



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**  
**Zertifizierungsrichtlinie**  
**(Certificate Practice Statement)**  
**für qualifizierte Zertifikate**  
**EU-Identity mobile**

Version: 1.1.4  
Datum: 13.02.2023

# Inhaltsverzeichnis

<b>1</b>	<b>Einführung</b>	<b>12</b>
1.1	Überblick . . . . .	12
1.2	Dokumentidentifikation . . . . .	12
1.3	Zertifizierungsinfrastruktur und Anwendungsbereich . . . . .	12
1.3.1	Zertifizierungsstellen . . . . .	12
1.3.2	Registrierungsstellen . . . . .	13
1.3.3	Widerrufsdienst . . . . .	13
1.3.4	Anwendende . . . . .	13
1.3.5	Anwendbarkeit . . . . .	13
1.3.6	Zertifizierungshierarchie . . . . .	13
1.3.7	A-Trust Verzeichnisbaum . . . . .	13
1.4	Ansprechpartner und Kontaktstellen . . . . .	14
1.4.1	Organisation zur Verwaltung dieses Dokuments . . . . .	14
1.4.2	Kontaktinformation . . . . .	14
1.4.3	Verantwortung für die Anerkennung anderer Anwendungsvorgaben (Policies) . . . . .	15
<b>2</b>	<b>Generelle Bestimmungen</b>	<b>16</b>
2.1	Verpflichtungen . . . . .	16
2.1.1	Verpflichtungen des Zertifizierungsdiensteanbieters . . . . .	16
2.1.2	Verpflichtungen der Registrierungsstellen . . . . .	16
2.1.3	Verpflichtungen der Zertifikatsinhabenden . . . . .	17
2.1.4	Verpflichtungen der Signaturempfangenden . . . . .	18
2.1.5	Funktionen der Verzeichnisdienste . . . . .	19
2.2	Haftung . . . . .	19
2.2.1	Haftung der Zertifizierungsstelle . . . . .	19
2.2.2	Haftung der Registrierungsstelle . . . . .	20
2.3	Finanzielle Verantwortung . . . . .	20
2.3.1	Schadensersatz der beteiligten Parteien . . . . .	20
2.3.2	Treuhänderische Beziehungen . . . . .	20

2.3.3	Administrative Prozesse . . . . .	20
2.4	Auslegung und (gerichtliche) Durchsetzung . . . . .	20
2.4.1	Zugrunde liegende Gesetzesbestimmungen . . . . .	20
2.4.2	Trennbarkeit der Bestimmungen, Fortbestehen von Ansprüchen, Fusion, Kündigung . . . . .	21
2.4.3	Schlichtungsverfahren . . . . .	21
2.5	Gebühren . . . . .	21
2.5.1	Ausgabe und Erneuerung von Zertifikaten . . . . .	21
2.5.2	Abrufen von Zertifikaten . . . . .	21
2.5.3	Aussetzung oder Widerruf von Zertifikaten . . . . .	21
2.5.4	Abrufen von Statusinformationen . . . . .	21
2.5.5	Gebühren für weitere Dienste . . . . .	22
2.5.6	Richtlinien von Entgelten . . . . .	22
2.6	Bekanntmachung und Verzeichnisdienste . . . . .	22
2.6.1	Web-Seiten und Verzeichnisse . . . . .	22
2.6.2	Widerruf . . . . .	22
2.6.3	A-Trust Stammzertifikat . . . . .	22
2.6.4	A-Trust Dienste-Zertifikat . . . . .	23
2.6.5	Widerrufsinformationen . . . . .	23
2.6.6	Suche nach einem Zertifikat . . . . .	24
2.6.7	Veröffentlichung von Informationen der Zertifizierungsstelle . . . . .	24
2.6.8	Frequenz der Aktualisierung . . . . .	25
2.6.9	Zugriffskontrollen . . . . .	25
2.6.10	Verzeichnisse . . . . .	26
2.7	Interne Prüfung (Audit) . . . . .	26
2.7.1	Häufigkeit des Audits . . . . .	26
2.7.2	Identität bzw. Anforderungen an die auditierende Person . . . . .	26
2.7.3	Beziehungen zwischen Auditor und zu untersuchender Partei . . . . .	26
2.7.4	Aspekte des Audits . . . . .	26
2.7.5	Handlungen nach unzureichendem Ergebnis . . . . .	27
2.7.6	Bekanntgabe der Ergebnisse . . . . .	27

2.8	Vertraulichkeit	27
2.8.1	Vertraulich eingestufte Informationen	27
2.8.2	Nicht vertraulich eingestufte Informationen	27
2.8.3	Offenlegung von Informationen zu Zertifikatswiderruf	27
2.8.4	Offenbarung an Behörden im Rahmen gesetzlicher Pflichten	28
2.8.5	Offenbarung im Rahmen zivilrechtlicher Auskunftspflichten	28
2.8.6	Weitere Gründe zur Freigabe von vertraulichen Informationen	28
2.9	Urheberrechte und Eigentumsrechte	28
<b>3</b>	<b>Identifizierung und Authentifikation</b>	<b>29</b>
3.1	Erstregistrierung	29
3.1.1	Namenstypen	29
3.1.2	Anforderungen an Namen	29
3.1.3	Regeln zur Interpretation unterschiedlicher Namensformen	29
3.1.4	Eindeutigkeit der Namen	30
3.1.5	Anspruch auf Namen und Beilegung von Streitigkeiten	30
3.1.6	Anerkennung, Bestätigung und Bedeutung von Warenzeichen	30
3.1.7	Methode zum Beweis des Besitzes des geheimen Schlüssels	30
3.1.8	Authentisierung von Organisationen	30
3.1.9	Authentisierung von Individuen	30
3.2	Erneute Registrierung/Rezertifizierung	31
3.3	Erneute Registrierung nach Widerruf	32
3.4	Aussetzungs- und Widerrufs Antrag	32
<b>4</b>	<b>Betriebliche Anforderungen</b>	<b>33</b>
4.1	Antrag auf Ausstellung von Zertifikaten	33
4.2	Ausstellung von Zertifikaten	33
4.2.1	Persönliche Ausstellung	33
4.2.2	Online-Ausstellung	33
4.2.3	Selbst-Aktivierung	33
4.3	Akzeptanz von Zertifikaten	34
4.4	Aussetzung und Widerruf von Zertifikaten	34

4.4.1	Gründe für einen Widerruf . . . . .	34
4.4.2	Wer kann einen Widerruf anordnen . . . . .	34
4.4.3	Prozedur für einen Widerrufs Antrag . . . . .	35
4.4.4	Frist bis zur Bekanntgabe des Widerrufs . . . . .	35
4.4.5	Gründe für eine Aussetzung . . . . .	36
4.4.6	Wer kann eine Aussetzung anordnen und aufheben . . . . .	36
4.4.7	Prozedur für einen Aussetzungsantrag . . . . .	36
4.4.8	Aufhebung der Aussetzung . . . . .	36
4.4.9	Bekanntgabe der Aussetzung bzw. Aufhebung . . . . .	37
4.4.10	Grenzen einer Aussetzungsperiode . . . . .	37
4.4.11	Aktualisierungsintervalle der Widerrufsliste . . . . .	37
4.4.12	Anforderungen an die Überprüfung mittels Widerrufslisten . . . . .	37
4.4.13	Weitere Möglichkeiten zur online Statusabfrage . . . . .	38
4.4.14	Anforderungen an die online Statusabfrage . . . . .	38
4.4.15	Weitere Verfahren zur Bekanntgabe von Widerrufen . . . . .	38
4.4.16	Anforderungen an die Überprüfung der weiteren Verfahren zur Bekanntgabe von Widerrufen . . . . .	38
4.4.17	Spezielle Verfahren bei Kompromittierung von privaten Schlüsseln . . . . .	38
4.5	Protokollierung sicherheitsrelevanter Ereignisse . . . . .	38
4.5.1	Protokollierte Ereignisse . . . . .	38
4.5.2	Intervalle der Überprüfung der Protokolldateien . . . . .	39
4.5.3	Aufbewahrungszeitraum der Protokolldateien . . . . .	40
4.5.4	Schutz der Protokolldateien . . . . .	40
4.5.5	Protokollierungssystem (intern / extern) . . . . .	40
4.5.6	Benachrichtigung beim Auftreten sicherheitskritischer Ereignisse . . . . .	40
4.5.7	Bewertungen zur Angreifbarkeit . . . . .	40
4.6	Archivierung . . . . .	40
4.6.1	Archivierte Daten . . . . .	40
4.6.2	Aufbewahrungszeiten . . . . .	41
4.6.3	Schutzvorkehrungen . . . . .	41
4.6.4	Anforderungen, die Daten mit Echtzeitangaben zu versehen . . . . .	41

4.6.5	System zur Erfassung der Archivierungsdaten (intern / extern) . . .	42
4.6.6	Prozeduren zum Abrufen und Überprüfen von Daten . . . . .	42
4.7	Schlüsselwechsel von CA- und Root-Schlüssel . . . . .	42
4.8	Kompromittierung und Notfallplan . . . . .	43
4.8.1	Rechner, Software und/oder Daten sind korrumpiert . . . . .	43
4.8.2	Widerruf von Zertifikaten zu Zertifizierungsstellen- und Dienst- Schlüsseln . . . . .	43
4.8.3	Widerruf von Zertifikaten der Dienste . . . . .	44
4.8.4	Widerruf des Zertifikats der Zertifizierungsstelle . . . . .	44
4.8.5	Schlüsselwechsel . . . . .	44
4.8.6	Schlüsselkompromittierung bzw. Verdacht auf Schlüsselkompromit- tierung . . . . .	45
4.8.7	Sicherheitsvorkehrungen nach Katastrophen . . . . .	45
4.9	Einstellung der Tätigkeit der Zertifizierungsstelle . . . . .	46
<b>5</b>	<b>Physische, verfahrensorientierte und personelle Sicherheitsvorkehrun- gen</b>	<b>47</b>
5.1	Physische Sicherheitsvorkehrungen . . . . .	47
5.1.1	Standort und örtliche Gegebenheiten . . . . .	47
5.1.2	Zugangskontrollen . . . . .	47
5.1.3	Stromversorgung und Klimaanlage . . . . .	48
5.1.4	Wasserschäden . . . . .	48
5.1.5	Feuer . . . . .	48
5.1.6	Datenträger . . . . .	48
5.1.7	Müllentsorgung . . . . .	48
5.1.8	Redundante Auslegung . . . . .	49
5.2	Verfahrensorientierte Sicherheitsvorkehrungen . . . . .	49
5.2.1	Funktionen der A-Trust . . . . .	50
5.2.2	Sicherheitskritische Funktionen . . . . .	51
5.2.3	Sonstige (nicht sicherheitskritische) Funktionen . . . . .	51
5.2.4	Anzahl erforderlicher Personen für sicherheitsrelevante Tätigkeiten	52
5.2.5	Identifikation der Rollen . . . . .	53

5.3	Personelle Sicherheitsvorkehrungen	53
5.3.1	Anforderungen an das Personal	53
5.3.2	Überprüfung des Personals	53
5.3.3	Anforderungen an die Schulung	54
5.3.4	Anforderungen und Häufigkeit von Schulungswiederholungen	54
5.3.5	Ablauf und Frequenz der Job Rotation	54
5.3.6	Sanktionen für unautorisierte Handlungen	54
5.3.7	Anforderungen an Vertragsvereinbarungen mit dem Personal	55
5.3.8	An das Personal auszuhändigende Dokumente	55
<b>6</b>	<b>Technische Sicherheitsvorkehrungen</b>	<b>56</b>
6.1	Schlüsselgenerierung und Installation	56
6.1.1	Schlüsselgenerierung	56
6.1.1.1	Schlüssel der signierenden Personen	56
6.1.1.2	Schlüssel der Zertifizierungsstelle	56
6.1.2	Zurverfügungstellung privater Schlüssel	56
6.1.3	Zurverfügungstellung öffentlicher Schlüssel an Zertifikatsausstellende	56
6.1.4	Zurverfügungstellung öffentlicher Schlüssel von der Zertifizierungsstelle an die signierenden Personen	56
6.1.5	Schlüssellängen	57
6.1.6	Parameter zur Schlüsselerzeugung	57
6.1.7	Qualitätsprüfung der Parameter	57
6.1.8	Hardware/Software Schlüsselerzeugung	57
6.1.9	Verwendungszweck der Schlüssel (nach X.509 v3 usage Feld)	57
6.1.9.1	Verwendung der Schlüssel der Root-CA	58
6.1.9.2	Verwendung der Schlüssel der Zertifizierungsstellen	58
6.1.9.3	Verwendung des Schlüssels der signierenden Person	58
6.2	Schutz der privaten Schlüssel	58
6.2.1	Standards des kryptografischen Moduls	58
6.2.1.1	Schlüssel der Zertifizierungsstelle	58
6.2.1.2	Schlüssel der signierenden Personen	59

6.2.2	Aufteilung privater Schlüssel auf mehrere Personen . . . . .	59
6.2.2.1	Schlüssel der Zertifizierungsstelle . . . . .	59
6.2.2.2	Schlüssel der signierenden Personen . . . . .	59
6.2.3	Hinterlegung privater Schlüssel . . . . .	59
6.2.4	Backup privater Schlüssel . . . . .	59
6.2.5	Archivierung privater Schlüssel . . . . .	59
6.2.6	Einbringung privater Schlüssel in das kryptografische Modul . . . . .	59
6.2.6.1	Schlüssel der Zertifizierungsstelle . . . . .	60
6.2.6.2	Schlüssel der signierenden Personen . . . . .	60
6.2.7	Methode zur Nutzung privater Schlüssel . . . . .	60
6.2.8	Methode zur Deaktivierung privater Schlüssel . . . . .	60
6.2.9	Methode zur Vernichtung privater Schlüssel . . . . .	60
6.3	Verwendungszeitraum öffentlicher und privater Schlüssel . . . . .	60
6.4	Aktivierungsdaten . . . . .	61
6.4.1	Erzeugung und Installation der Aktivierungsdaten (PINs) . . . . .	61
6.4.1.1	Aktivierungsdaten für Schlüssel der Zertifizierungsstelle . . . . .	61
6.4.1.2	Aktivierungsdaten für Schlüssel der signierenden Personen . . . . .	61
6.4.2	Schutz der Aktivierungsdaten . . . . .	61
6.4.2.1	Aktivierungsdaten für Schlüssel der Zertifizierungsstelle . . . . .	61
6.4.2.2	Aktivierungsdaten für Schlüssel der signierende Personen . . . . .	61
6.4.3	Weitere Aspekte zu den Aktivierungsdaten . . . . .	62
6.5	Computer Sicherheitsbestimmungen . . . . .	62
6.5.1	Spezifische Sicherheitsanforderungen an die Computer . . . . .	62
6.5.2	Bewertung der Computersicherheit . . . . .	62
6.6	Life-Cycle der Sicherheitsvorkehrungen . . . . .	62
6.6.1	Systementwicklung . . . . .	62
6.6.2	Sicherheitsmanagement . . . . .	62
6.6.3	Bewertung . . . . .	63
6.7	Vorkehrungen zur Netzwerksicherheit . . . . .	63
6.8	Vorkehrungen zur Wartung (Analyse) des kryptografischen Moduls . . . . .	63



<b>7</b>	<b>Profile von Zertifikaten und Widerrufslisten</b>	<b>64</b>
7.1	Zertifikatsprofile . . . . .	64
7.1.1	CA-Zertifikate . . . . .	64
7.1.2	Zertifikate der Zertifikatsinhabenden . . . . .	65
7.1.3	Erweiterungen (certificate extensions) . . . . .	66
7.1.4	Identifikation der Policy . . . . .	67
7.1.5	Semantik für die Verfahrensweise bei Certificate Policy Extension . . . . .	67
7.2	Profil der Widerrufsliste . . . . .	67
7.2.1	Versionsnummern . . . . .	67
7.2.2	CRL und CRL Entry Extensions . . . . .	67
<b>8</b>	<b>Nachsignieren</b>	<b>69</b>
<b>9</b>	<b>Administration dieser Spezifikation</b>	<b>70</b>
9.1	Prozeduren zur Änderung dieses Dokuments . . . . .	70
9.2	Verfahren zur Publizierung und Bekanntgabe . . . . .	70
9.3	Genehmigung und Eignung einer Zertifizierungsrichtlinie . . . . .	70
<b>A</b>	<b>Anhang</b>	<b>71</b>
A.1	Begriffe und Abkürzungen . . . . .	71
A.2	Referenzdokumente . . . . .	75

Rev	Verfasst von	Änderungen
1.0.0	RS	initiale Version.
1.1.0	RS, PT	eIDAS Anpassungen
1.1.1	RS	Adresse, Logo
1.1.2	RS, PT RS, PT	Adresse Rechenzentrum QSCD Referenz (6.1.1) Kontaktdaten ExpiredCertsOnCRL (7.2.1) Gültigkeitsprüfung vor Anwendung (6.2.7)
1.1.3 (intern)	IH	Generation 08 Genderneutrale Sprache Empfehlungen Auditor Firmenname (7.1.1) Schlüssellängen (7.1.1)
1.1.4	IH	Verwendung Schlüssel Zertifizierungsstellen: digitalSignature

Tabelle 1: Dokumentenhistorie

## Tabellenverzeichnis

1	Dokumentenhistorie . . . . .	9
2	Homepage und Verzeichnisse . . . . .	22
3	Örtlichkeiten . . . . .	47
4	Funktionen der A-Trust . . . . .	50
5	Sicherheitskritische Funktionen . . . . .	51
6	Sonstige Funktionen . . . . .	51
7	Anzahl erforderlicher Personen . . . . .	53
8	Schlüssellängen . . . . .	57
9	Gültigkeitsdauer von Zertifikaten . . . . .	61
10	Profil für CA-Zertifikat . . . . .	64
11	Profil für EU-Identity mobile Zertifikate . . . . .	65
12	Erweiterungen (CA-Zertifikate) . . . . .	66
13	Erweiterungen EU-Identity mobile Zertifikat . . . . .	66

## Abbildungsverzeichnis

1	Zertifikathierarchie . . . . .	14
2	A-Trust Verzeichnisbaum . . . . .	14

# 1 Einführung

## 1.1 Überblick

Das Ziel der vorliegenden Zertifizierungsrichtlinie besteht darin, die Umsetzung der Ausgabe, Administration und Anwendung von EU-Identity mobile Zertifikaten derart festzulegen, dass eine sichere und zuverlässige Durchführung der angebotenen EU-Identity mobile Zertifizierungsdienstleistungen sowie der Anwendung der ausgegebenen Zertifikate gewährleistet ist.

Eine Zertifizierungsrichtlinie gibt Auskunft über die Praktiken der Zertifizierungsstellen zur Ausstellung von EU-Identity mobile Zertifikaten. Sie dient dazu, die Praktiken intern zu fixieren und den Anwendenden die Vorgehensweise der Zertifizierungsstelle zu erläutern. Somit können sich die Anwendenden ein Bild von den vorhandenen Sicherheitsmaßstäben machen.

## 1.2 Dokumentidentifikation

Name der Richtlinie: A-Trust Zertifizierungsrichtlinie (Certification Practice Statement) für qualifizierte Zertifikate EU-Identity mobile  
Version: 1.1.4 / 13.02.2023  
Object Identifier: 1.2.040.0.17 (A-Trust) .2 (CPS) .23 (EU-Identity mobile )  
.1.1.4 (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, die die Schlüssel der signierenden Personen sowie die Widerruflisten für Zertifikate signiert. A-Trust stellt qualifizierte Zertifikate (gemäß [eIDAS-VO]) aus, die auf einer sicheren Signaturerstellungseinheit basieren.

Darüber hinaus existiert eine Root-Zertifizierungsstelle, welche das Zertifikat und die Widerruflisten für die Zertifizierungsstellen signiert. Anwender:innenzertifikate 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-VO] und ist in die österreichische Vertrauensliste im Sinne des Artikels 22 [eIDAS-VO] 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 Anwender:innendaten und die Weiterleitung von Informationen an die übergeordnete Zertifizierungsstelle. Die Ausstellung des Zertifikats erfolgt auf Veranlassung der Registrierungsstelle.

### 1.3.3 Widerrufsdienst

Die signierenden Personen können sich telefonisch bzw. über Fax an den Widerrufsdienst wenden und das Zertifikat widerrufen lassen. Wollen sie eine Aussetzung durchführen oder aufheben lassen, so kann dies mittels eines Telefonats oder durch eine von A-Trust zur Verfügung gestellte Webanwendung erfolgen.

### 1.3.4 Anwendende

Unter "Anwendende" sind die Personen zusammengefasst, die EU-Identity mobile Zertifikate von A-Trust erhalten (Zertifikatsinhabende bzw. signierende Personen), oder welche EU-Identity mobile Zertifikate nutzen bzw. den Zertifikatsangaben vertrauen (Signatur-empfangende).

### 1.3.5 Anwendbarkeit

Dieses Dokument ist relevant für die Zertifizierungsstelle, die angeschlossenen Registrierungsstellen, Dienstleistungen der Zertifizierungs- und Registrierungsstelle und die Anwendenden. Der zertifizierte Signaturschlüssel der signierenden Person darf ausschließlich für das Erstellen von Signaturen 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 Artikel 3 Z. 12 [eIDAS-VO].

### 1.3.6 Zertifizierungshierarchie

Abbildung [1.3.6](#) zeigt eine schematische Darstellung der Zertifikatshierarchie.

### 1.3.7 A-Trust Verzeichnisbaum

Eine schematische Darstellung des Verzeichnisbaums ist in [Abbildung 2](#) zu finden.

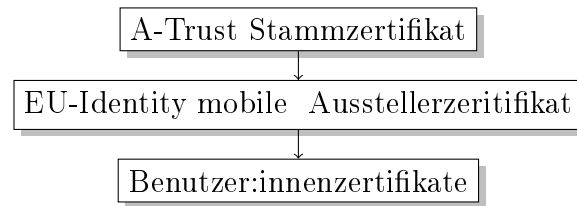


Abbildung 1: Zertifikatshierarchie

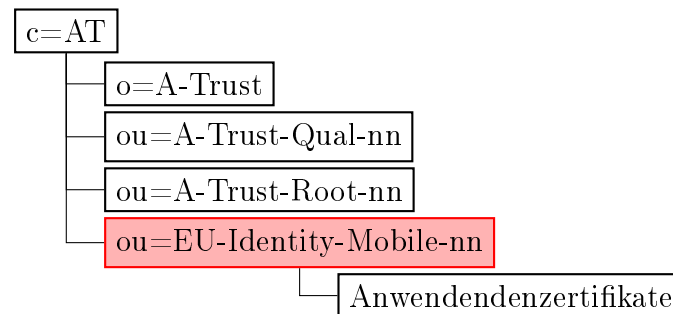


Abbildung 2: A-Trust Verzeichnisbaum

Das Zertifikat des Schlüssels A-Trust-Qual-nn (bzw. 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-Qual-nn werden die (ZwischenInstanz-) CA-Zertifikate und die zugehörigen CRLs signiert.

Die Zertifikate der Zertifikatsinhabenden von EU-Identity mobile Zertifikaten und die zugehörigen CRLs werden mit dem CA-Schlüssel EU-Identity-Mobile-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 EU-Identity mobile 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.
- In ausgewählten Registrierungsstellen von A-Trust und
- Auf schriftliche Anfrage

Geschäftszeiten A-Trust: 8–18 Uhr

### **1.4.3 Verantwortung 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 Zertifikate für signierende Personen werden im Einklang mit der Zertifizierungsrichtlinie erstellt und können ausgesetzt, widerrufen oder verlängert werden.
- Die Zertifizierungsstelle arbeitet im Einklang mit dem der Aufsichtsbehörde vorgelegten Sicherheits- und Zertifizierungskonzept.
- Die Zertifizierungsstelle beschäftigt ausschließlich qualifiziertes Personal.
- Die Zertifizierungsstelle kommt ihrer Informationspflicht gegenüber signierenden Personen und Aufsichtsbehörden nach.
- Die Zertifizierungsstelle sorgt durch geeignete Maßnahmen (technisch, organisatorisch, infrastrukturell und personell) für den Schutz des privaten Schlüssels der Zertifizierungsstelle.
- Der Einsatz des privaten Schlüssels der Zertifizierungsstelle erfolgt ausschließlich zum Signieren der Zertifikate der signierenden Personen und zum Signieren der Widerrufsinformationen.
- Die Zertifizierungsstelle veröffentlicht alle ausgestellten Zertifikate (sofern die Ausstellung von der signierenden Person gewünscht ist). Bei Aussetzung eines Zertifikats wird die betroffene signierende Person benachrichtigt. Ein nicht veröffentlichtes Zertifikat wird bei einer Aussetzung oder einem Widerruf in die Widerrufsliste aufgenommen.
- A-Trust hat insbesondere die Verpflichtung, eine Liste der für eine qualifizierte Signaturerstellung und -prüfung zu verwendenden Komponenten und Verfahren zur erstellen und aktuell zu halten und diese den signierenden Personen und Signaturempfangenden von Zertifikaten jederzeit zugänglich zu machen.

#### 2.1.2 Verpflichtungen der Registrierungsstellen

Die Registrierungsstellen der A-Trust befolgen die Regelungen der Zertifizierungsrichtlinie, die sich insbesondere auf die folgenden Aspekte erstreckt:

- Die Registrierungsstellen arbeiten im Einklang mit dem der Aufsichtsbehörde vorgelegten Sicherheits- und Zertifizierungskonzept.
- Die Registrierungsstellen stellen die Einhaltung der Identifikations- und Authentifikationsmechanismen sicher, die in der Zertifizierungsrichtlinie beschrieben sind.
- Die Registrierungsstellen beschäftigen Personal mit angemessener Qualifikation.
- Das EU-Identity mobile Zertifikat wird im Zuge des Registrierungsprozesses, nach erfolgreicher Identifikation durch die Registrierungsstelle, ausgestellt. A-Trust stellt der signierenden Person insbesondere folgende Dokumente elektronisch zur Verfügung:
  - die Anwendungsvorgabe (siehe [[Policy](#)]),
  - die gegenständliche Zertifizierungsrichtlinie für EU-Identity mobile ,
  - die Allgemeinen Geschäftsbestimmungen [[AGB](#)],
  - die Unterrichtung für die signierende Person,
  - die Entgeltbestimmungen
  - den Antrag/Signaturvertrag
  - die A-Trust Liste der empfohlenen Komponenten und Verfahren.

### 2.1.3 Verpflichtungen der Zertifikatsinhabenden

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

- Die signierenden Personen verpflichten sich die in [2.1.2](#) genannten Dokumente anzuerkennen.
- Die signierende Person ist für die Richtigkeit der Angaben verantwortlich, die sie bei der Registrierung macht und wirkt gemäß den in der Zertifizierungsrichtlinie angegebenen Verfahren zur Identitätsfeststellung und Authentifikation mit.
- Die signierende Person ist verpflichtet, ihre für das Auslösen der Signatur nötigen Komponenten angemessen zu schützen. Dies umfasst insbesondere das Verhindern des Zugriffs durch unautorisierte Personen auf die SIM-Karte/Mobiltelefon und das von der signierenden Person gewählte Signaturpasswort.
- Falls nötig initiiert die signierende Person unverzüglich die Aussetzung oder den Widerruf ihres Zertifikats. Wird die Aussetzung nicht nach einem vorgegebenen Zeitraum aufgehoben, so erfolgt automatisch ein Widerruf des Zertifikats.

- Die signierende Person setzt ihr Zertifikat nur zu dem im Zertifikat angegebenen Zweck ein. Maßgeblich hierfür sind die zum Zeitpunkt der Ausstellung des Zertifikats gültige Zertifizierungsrichtlinie und die zugehörigen Anwendungsvorgaben (Policy).
- Die signierende Person ist sich bewusst, dass A-Trust eine Liste mit empfohlenen technischen Komponenten und Verfahren für die Erstellung von qualifizierten Signaturen bereitstellt und dass bei der Verwendung anderer Komponenten und Verfahren A-Trust für Schäden, die durch diese verursacht werden, nicht haftbar gemacht werden kann.
- Die signierende Person muss weiters dafür Sorge tragen, dass sowohl auf dem PC-Arbeitsplatz, als auch auf dem eingesetzten Mobiltelefon, auf welchem die qualifizierte Signatur erstellt/ausgelöst wird, kein unbefugt eingebrachter Programmcode zur Anwendung kommt. Dazu sind folgende Vorgaben von A-Trust eingehalten werden:
  - Die signierende Person muss alle notwendigen technischen und organisatorischen Maßnahmen ergreifen, um unbefugten Zugriff auf dem PC-Arbeitsplatz sowie dem Mobiltelefon und die darauf befindlichen Programmcodes zu verhindern.
  - A-Trust verpflichtet die signierende Person sich an die Empfehlungen der herstellenden Unternehmen des verwendeten Betriebssystems sowie der anderen Software-Produkte, die installiert wurden, zu halten (z.B. Virens Scanner, Firewall).
  - Die signierende Person hat die notwendigen Maßnahmen zu ergreifen, um sich gegen Phishing zu schützen (Kontrolle der SSL Verbindung bzw. des zugrunde liegenden Zertifikats)

#### 2.1.4 Verpflichtungen der Signaturempfangenden

Den Zertifikatsnutzenden von EU-Identity mobile Zertifikaten (Signaturempfangenden) wird empfohlen, vor der Akzeptanz folgende Prüfungen durchzuführen:

- Prüfung der digitale Signatur.
- Prüfung der der Gültigkeit des Zertifikats.
- ob das Zertifikat zweckgemäß (d.h. für die Signaturerstellung) eingesetzt wurde.

Wenn der Überprüfer eines Zertifikats eine qualifizierte Signaturprüfung durchzuführen beabsichtigt, dann empfiehlt ihm A-Trust die Verwendung der für eine qualifizierte Überprüfung einer Signatur empfohlenen Komponenten und Verfahren.

### 2.1.5 Funktionen der Verzeichnisdienste

Folgende Entitäten werden in regelmäßige Abständen im Verzeichnisdienst veröffentlicht:

- die ausgestellten Zertifikate, die zur Veröffentlichung freigegeben sind
- Listen der ausgesetzten Zertifikate
- widerrufenen Zertifikate.

Diese Listen werden in regelmäßigen Abständen, wie in dieser Zertifizierungsrichtlinie vereinbart, aktualisiert und hochverfügbar gehalten.

## 2.2 Haftung

A-Trust haftet als Ausstellerin von qualifizierten Zertifikaten gem. den Bestimmungen des Artikels 13 [eIDAS-VO].

### 2.2.1 Haftung der Zertifizierungsstelle

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

- die Signaturerstellungsdaten und die ihnen zugeordneten Signaturprüfdaten einander bei der Verwendung der von der A-Trust bereitgestellten oder als geeignet bezeichneten Produkte und Verfahren in komplementärer Weise entsprechen,
- das Zertifikat bei Vorliegen der Voraussetzungen unverzüglich widerrufen wird und ein Widerrufsdienst verfügbar ist,
- die Anforderungen des Artikels 24 [eIDAS-VO] und die Anforderungen des Anhangs II [eIDAS-VO] für die Erzeugung und Speicherung von Signaturerstellungsdaten 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 einer qualifizierten Signatur, wenn diese unter Einhaltung aller von A-Trust der signierenden Person auferlegten Vorschriften und unter Verwendung der empfohlenen Komponenten und Verfahren erstellt wurde. A-Trust kann in den Zertifikaten eine Haftungsobergrenze 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 Mitarbeitenden 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**

A-Trust haftet für die ordnungsgemäße Tätigkeit der Registrierungsstellen wie in der Anwendungsvorgabe [Policy] und dieser Zertifizierungsrichtlinie beschrieben.

## **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 der signierenden Person geschlossene Vertrag unterliegt dem österreichischen Recht und richtet sich nach [eIDAS-VO], [SVG] und [SVV]. Im Verhältnis zu ausländischen signierenden Personen wird die Anwendung des UN-Kaufrechts ausdrücklich ausgeschlossen.

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

### **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. Der signierenden Person entsteht dadurch kein besonderes Kündigungsrecht, solange Dritte die Rechten und Pflichten des Vertrags erfüllen.

Änderungen der Vertragsdokumente werden der signierenden Person vor der Zertifikatserneuerung schriftlich mitgeteilt. Ändert A-Trust die Allgemeinen Geschäftsbedingungen, so hat die signierende Person jederzeit die Möglichkeit zu kündigen. Widerspricht die signierende Person 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. Alle Entgelte, die nicht im Grundentgelt enthalten sind, werden mit der Nutzung der jeweiligen Leistung fällig.

### **2.5.1 Ausgabe und Erneuerung von Zertifikaten**

Die aktuell gültige Regelung findet sich in den Entgeltbestimmungen.

### **2.5.2 Abrufen von Zertifikaten**

Der Abruf von EU-Identity mobile Zertifikaten über den Verzeichnisdienst der A-Trust ist kostenfrei.

### **2.5.3 Aussetzung oder Widerruf von Zertifikaten**

Die Aussetzung oder der Widerruf eines Zertifikats ist kostenfrei.

### **2.5.4 Abrufen von Statusinformationen**

Der Zugang zu Widerrufslisten und Statusinformationen ist kostenfrei.

### 2.5.5 Gebühren für weitere Dienste

A-Trust stellt Hilfestellung in Form eines gebührenpflichtigen Call Centers bereit.

### 2.5.6 Richtlinien von Entgelten

Die signierende Person hat keinen Anspruch auf die Rückerstattung von Entgelten. Im Falle einer Kündigung des Vertrags hat die signierende Person das Entgelt bis zum Ende der Abrechnungsperiode zu entrichten.

## 2.6 Bekanntmachung und Verzeichnisdienste

### 2.6.1 Web-Seiten und Verzeichnisse

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

Bekanntmachungen:	<a href="http://www.a-trust.at/">http://www.a-trust.at/</a>
Verzeichnisdienst:	<a href="ldap://ldap.a-trust.at/">ldap://ldap.a-trust.at/</a>
Widerrufsliste:	<a href="ldap://ldap.a-trust.at/">ldap://ldap.a-trust.at/</a> und <a href="http://crl.a-trust.at">http://crl.a-trust.at</a>
OCSP:	<a href="http://ocsp.a-trust.at/ocsp">http://ocsp.a-trust.at/ocsp</a>

Tabelle 2: Homepage und Verzeichnisse

Die Liste der empfohlenen Komponenten und Verfahren für die sichere Signaturerstellung und -prüfung stellt A-Trust auf ihrer Homepage unter

- <http://www.a-trust.at/downloads> zur Verfügung.

### 2.6.2 Widerruf

Die Informationen betreffend den Widerrufsdienst und die Durchführung von Widerrufen stellt A-Trust unter

- <http://www.a-trust.at/widerruf> zur Verfügung.

### 2.6.3 A-Trust Stammzertifikat

Die Stammzertifikate sind 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> oder

- <http://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 des Stammzertifikats kann auf sichere Weise über https erfolgen, ebenso wie auch über http. Über den entsprechenden Menüpunkt auf der A-Trust Homepage oder direkt unter dem oben angeführten Link kann der Download des Stammzertifikats erfolgen.

#### 2.6.4 A-Trust Dienste-Zertifikat

Das benötigte CA-Zertifikat ist unter

- <https://www.a-trust.at/certs/EU-Identity-Mobile-nnx.crt> oder
- <http://www.a-trust.at/certs/EU-Identity-Mobile-nnx.crt>

zu finden (die Bedeutung von -nnx ist in Abschnitt 2.6.3 beschrieben) und kann von hier heruntergeladen werden.

#### 2.6.5 Widerrufsinformationen

Verteilungspunkt für die Widerrufslisten (CRLs)

Ab der CA Version 08:

- <http://crl.a-trust.at/crl/EU-Identity-Mobile-nn/CRLmm>

Vor der CA Version 08:

- <http://crl.a-trust.at/crl/EU-Identity-Mobile-nn>

Optional kann die Sperrliste auch über LDAP abgefragt werden.

Ab der CA-Version 08:

- <ldap://ldap.a-trust.at/cn=CRLmm,ou=EU-Identity-Mobile-nn,o=A-Trust,c=AT?certificaterevocationlist?base?objectclass=eidcertificationauthority>



Es werden ab CA Generation 08 Partitioned CRLs eingesetzt. Hier gibt *mm* an, in welcher Sperrliste die Sperrinformationen des betroffenen Zertifikates stehen.

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

- `ldap://ldap.a-trust.at/ou=EU-Identity-Mobile-mm,o=A-Trust,c=AT?certificaterevocationlist?base?objectclass=eidcertificationauthority`

Verteilungspunkt für die Widerrufslisten für CA-Version 01:

- `ldap://ldap.a-trust.at/ou=EU-Identity-Mobile-mm,o=A-Trust,c=AT?certificaterevocationlist`

### 2.6.6 Suche nach einem Zertifikat

Für die Suche nach einem bestimmten Zertifikat (Suchkriterien sind wahlweise Nachname, Vorname, CIN oder Pseudonym) 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/verzeichnisdienst):

- <https://www.a-trust.at/verzeichnisdienst>

### 2.6.7 Veröffentlichung von Informationen der Zertifizierungsstelle

Die Zertifizierungsstelle veröffentlicht:

- die jeweils gültige Zertifizierungsrichtlinie (Certificate Practice Statement),
- die jeweils gültige Anwendungsvorgabe (Certificate Policy),
- die gültige Entgeltbestimmung,
- die Zertifikate der Zertifizierungsstelle,
- die Allgemeinen Geschäftsbedingungen [[AGB](#)],
- die Unterrichtung für den signierende Person,
- die Information über die zu verwendenden Komponenten und Verfahren,
- eine Liste mit Kontaktstellen bzw. Registrierungsstellen.
- auf ihrer Homepage [www.a-trust.at](http://www.a-trust.at).

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

Die signierenden Personen 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
- Einstellung der Tätigkeit der Zertifizierungsstelle

A-Trust stellt alle Informationen wie folgt bereit:

- Auf der Web-Seite [www.a-trust.at](http://www.a-trust.at)
- Optional: in einem elektronischen Newsletter per E-Mail
- Optional: Briefsendung
- Optional: Printmedien oder TV

Informationen, die nur einzelne signierende Personen betreffen, werden diesen direkt zugestellt. Ist eine Vielzahl von signierenden Personen 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.

### **2.6.8 Frequenz der Aktualisierung**

Eine Aktualisierung der Zertifizierungsrichtlinie erfolgt gemäß Kapitel 9.

### **2.6.9 Zugriffskontrollen**

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.

### 2.6.10 Verzeichnisse

Folgende Verzeichnisse werden von der Zertifizierungsstelle unterhalten:

- Ein öffentlich zugängliches Verzeichnis; es enthält die Zertifikate der Zertifizierungsstellen, die Widerrufslisten und die Zertifikate der signierenden Personen.
- 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 die auditierende Person

Die Aufsichtsbehörde 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.

### 2.7.3 Beziehungen zwischen Auditor und zu untersuchender Partei

Die Aufsichtsbehörde bestimmt die auditierende Person, die in ihrem Auftrag die Überprüfung vornimmt.

### 2.7.4 Aspekte des Audits

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.

### **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**

Die A-Trust verpflichtet sich, die von der signierenden Person bekannt gegebenen Daten vertraulich im Sinne der DSGVO zu behandeln. Die Daten, die bei der Anmeldung angegeben werden, werden ausschließlich für die Dienstleistungen der Zertifizierungsstelle benutzt. Bei der Verwendung von Pseudonymen durch die signierende Person muss A-Trust den ihr bekannten korrekten und vollständigen Namen der signierenden Person an berechnete Dritte weitergeben.

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 Zertifikatswiderrief**

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 der signierenden Person nur auf Verlangen an laut [SVG] berechnigte Gerichte bzw. andere Behörden weiter (gemäß Artikel 24 (2) Lit. h [eIDAS-VO] iVm Art 9 (2) [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.

Die Eigentumsrechte der folgenden Schlüssel liegen bei der signierenden Person:

- Privater Schlüssel der signierenden Person sowie
- Öffentlicher Schlüssel der signierenden Person.

## 3 Identifizierung und Authentifikation

### 3.1 Erstregistrierung

#### 3.1.1 Namenstypen

Qualifizierte EU-Identity mobile Zertifikate enthalten zumindest:

- Name für das EU-Identity mobile Zertifikat: Nachname und Vorname sind erforderlich. Bei Namensteilen welche die Maximallänge des technischen Zertifikatsstandards überschreiten, können diese entsprechend ihrer Reihenfolge entfallen. Im Falle von Standard EU-Identity 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.
- Die Angabe der Meldeadresse ist optional.
- 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 (siehe Kapitel 4.1).

#### 3.1.2 Anforderungen an Namen

Der Name der signierenden Person muss den bei der Registrierung vorliegenden Identitätsdaten entsprechen.

Wird ein Pseudonym verwendet, so muss es wie folgt codiert werden: "Pseudonym: Pseudonymbezeichnung". Auf Wunsch der signierenden Person kann als Firmenpseudonym auch der Name eines Unternehmens (vollständiger Name lt. Firmenbuch oder eindeutige Abkürzung des Unternehmensnamens) in der Form "Organisationsname:Firma" eingetragen werden, sofern die signierende Person, durch Vorlage geeigneter Dokumente (Vollmacht einer vertretungsbefugten Person) darlegen kann, dass sie den Organisationsnamen im Zertifikat verwenden darf.

#### 3.1.3 Regeln zur Interpretation unterschiedlicher Namensformen

Keine Bestimmungen.

### **3.1.4 Eindeutigkeit 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.

### **3.1.5 Anspruch auf Namen und Beilegung von Streitigkeiten**

Keine Bestimmungen.

### **3.1.6 Anerkennung, Bestätigung und Bedeutung von Warenzeichen**

Keine Bestimmungen.

### **3.1.7 Methode zum Beweis des Besitzes des geheimen Schlüssels**

Die signierende Person bestätigt, dass sie berechtigt ist, eine Signatur auszulösen, indem sie einerseits im Besitz des von ihr gewählten Signaturpasswortes ist und sie den Inhalt des Verifikations-Codes, welcher vor jeder Anwendung des privaten Schlüssels an das bei der Registrierung angegebene Mobiltelefon (SIM-Karte oder installierte A-Trust App) gesendet wird, kennt.

### **3.1.8 Authentisierung von Organisationen**

Keine Bestimmungen.

### **3.1.9 Authentisierung von Individuen**

Die Angaben der Antragstellenden werden bei der Ausstellung des Zertifikates in der Registrierungsstelle durch die Registrierungsstelle überprüft. Antragsstellende beweisen deren Identität durch das Vorlegen eines gültigen, amtlichen Lichtbildausweises. Dabei sind die folgenden Ausweise zulässig:

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

Mittels eines RSa Briefs (§ 3 Z 2 [SVV]) wird ein für die Ausstellung der Zertifikate erforderlicher Aktivierungscode an die Meldeadresse der Antragstellenden versendet. Im Rahmen der Zustellung des RSa Briefs ist es notwendig, dass die Antragstellenden ihre Identität durch das Vorlegen eines gültigen, amtlichen Lichtbildausweises beweisen.

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 Artikel 24 (1) [eIDAS-VO] bzw. § 4a [E-GovG] entspricht. Diese Bestätigung wird in elektronischer Form, durch die öffentliche Stelle signiert, vor der Zertifikatsausstellung an A-Trust übermittelt.

Es ist ebenfalls zulässig, dass die signierende Person ein neues qualifiziertes Zertifikat, mittels einer qualifizierten Signatur aktiviert. In diesem Falle ist keine erneute Registrierung / Rezertifizierung erforderlich. Sollten sich personenbezogene Daten geändert haben, muss eine erneute Registrierung / Rezertifizierung erfolgen.

Darüber hinaus können gemäß Artikel 24 (1) [eIDAS-VO] Lit d für die Identifizierung von Individuen auch sonstige Identifizierungsmethoden - deren gleichwertige Sicherheit hinsichtlich der Verlässlichkeit einer persönlichen Identifizierung entspricht - eingesetzt werden. Die gleichwertige Sicherheit muss in diesem Fall durch eine Konformitätsbewertungsstelle bestätigt worden sein.

Nach Maßgabe der technischen Möglichkeiten, kann die Identität auch aus der Ferne mittels elektronischer Identifizierungsmittel festgestellt werden, für die vor der Ausstellung des qualifizierten Zertifikates eine persönliche Anwesenheit gewährleistet war und die die Anforderungen gemäß Artikel 8 [eIDAS-VO] hinsichtlich des Sicherheitsniveaus „Substanziell“ oder „Hoch“ erfüllen (Artikel 24 (1) [eIDAS-VO] Lit b).

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

## 3.2 Erneute Registrierung/Rezertifizierung

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

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

Sollten sich Zertifikatsdaten geändert haben, muss eine erneute Registrierung / Rezertifizierung erfolgen. Werden geänderte Zertifikatsdaten einer signierenden Person von einer öffentlichen Stelle signiert übermittelt, wird der Prozess der Registrierung/Rezertifizierung



automatisiert durchgeführt (§ 4 Abs 4 [E-GovG]).

### 3.3 Erneute Registrierung nach Widerruf

Nach dem Widerruf eines Zertifikates kann die signierende Person ein neues Zertifikat beantragen. Der Vorgang entspricht den Abläufen einer erneuten Registrierung / Rezertifizierung (siehe Abschnitt 3.2).

### 3.4 Aussetzungs- und Widerrufsanspruch

Die signierende Person kann das Zertifikat per Telefon oder Webanwendung aussetzen bzw. eine Aussetzung aufheben lassen und per Telefon oder Fax einen Widerruf veranlassen.

Dazu muss die signierende Person zumindest ihren Namen, Daten des betroffenen Zertifikats (Seriennummer) und das Aussetzungs- und Widerrufspasswort bzw. das Aussetzungsaufhebungspasswort angeben. Sollte das Aussetzungs- und Widerrufspasswort nicht bekannt sein, ist eine Aussetzung (kein Widerruf) mit folgenden Angaben möglich:

- Vollständiger Name,
- Pseudonym (falls verwendet),
- Geburtstag und
- 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.

## 4 Betriebliche Anforderungen

### 4.1 Antrag auf Ausstellung von Zertifikaten

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 EU-Identity mobile 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.

Wenn in einem EU-Identity mobile Zertifikat die Zugehörigkeit zu einer Behörde abgebildet werden soll (Behördenkennzeichen siehe Kapitel [7.1.3](#)), so wird von einer autorisierten Behördenvertretung zusätzlich zum Antrag ein Schreiben an die A-Trust Registrierungsstelle gesandt, das die Rechtmäßigkeit dieser Angabe bestätigt.

### 4.2 Ausstellung von Zertifikaten

#### 4.2.1 Persönliche Ausstellung

Für die Ausstellung der Zertifikate der Antragstellenden werden diese persönlich in einer Registrierungsstelle vorstellig. Registration Officer stellen die Zertifikate aus, wenn

- die Identität der Antragstellenden anhand eines gültigen, amtlichen Lichtbildausweises (zulässige Ausweise siehe Kapitel [3.1.9](#)) überprüft wurde,
- die Antragstellenden unterrichtet wurden und
- die Allgemeinen Geschäftsbedingungen akzeptiert wurden.

#### 4.2.2 Online-Ausstellung

siehe Kapitel [3.1.9](#)

#### 4.2.3 Selbst-Aktivierung

Es gibt die Möglichkeit mittels einer qualifizierten Signatur ein neues Zertifikat zu beantragen. Sollten sich personenbezogene Daten geändert haben, muss eine erneute Registrierung durchgeführt werden.

## 4.3 Akzeptanz von Zertifikaten

Keine Bestimmungen.

## 4.4 Aussetzung und Widerruf von Zertifikaten

EU-Identity mobile Zertifikate können vorübergehend ausgesetzt werden. Diese Aussetzung kann auch in einen endgültigen Widerruf umgewandelt werden. Ebenso ist ein sofortiger und permanenter Widerruf des Zertifikats möglich. Die signierende Person wird von einer erfolgten Aussetzung informiert.

### 4.4.1 Gründe für einen Widerruf

Der Widerruf eines EU-Identity mobile Zertifikats wird erforderlich, wenn

- Angaben im Zertifikat nicht mehr korrekt sind,
- die signierende Person nicht mehr im alleinigen Besitz der Signaturlösedaten 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 oder
- die eingesetzten Algorithmen nicht mehr den Sicherheitserwartungen entsprechen und dadurch eine sichere Anwendung der Signaturlösedaten nicht mehr gegeben wäre.

### 4.4.2 Wer kann einen Widerruf anordnen

Ein Widerruf eines EU-Identity mobile Zertifikats kann angeordnet werden. Durch:

- die betreffende signierende Person oder eine andere Person, die das Passwort für den Widerruf kennt,
- bei Verwendung eines Organisationsnamens als Pseudonym (gemäß [3.1.2](#)) ein Vertretungsbefugter der Organisation,
- die Zertifizierungsstelle selbst.

### 4.4.3 Prozedur für einen Widerrufs Antrag

Ein Widerruf kann durch die signierende Person vorgenommen werden. Dies kann wie folgt geschehen:

- Die signierende Person bzw. die Vertretungsbefugten wenden sich per Telefon an den Widerrufsdienst.
- Die signierende Person bzw. die Vertretungsbefugten veranlassen den Widerruf per Fax.
- Bei Verlust des Passworts für den Widerruf kann keinen Widerruf, sondern nur eine Aussetzung beantragt werden.

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

- **Telefonat:** 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), Kartenummer oder Seriennummer des Zertifikats.
- **Fax:** Ein Widerruf per Fax kann von 0 bis 24 Uhr vorgenommen werden. Das Fax muss das Aussetzungs- und Widerrufs-Passwort sowie die vollständige Seriennummer oder die Kartenummer 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.

### 4.4.4 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

Die befugten Personen für eine Aussetzung sind:

- die signierende Person und
- jede Person, die das Passwort für Aussetzung und Widerruf kennt.

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

#### 4.4.7 Prozedur für einen Aussetzungsantrag

Die Aussetzung erfolgt wie 4.4.3 mit der Ausnahme, dass ein Antrag nicht per Fax eingebracht werden kann.

Im Rahmen einer Aussetzung muss ein mindestens vier-stelliges 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.

#### 4.4.8 Aufhebung der Aussetzung

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. Kartenummer oder die Signaturvertragsnummer.

#### 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

Die Aussetzung kann bis 23:00 Uhr des neunten auf den Tag der Aussetzung folgenden Tags wieder aufgehoben werden, sonst wird sie durch A-Trust in einen Widerruf umgewandelt.

#### 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 Zertifikaten liegt in der Verantwortung der Zertifikatsnutzenden. Der Inhalt eines EU-Identity mobile Zertifikats kann nur dann als authentisch gelten, wenn sich die Zertifikatsnutzenden 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.

Zertifikatsnutzende 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 Internet-Verbindungsprobleme), sollten keine Zertifikate akzeptiert werden. Jede Akzeptanz eines solchen Zertifikats erfolgt auf das Risiko der Zertifikatsnutzenden.

#### **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**

Zertifikatsnutzende 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 technischen Gründen), sollte das Zertifikat nicht akzeptiert werden. Jede Akzeptanz eines solchen Zertifikats erfolgt auf Risiko der Zertifikatsnutzenden.

#### **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**

Bei Eintritt einer der unter Kapitel 4.4.1 genannten Gründe führt die signierende Person eine Aussetzung oder einen Widerruf durch.

### **4.5 Protokollierung sicherheitsrelevanter Ereignisse**

#### **4.5.1 Protokollierte 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), 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 Widerrufsanträge,
  - Ausgeführte Aussetzungen und Widerrufe sowie
  - 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-VO](#)],
- das Einverständnis der signierenden Person 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 Widerruflisten 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 Anwendenden.

### 4.5.7 Bewertungen zur Angreifbarkeit

Keine Bestimmungen.

## 4.6 Archivierung

### 4.6.1 Archivierte Daten

Archiviert werden:

- Persönliche Daten der signierenden Person, die zur Zertifizierung verwendet wurden (Lichtbildausweis),
- Zertifizierungsanträge (Antragstellerformular und Vertrag),
- alle von der Zertifizierungsstelle ausgestellten Zertifikate (Zertifikate der Zertifizierungsstelle und Dienste und Zertifikate der signierenden Personen),

- Aussetzungs- und Widerrufsanträge 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.

Im Zuge einer Onlineaktivierung werden die signierten Identifikationsdaten archiviert. Dies betrifft unter anderem von der Registrierungsstelle signierte Ausweisdaten.

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 Widerruflisten 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 2.6.7) angekündigt. Die Gültigkeitsdauer der Zertifikate ist Kapitel 6.3 zu entnehmen.

Die Signaturempfänger 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. 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 signierenden Personen) 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 signierenden Personen 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 anwendenden Personen 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 signierenden Personen rechtzeitig über den bevorstehenden Widerruf informiert. Ein ungeplanter Widerruf erfordert eine umgehende Benachrichtigung der signierenden Personen. 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 anwendenden Personen 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 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.

#### **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 die sicherheitsbeauftragte Person der Zertifizierungsstelle informiert. Diese ordnet gegebenenfalls einen Widerruf betroffener Zertifikate an. Wichtige Maßnahmen dazu sind:

- Die Anwendenden 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 Anwendenden.

Die sicherheitsbeauftragte Person 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 Sicherheitsvorkehrungen nach Katastrophen**

Die sicherheitsbeauftragte Person 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 Personen 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 und der Inhabenden von gültigen Zertifikaten. Rechtzeitig vor der endgültigen Einstellung der Zertifizierungsstelle werden alle noch gültigen und von der Zertifizierungsstelle ausgestellten Zertifikate widerrufen. Alle von den Widerruf betroffenen Zertifikatsinhabenden 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 Nutzenden 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 GmbH Landstrasser Hauptstrasse 1b A-1030 Wien
Registrierung, Widerrufsdienst	Die Registrierungsstellen und der Widerrufsdienst sind auf der Web-Seite der A-Trust veröffentlicht.
Zertifizierung, Brief-Versand (Antragstellerformular, Aussetzungs- und Widerrufsinformation, PUKs, etc.)	Nessus GmbH Fernkorngasse 10/2/1 A-1100 Wien  Ausfallsrechenzentrum: Nessus GmbH Karmarschgasse 23-25 A-1100 Wien
Kartenproduktion Initialisierung  Zentrale Personalisierung	Austria Card Lamezanstr. 4-8 A-1232 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 Verfahrenorientierte 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

<b>Rolle</b>	<b>Funktion</b>
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

### 5.2.2 Sicherheitskritische Funktionen

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

### 5.2.3 Sonstige (nicht 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

### 5.2.4 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	Vieraugenprinzip	Hochsicherheit
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

Tätigkeit	Personen	Vier- augen- prinzip	Hoch- sicher- heit
Anfertigung eines Backups der Protokolldateien und Lagerung desselben	Sicherheits- systemadministration (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 [SVV] darf im Rahmen der bereitgestellten Signatur- und Zertifizierungsdienste ein qualifizierter VDA nur zuverlässiges Personal beschäftigen. Die Zuverlässigkeit ist jedenfalls bei Personen nicht gegeben, 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 Gesetzes über das Strafregister und die Tilgung gerichtlicher Verurteilungen 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 Mitarbeitenden 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 Mitarbeitenden der Registrierungsstelle und des Widerrufsdienstes als primäre Schnittstelle zum signierende Person besonderer Wert gelegt.

Die Mitarbeitenden 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. ROs haben außerdem Checklisten und Merkblätter zur Verfügung, die sie in standardisierter Weise durch den Registrierungsprozesses durchführen sollen.

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

### **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 DSGVO 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 der signierenden Personen

Die Schlüssel werden in einer sicheren Signaturerstellungseinheit erzeugt und nur in verschlüsselter Form gespeichert. Siehe auch Kapitel 6.2.1. Die Signaturerstellungseinheit wurde gemäß Artikel 30 [eIDAS-VO] von einer Konformitätsbewertungsstelle zertifiziert: <https://www.a-sit.at/downloads/1253>.

##### 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. Die Erzeugung von Schlüsseln in der Zertifizierungsstelle erfolgt immer unter der Aufsicht von zwei befugten A-Trust Mitarbeitenden und muss von der Geschäftsführung der A-Trust angeordnet werden.

#### 6.1.2 Zurverfügungstellung privater Schlüssel

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

#### 6.1.3 Zurverfügungstellung öffentlicher Schlüssel an Zertifikatsausstellende

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

#### 6.1.4 Zurverfügungstellung öffentlicher Schlüssel von der Zertifizierungsstelle an die signierenden Personen

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 in einer Ausgabe der Wiener Zeitung veröffentlicht.

### 6.1.5 Schlüssellängen

Die Schlüssel der Root-CA und aller Zertifizierungsstellen, 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: Schlüssellängen

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

### 6.1.6 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 für prime256v1 gem. [ANSI X9.62].

### 6.1.7 Qualitätsprüfung der Parameter

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.

### 6.1.8 Hardware/Software Schlüsselerzeugung

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

Die Schlüssel der signierenden Personen werden in der sicheren Signaturerstellungseinheit im Rechenzentrum des Zertifizierungsdiensteanbieters erzeugt.

### 6.1.9 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.

#### **6.1.9.1 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 Widerruflisten)

gesetzt sind.

#### **6.1.9.2 Verwendung der Schlüssel der Zertifizierungsstellen**

Folgende Bits werden für die Verwendung der Schlüssel der Zertifizierungsstellen gesetzt:

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

#### **6.1.9.3 Verwendung des Schlüssels der signierenden Person**

Der Schlüssel der signierenden Person dient zur Erstellung einer digitalen Signatur. Deshalb werden die Bits

- nonRepudiation und
- digitalSignature

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 Widerruflisten. Er wird nur in einer gesicherten Umgebung eingesetzt.

Der Schlüssel einer Zertifizierungsstelle dient zur Signatur von Zertifikaten und Widerruflisten. 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 signierenden Personen**

Die Schlüssel der signierenden Personen werden auf einer den Anforderungen entsprechenden sicheren Signaturerstellungseinheit gespeichert. Es handelt sich hierbei um ein von einer Bestätigungsstelle (wie z.B. A-SIT) bescheinigtes System, welche eine sichere Signaturerstellungseinheit darstellt und die Erzeugung und Speicherung der Signaturerstellungsdaten ermöglicht.

## **6.2.2 Aufteilung privater Schlüssel auf mehrere Personen**

### **6.2.2.1 Schlüssel der Zertifizierungsstelle**

Die privaten Schlüssel befinden sich in einem Hardware Security Modul. Für die Aktivierung des Schlüssels der Root-CA oder einer Zertifizierungsstelle ist ein Vieraugenprinzip erforderlich. Eine einzelne Person darf nicht über die Mittel verfügen, einen dieser privaten Schlüssel zu nutzen.

### **6.2.2.2 Schlüssel der signierenden Personen**

Für signierende Personenschlüssel ist ausschließlich die Kontrolle einer einzelnen Person, der signierenden Person, gefordert.

## **6.2.3 Hinterlegung privater Schlüssel**

Private Schlüssel können nicht hinterlegt werden. Dies gilt sowohl für die Schlüssel der Zertifizierungsstelle als auch für Signaturschlüssel von signierenden Personen.

## **6.2.4 Backup privater Schlüssel**

Es gibt keine Backup Möglichkeiten - weder für private Schlüssel der Zertifizierungsstelle noch für Signaturschlüssel von signierenden Personen.

## **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, 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 Anwenderzertifikate.

#### **6.2.6.2 Schlüssel der signierenden Personen**

Die privaten Signaturschlüssel der signierenden Personen werden in einer sicheren Signaturerstellungseinheit im Hochsicherheitsbereich des Zertifizierungsdiensteanbieters generiert und sind vor dem Auslesen geschützt.

#### **6.2.7 Methode zur Nutzung privater Schlüssel**

Die Nutzung bzw. Aktivierung der privaten Schlüssel der Zertifizierungsstelle ist durch eine Benutzer:innenauthentifikation gesichert.

Die Schlüssel der signierenden Personen werden durch ein Signaturpasswort und eine Verifikations-Code geschützt. Die privaten Schlüssel der Anwendenden werden von der Zertifizierungsstelle verwaltet und können nur angewendet werden, wenn sie noch gültig sind.

#### **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.

Die privaten Schlüssel der signierenden Personen werden deaktiviert, wenn die vorgegebene Anzahl von Fehlversuchen bei der Signaturauslösung überschritten wird.

#### **6.2.9 Methode zur Vernichtung privater Schlüssel**

Die signierende Person hat die Option den zu einem Widerrufenen oder abgelaufenen Zertifikat gehörenden Schlüssel über eine Serviceseite löschen zu lassen.

### **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	20
Zertifizierungsstellen	20
Zertifikatsinhabende	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 Aktivierungsdaten

### 6.4.1 Erzeugung und Installation der Aktivierungsdaten (PINs)

#### 6.4.1.1 Aktivierungsdaten für Schlüssel der Zertifizierungsstelle

Die Schlüssel der Zertifizierungsstelle können ausschließlich im Vieraugenprinzip durch zwei Beauftragte mittels Chipkarte und PIN aktiviert werden. Die Aktivierungsdaten werden direkt in einem HSM vom CA-System erzeugt. Erzeugte Aktivierungsdaten werden nicht schriftlich festgehalten.

Es werden genügend Chipkarten zur Aktivierung erzeugt, damit die Schlüssel der Zertifizierungsstelle nicht durch Zerstörung oder Verlust von Chipkarten unbrauchbar werden.

#### 6.4.1.2 Aktivierungsdaten für Schlüssel der signierenden Personen

Die signierenden Personen aktivieren ihren privaten Schlüssel über ein Signaturpasswort und einen Verifikations-Code.

### 6.4.2 Schutz der Aktivierungsdaten

#### 6.4.2.1 Aktivierungsdaten für Schlüssel der Zertifizierungsstelle

Die Mitarbeitenden, die über die Aktivierungsdaten für Schlüssel der Zertifizierungsstelle verfügen, verpflichten sich diese geheim zu halten (PIN) und sicher aufzubewahren (Chipkarte).

#### 6.4.2.2 Aktivierungsdaten für Schlüssel der signierende Personen

Das Signaturpasswort wird nur gehashed gespeichert.

Das selbst gewählte EU-Identity mobile Signatur-Passwort jeder signierenden Person ist niemand anderem als der signierenden Person bekannt und von der signierenden Person unbedingt entsprechend geheim zu halten.

### **6.4.3 Weitere Aspekte zu den Aktivierungsdaten**

Keine Bestimmungen.

## **6.5 Computer Sicherheitsbestimmungen**

### **6.5.1 Spezifische Sicherheitsanforderungen an die Computer**

Keine Bestimmungen.

### **6.5.2 Bewertung der Computersicherheit**

Keine Bestimmungen.

## **6.6 Life-Cycle der Sicherheitsvorkehrungen**

### **6.6.1 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 Echtssystem getrennt sein
- Die Übernahme der neu entwickelten/geänderten Software in das Echtssystem findet nach erfolgreich abgeschlossenem Test und nach erteilter Freigabe durch die Betriebsleitung statt.

### **6.6.2 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,
- Mitarbeitende 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).

### 6.6.3 Bewertung

Für die Bewertung von Software sind die folgenden Tätigkeiten durchzuführen:

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

## 6.7 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.

## 6.8 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	$\geq$ SHA-2	Für die Signatur über das Zertifikat verwendeter Algorithmus
Ausstellende Entität des Zertifikats	CN = CommonName OU = OrganizationalUnit O = Organization C = AT	CommonName, OrganizationalUnit: A-Trust-Qual- nn bzw. A-Trust-Root-nn Organization: A-Trust GmbH
Gültig von Gültig bis	Beginn und Ende der Gültigkeit des Zertifikats	Der Gültigkeitszeitraum beträgt höchstens 20 Jahre
Zertifikatsinhabende	CN = CommonName OU = OrganizationalUnit  O = Organization C = AT	CommonName, OrganizationalUnit: EU-Identity-Mobile-nn -nn bezeichnet die Generation der CA
Öffentlicher Schlüssel	$\geq$ RSA 4096 Bit	Öffentliche Schlüssel der Zertifikatsinhabenden (der CA)

Tabelle 10: Profil für CA-Zertifikat

### 7.1.2 Zertifikate der Zertifikatsinhabenden

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 Zertifizierungsinfrastuktur
Algorithmus	$\geq$ SHA-2	Für die Signatur über das Zertifikat verwendeter Algorithmus
Ausstellende Entität des Zertifikats	CN=CommonName OU=OrganizationalUnit O=Organization C=AT	Wert Zertifikatsinhabende aus CA-Zertifikat
Gültig von Gültig bis	Beginn und Ende der Gültigkeit des Zertifikats	Der Gültigkeitszeitraum beträgt höchstens fünf Jahre
Zertifikatsinhabende (subject)	C = CountryName T = Title SN = SurName G = GivenName CN = CommonName Seriennummer = Serial-Number O = OrganizationName OU = OrganizationalUnit-Name	CountryName: AT etc., enthält das Land, in dem das zur Registrierung vorgelegte Identifikationsdokument ausgestellt wurde. Title: Titel (Dr. etc.) SurName: Zuname GivenName: Vorname CommonName: entweder Vorname + Zuname oder Pseudonym Titel, Zuname, Vorname entfallen bei Verwendung eines Pseudonyms
Öffentlicher Schlüssel	$\geq$ ECC 256 Bit	Öffentlicher Schlüssel der Zertifikatsinhabenden

Tabelle 11: Profil für EU-Identity mobile 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
<b>Standarderweiterungen</b>				
authorityKeyIdentifier	Nein	Ja		X
subjectKeyIdentifier	Ja	Ja		X
keyUsage	Ja	Ja	X	
subjectAltName	Optional	Optional		X
basicConstraints	Ja	Ja	X	
CRLDistributionPoints	Nein	Ja		X
<b>Private Extensions</b>				
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
<b>Standarderweiterungen</b>			
authorityKeyIdentifier	Ja		X
subjectKeyIdentifier	Ja		X
keyUsage	Ja	X	
certificatePolicies	Ja		X
basicConstraints	Ja		X
cRLDistributionPoints	Ja		X
subjectAltName	optional		X
<b>Private Extensions</b>			
authorityInfoAccess	Ja		X
qc-Statement	Ja		X
1.2.40.0.10.1.1.1	optional		X

Tabelle 13: Erweiterungen EU-Identity mobile Zertifikat

Erweiterung subjectDirectoryAttributes enthält bei EU-Identity mobile Zertifikaten optional das Geburtsdatum der signierenden Person, verpflichtend bei Minderjährigen.

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

Optional können EU-Identity 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.

#### 7.1.4 Identifikation der Policy

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

Die Erweiterung certificatePolicies im Zertifikat wird mit

- OID 0.4.0.194112.1.2 gem. [\[ETSI 319 411\]](#)  
itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2)

und mit

- OID 1.2.040.0.17.1.23 gem. [\[Policy\]](#)  
1.2.040.0.17 (A-Trust).1 (Policy).23 (EU-Identity mobile )

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 Zertifikatsinhabenden. 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 EU-Identity mobile . A-Trust stellt sicher, dass diese Zertifizierungsrichtlinie für die betroffenen Certificate Policies geeignet ist.

## A Anhang

### A.1 Begriffe und Abkürzungen

Aktivierungsdaten	Daten, die zur Aktivierung der Schlüssel benötigt werden.
Anwendende	Person, die die Dienstleistungen der Zertifizierungsstelle der A-Trust nutzt. Anwendende sind sowohl Zertifikatsinhabende als auch Zertifikatsnutzende.
Audit	Von externen Personen durchgeführte Sicherheitsüberprüfung.
CA (Certification Authority), Zertifizierungsdiensteanbietende	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 Widerruflisten (Zertifizierung) verwendet werden.
CA-Zertifikat, Zertifizierungsstellenzertifikat	Zertifikat der Zertifizierungsstelle, das zur Signatur der Zertifikate der signierenden Personen und der zugehörigen CRLs dient
Certification Policy, Policy	Ein Regelwerk, das den Einsatzbereich eines Zertifikates für eine bestimmte Benutzer:innengruppe und/oder Anwendungsklasse festhält.
Certification Practice Statement, CPS, Zertifizierungsrichtlinie	Aussagen über die bei der Ausstellung von Zertifikaten von einem Zertifizierungsdiensteanbietende eingehaltenen Vorgehensweise
Dienste (CA-Dienste)	Überbegriff für angebotene Dienstleistungen wie Verzeichnisdienst, Statusauskunft und Zeitstempeldienst
Dienste-Schlüssel	Schlüssel eines Dienstes (z.B. Signaturschlüssel zur Signatur von Statusauskünften)
Digitale Signatur	Elektronische Signatur, die mit Hilfe von Verfahren der asymmetrischen Kryptographie erzeugt wird.
E-Mail	Electronic Mail; Nachrichten, die in digitaler Form über computerbasierte Kommunikationswege versandt oder empfangen werden.
Elektronische Signatur	Eine Signatur in digitaler Form, die in Daten enthalten ist, Daten beigefügt wird oder logisch mit ihnen verknüpft ist und von einer unterzeichnenden Person verwendet wird, um zu bestätigen, dass der Inhalt dieser Daten gebilligt wird. Sie ist so mit den Daten verknüpft, dass eine nachträgliche Veränderung der Daten offenkundig wird.



---

Gültigkeitsmodell	Modell, nach dem die Prüfung der Gültigkeit von Zertifikaten und Signaturen vorgenommen wird.
Hardware Security Modul, HSM	Elektronisches System zur sicheren Speicherung von Schlüsseln und zur Berechnung und Verifizierung von Signaturen.
Integrität (von Daten)	Ein Zustand, in dem Daten weder von Unbefugten verändert noch zerstört wurden.
Kettenmodell	Gültigkeitsmodell, nach dem eine gültige Anwendung des Schlüssels dann erfolgt, wenn zum Zeitpunkt der Anwendung das Zertifikat gültig ist und das übergeordnete Zertifikat zum Zeitpunkt der Erstellung des eingesetzten Zertifikats gültig war.
Kompromittierung	Eine unautorisierte Offenlegung von oder der Verlust der Kontrolle über sicherheitskritische Informationen und geheim zuhaltende Daten.
LDAP	Lightweight Directory Access Protocol ist ein Standardprotokoll 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.
Qualifiziertes Zertifikat	Zertifikat, welches den Bestimmungen des Anhang I [eIDAS-VO] entspricht.
Qualifiziertes Zertifikat für Siegel	Zertifikat, welches den Bestimmungen des Anhang III [eIDAS-VO] entspricht.
Registrierungsstelle, Registration Authority, RA	Eine vertrauenswürdige Einrichtung, welche die Überprüfung der Identität der Zertifikatsbewerbenden im Namen der Zertifizierungsdiensteanbietenden unter Berücksichtigung der Zertifizierungsrichtlinien durchführt und selbst keine Zertifikate ausstellt.

RFC		Request for Comments, Artikel über Standards und Protokolle im Internet. Neue Standards werden zunächst vorgeschlagen und zur Diskussion gestellt (daher “mit der Bitte um Stellungnahme”). Erst nachdem sie ausdiskutiert und für gut befunden worden sind, werden sie unter einer RFC-Nummer veröffentlicht.
Root-CA, Zertifizierungsstelle	Root-	Die Root-CA ist die oberste CA in der Zertifizierungshierarchie der A-Trust. Sie stellt die Zertifikate für die nachgeordneten CAs aus.
Root-Zertifikat, Stammzertifikat, Root-CA Zertifikat		Zertifikat des Root-Keys, der zur Signatur der Zertifikate der Zertifizierungsstellen und der zugehörigen CRLs dient
RSA		Signatur- und Verschlüsselungsverfahren; benannt nach Rivest, Shamir und Adleman
Schlüsselpaar		Ein privater Schlüssel und der dazugehörige öffentliche Schlüssel. Abhängig vom verwendeten Algorithmus kann man mit Hilfe des öffentlichen Schlüssels eine digitale Unterschrift, die mit dem dazu gehörigen privaten Schlüssel erstellt wurde, verifizieren bzw. mit dem privaten Schlüssel Daten entschlüsseln, welche mit dem zugehörigen öffentlichen Schlüssel verschlüsselt wurden.
signierende Person		Eine natürliche Person, die eine elektronische Signatur erstellt, Zertifikatsinhaber
Siegelersteller		Eine juristische Person, die ein elektronisches Siegel erstellt
Signaturerstellungsdaten		Signaturerstellungsdaten sind einmalige Daten wie Codes oder private Signaturschlüssel, die von dem signierende Person zur Erstellung einer elektronischen Signatur verwendet werden.
Signaturprüfdaten		Signaturprüfdaten sind Daten wie Codes oder öffentliche Signaturschlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden.
Aussetzung		Eine Aussetzung ist ein zeitlich begrenztes vorübergehendes Aussetzen der Gültigkeit eines EU-Identity mobile Zertifikats.
Statusauskunft		Dienst, bei dem die Anwendenden 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 Anwendenden Zertifikate der CA oder anderer Anwendenden 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.
Zertifikatsinhabende	Anwendende, deren Schlüssel und persönliche Daten im Zertifikat der A-Trust festgehalten sind, auch signierende Person genannt.
Zertifikatsnutzende, Signaturempfangende	Anwendende, die Zertifikate über die Schlüssel und Daten anderer nutzt, um Signaturen zu prüfen.
Zertifikats-Widerrufsliste, CRL	Eine digital signierte Datenstruktur, die widerrufenen und ausgesetzten Zertifikate anführt, welche von bestimmten Zertifizierungsdiensteanbietenden ausgestellt wurden.

## A.2 Referenzdokumente

- [AGB] Allgemeine Geschäftsbedingungen (AGB) A-Trust für qualifizierte und fortgeschrittene Zertifikate Version 7.2
- [eIDAS-VO] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
- [SVG] Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur und Vertrauensdienstegesetz - SVG)  
StF: BGBl. I Nr. 50/2016 (NR: GP XXV RV 1145 AB 1184 S. 134. BR: 9594 AB 9607 S. 855.)
- [SVV] Verordnung über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdiensteverordnung – SVV) StF: BGBl. II Nr. 208/2016
- [CPS] A-Trust Zertifizierungsrichtlinie für qualifizierte Zertifikate für sichere Signaturen, in der jeweils aktuellen Version.
- [Policy] A-Trust Certificate Policy für qualifizierte EU-Identity mobile Zertifikate für sichere Signaturen
- [RFC3647] RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003
- [RFC3161] RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol, August 2001
- [ETSI 319 411] Policy and security requirements for Trust Service Providers issuing certificates - ETSI EN 319 411-2 v2.2.2 (April 2018)
- [ETSI TS 119 495] Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366
- [ACOS-05] A-SIT Bescheinigung nach § 18 (5) SigG: Sichere Signaturerstellungseinheit ACOS EMV-A05V1, Konfiguration A+B, (23-06-2016), Referenznummer A-SIT-VI-15-062
- [CardOS5.3] A-SIT Bescheinigung nach § 1 (5) SigG: Sichere Signaturerstellungseinheit CardOS V5.3 QES, V1.0,(24.06.2016) ,Referenznummer A-SIT-VI-16-057

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

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

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