eIDAS] 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

[ETSI TS 119 495] Electronic Signatures and Infrastructures (ESI)

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

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

[EV-GL] Guidelines For The Issuance And Management of Extended Validation Certificates 1.6.2, 2017

[PSD2] DELEGIERTE VERORDNUNG (EU) 2018/389 DER KOMMISSION vom 27. November 2017

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

[RFC6960] RFC6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP

[RFC6484] RFC 6484, Certificate Policy (CP) for the Resource Public Key Infrastructure (RPKI)

[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