



A-Trust Gesellschaft für Sicherheitssysteme im elektronischen  
Zahlungsverkehr GmbH.  
Landstraßer Hauptstraße 5  
Tel.: +43 (1) 713 21 51 – 0  
Fax: +43 (1) 713 21 51 – 350  
office@a-trust.at  
www.a-trust.at

# A-Trust

## Certification Practice Statement

### trust|sign

**Version: 1.0**

**Datum: 04.12.2001**

## Inhaltsverzeichnis

1	Einleitung .....	13
1.1	Überblick .....	13
1.2	Dokumentidentifikation .....	13
1.3	Zertifizierungsinfrastruktur und Anwendbarkeit.....	13
1.3.1	Zertifizierungsstellen.....	13
1.3.2	Registrierungsstellen .....	14
1.3.3	Widerrufsdienst.....	14
1.3.4	Anwender.....	14
1.3.5	Anwendbarkeit .....	14
1.3.6	Zertifizierungshierarchie .....	15
1.3.7	A-Trust Verzeichnisbaum.....	16
1.4	Ansprechpartner und Kontaktstellen.....	16
1.4.1	Organisation zur Verwaltung dieses Dokuments .....	16
1.4.2	Kontaktperson.....	17
1.4.3	Verantwortlicher für die Anerkennung anderer Policies.....	17
2	Generelle Bestimmungen .....	18
2.1	Verpflichtungen.....	18
2.1.1	Verpflichtungen der Zertifizierungsstellen.....	18
2.1.2	Verpflichtungen der Registrierungsstellen .....	19
2.1.3	Verpflichtungen der Zertifikatsinhaber .....	19
2.1.4	Verpflichtungen der Zertifikatsnutzer .....	20
2.1.5	Verpflichtungen der Verzeichnisdienste .....	20
2.2	Haftung.....	21

2.2.1	Haftung der Zertifizierungsstelle .....	21
2.2.2	Haftung der Registrierungsstelle .....	22
2.3	Finanzielle Verantwortung .....	22
2.3.1	Schadensersatz der beteiligten Parteien.....	22
2.3.2	Treuhänderische Beziehungen.....	22
2.3.3	Administrative Prozesse.....	22
2.4	Auslegung und (gerichtliche) Durchsetzung .....	22
2.4.1	Zugrunde liegende Gesetzesbestimmungen.....	22
2.4.2	Trennbarkeit der Bestimmungen, Fortbestehen von Ansprüchen, Vereinigung (Fusion), Kündigung .....	23
2.4.3	Schlichtungsverfahren .....	23
2.5	Gebühren.....	23
2.5.1	Ausgabe und Erneuerung von Zertifikaten.....	23
2.5.2	Abrufen von Zertifikaten.....	24
2.5.3	Sperre oder Widerruf von Zertifikaten.....	24
2.5.4	Abrufen von Statusinformationen .....	24
2.5.5	Gebühren für weitere Dienste .....	24
2.5.6	Richtlinien für Gebührenrückerstattung .....	24
2.6	Bekanntmachung und Verzeichnisdienste .....	24
2.6.1	A-Trust Stammzertifikat.....	25
2.6.2	A-Trust CA-Zertifikat .....	25
2.6.3	Widerrufsinformationen .....	25
2.6.4	Suche nach einem Zertifikat.....	26
2.6.5	Veröffentlichung von Informationen der Zertifizierungsstelle .....	26
2.6.6	Frequenz der Aktualisierung.....	27

2.6.7	Zugriffskontrollen.....	27
2.6.8	Verzeichnisse.....	27
2.7	Audit.....	28
2.7.1	Häufigkeit des Audits .....	28
2.7.2	Identität bzw. Anforderungen an den Auditor .....	28
2.7.3	Beziehungen zwischen Auditor und zu untersuchender Partei .....	28
2.7.4	Aspekte des Audits .....	28
2.7.5	Handlungen nach unzureichendem Ergebnis.....	29
2.7.6	Bekanntgabe der Ergebnisse .....	29
2.8	Vertraulichkeit .....	29
2.8.1	Vertraulich eingestufte Informationen.....	29
2.8.2	Nicht vertraulich eingestufte Informationen.....	30
2.8.3	Offenlegung von Informationen zu Sperrungen und Widerruf.....	30
2.8.4	Offenbarung an Behörden im Rahmen gesetzlicher Pflichten.....	30
2.8.5	Offenbarung im Rahmen zivilrechtlicher Auskunftspflichten.....	30
2.8.6	Weitere Gründe zur Freigabe von vertraulichen Informationen.....	30
2.9	Urheberrechte und Eigentumsrechte .....	30
3	Identifizierung und Authentisierung .....	32
3.1	Erstregistrierung .....	32
3.1.1	Namenstypen.....	32
3.1.2	Anforderungen an Namen.....	32
3.1.3	Regeln zur Interpretation unterschiedlicher Namensformen.....	33
3.1.4	Eindeutigkeit von Namen.....	33
3.1.5	Anspruch auf Namen und Beilegung von Streitigkeiten.....	33
3.1.6	Anerkennung, Bestätigung und Bedeutung von Warenzeichen.....	33

3.1.7	Methode mit der der Besitz des geheimen Schlüssels bewiesen wird .....	33
3.1.8	Authentisierung von Organisationen.....	34
3.1.9	Authentisierung von Individuen.....	34
3.2	Erneute Registrierung / Re-Zertifizierung .....	34
3.3	Erneute Registrierung nach Widerruf.....	34
3.4	Sperr- und Widerrufsanspruch .....	34
4	Betriebliche Anforderungen.....	36
4.1	Antrag auf Ausstellung von Zertifikaten.....	36
4.2	Herausgabe von Zertifikaten .....	36
4.3	Akzeptanz von Zertifikaten .....	37
4.4	Sperrungen und Widerruf von Zertifikaten .....	37
4.4.1	Gründe für einen Widerruf .....	37
4.4.2	Wer kann einen Widerruf anordnen .....	38
4.4.3	Prozedur für einen Widerrufsanspruch .....	38
4.4.4	Frist bis zur Bekanntgabe des Widerrufs .....	39
4.4.5	Gründe für eine Sperre.....	39
4.4.6	Wer kann eine Sperre anordnen und aufheben .....	39
4.4.7	Prozedur für einen Sperrantrag .....	40
4.4.8	Sperraufhebung .....	41
4.4.9	Frist bis zur Bekanntgabe der Sperre bzw. Sperraufhebung .....	41
4.4.10	Grenzen einer Sperrperiode .....	41
4.4.11	Aktualisierungsfrequenz der Widerrufsliste .....	42
4.4.12	Anforderungen an die Überprüfung durch Widerrufslisten .....	42
4.4.13	Möglichkeiten zur on-line Statusabfrage.....	42
4.4.14	Anforderungen an die Statusabfrage .....	42

4.4.15	Weitere Verfahren zur Bekanntgabe von Widerrufen.....	43
4.4.16	Anforderungen an die Überprüfung der weiteren Verfahren zur Bekanntgabe von Widerrufen .....	43
4.4.17	Spezielle Verfahren bei Kompromittierung von privaten Schlüsseln .....	43
4.5	Protokollierung sicherheitsrelevanter Ereignisse .....	43
4.5.1	Protokollierte Ereignisse .....	43
4.5.2	Frequenz der Überprüfung der Protokolldateien.....	44
4.5.3	Aufbewahrungszeitraum der Protokolldateien.....	45
4.5.4	Schutz der Protokolldateien.....	45
4.5.5	Protokollierungssystem (intern / extern) .....	45
4.5.6	Benachrichtigung beim Auftreten sicherheitskritischer Ereignisse.....	45
4.5.7	Bewertungen zur Angreifbarkeit.....	45
4.6	Archivierung .....	46
4.6.1	Archivierte Daten.....	46
4.6.2	Aufbewahrungszeiten.....	46
4.6.3	Schutzvorkehrungen.....	47
4.6.4	Anforderungen, die Daten mit Zeitstempeln zu versehen .....	47
4.6.5	System zur Erfassung der Archivierungsdaten (intern / extern) .....	47
4.6.6	Prozeduren zum Abrufen und Überprüfen von Daten.....	47
4.7	Schlüsselwechsel von CA- und Root-Schlüssel.....	48
4.8	Kompromittierung und Notfallplan.....	49
4.8.1	Rechner, Software und/oder Daten sind korrumpiert.....	49
4.8.2	Widerruf von Zertifikaten zu Zertifizierungsstellen- und Dienste-Schlüsseln	49
4.8.3	Schlüsselkompromittierung bzw. Verdacht auf Schlüsselkompromittierung	51
4.8.4	Sicherheitsvorkehrungen nach Katastrophen.....	52

4.9	Einstellung der Tätigkeit der Zertifizierungsstelle .....	52
5	Physische, verfahrensorientierte und personelle Sicherheitsvorkehrungen..	54
5.1	Physische Sicherheitsvorkehrungen .....	54
5.1.1	Standort und örtliche Gegebenheiten.....	54
5.1.2	Zugangskontrollen.....	56
5.1.3	Stromversorgung und Klimaanlage .....	56
5.1.4	Wasserschäden.....	56
5.1.5	Feuer .....	56
5.1.6	Datenträger .....	57
5.1.7	Müllentsorgung .....	57
5.1.8	Redundante Auslegung .....	57
5.2	Verfahrensorientierte Sicherheitsvorkehrungen.....	57
5.2.1	Funktionen der A-Trust.....	57
5.2.2	Sicherheitskritische Funktionen.....	58
5.2.3	Sonstige (nicht sicherheitskritische) Funktionen.....	60
5.2.4	Anzahl erforderlicher Personen für sicherheitsrelevante Tätigkeiten .....	60
5.2.5	Identifikation und Authentikation der Rollen.....	62
5.3	Personelle Sicherheitsvorkehrungen .....	62
5.3.1	Anforderungen an das Personal .....	62
5.3.2	Überprüfung des Personals (z. B. Strafregisterauszug) .....	63
5.3.3	Anforderungen an die Schulung .....	63
5.3.4	Anforderungen und Häufigkeit von Schulungswiederholungen.....	63
5.3.5	Ablauf und Frequenz der Job Rotation.....	63
5.3.6	Sanktionen für unautorisierte Handlungen.....	63
5.3.7	Anforderungen an Vertragsvereinbarungen mit dem Personal .....	64

5.3.8	An das Personal auszuhändigende Dokumente .....	64
6	Technische Sicherheitsvorkehrungen .....	65
6.1	Schlüsselgenerierung und Installation .....	65
6.1.1	Schlüsselgenerierung .....	65
6.1.2	Auslieferung privater Schlüssel.....	65
6.1.3	Auslieferung öffentlicher Schlüssel an Zertifikatsaussteller .....	66
6.1.4	Auslieferung öffentlicher Schlüssel von der Zertifizierungsstelle an die Signatoren.....	66
6.1.5	Schlüssellängen .....	66
6.1.6	Parameter zur Schlüsselerzeugung .....	67
6.1.7	Qualitätsprüfung der Parameter .....	67
6.1.8	Hardware/Software Schlüsselerzeugung .....	67
6.1.9	Verwendungszweck der Schlüssel (nach X.509 v3 usage Feld).....	67
6.2	Schutz der privaten Schlüssel.....	69
6.2.1	Standards des kryptographischen Moduls .....	69
6.2.2	Aufteilung privater Schlüssel auf mehrere Personen.....	69
6.2.3	Hinterlegung privater Schlüssel.....	70
6.2.4	Backup privater Schlüssel.....	70
6.2.5	Archivierung privater Schlüssel.....	70
6.2.6	Einbringung privater Schlüssel in das kryptographische Modul .....	70
6.2.7	Methode zur Freischaltung / Aktivierung privater Schlüssel .....	71
6.2.8	Methode zur Deaktivierung privater Schlüssel .....	71
6.2.9	Methode zur Vernichtung privater Schlüssel.....	71
6.3	Verwendungszeitraum öffentlicher und privater Schlüssel.....	71
6.4	Aktivierungsdaten.....	72



6.4.1	Erzeugung und Installation der Aktivierungsdaten (PINs).....	72
6.4.2	Schutz der Aktivierungsdaten.....	73
6.4.3	Weitere Aspekte zu den Aktivierungsdaten.....	73
6.5	Computer Sicherheitsbestimmungen.....	74
6.5.1	Spezifische Sicherheitsanforderungen an die Computer.....	74
6.5.2	Bewertung der Computersicherheit.....	74
6.6	Life-Cycle der Sicherheitsvorkehrungen.....	74
6.6.1	Systementwicklung .....	74
6.6.2	Sicherheitsmanagement .....	75
6.6.3	Bewertung .....	75
6.7	Vorkehrungen zur Netzwerksicherheit.....	76
6.8	Vorkehrungen zur Wartung (Analyse) des kryptographischen Moduls .....	76
7	Profile von Zertifikaten und Widerrufslisten .....	77
7.1	Zertifikatsprofile .....	77
7.1.1	A-Trust CA-Zertifikate .....	78
7.1.2	Zertifikate für Signatoren.....	79
7.1.3	Erweiterungen (certificate extensions).....	80
7.1.4	Namensformen .....	81
7.1.5	Identifikation der Policy .....	81
7.1.6	Semantik für die Verfahrensweise bei Certificate Policy Extension.....	82
7.2	Profil der Widerrufsliste .....	82
7.2.1	Versionsnummern.....	82
7.2.2	CRL und CRL Entry Extensions .....	82
8	Administration dieser Spezifikation .....	83
8.1	Prozeduren zur Änderung dieses Dokuments .....	83

8.2	Verfahren zur Publizierung und Bekanntgabe.....	83
8.3	Genehmigung und Eignung einer Zertifizierungsrichtlinie .....	84
9	Anhang .....	85

## Tabellenverzeichnis

Tabelle 1 Homepage und Verzeichnisse .....	24
Tabelle 2 Örtlichkeiten .....	55
Tabelle 3 Übergeordnete Rollen der A-Trust .....	58
Tabelle 4 Sicherheitsrelevante Rollen.....	59
Tabelle 5 Nicht sicherheitsrelevante Rollen .....	60
Tabelle 6 Anzahl erforderlicher Personen.....	62
Tabelle 7 Gültigkeitsdauer von Zertifikaten.....	72
Tabelle 8 Profil für CA-Zertifikat .....	78
Tabelle 9 Profil für trust sign Zertifikat.....	79
Tabelle 10 Erweiterungen (CA-Zertifikate) .....	80
Tabelle 11 Erweiterungen (trust sign Zertifikat) .....	81

## Abbildungsverzeichnis

Abbildung 1 Zertifizierungshierarchie .....	15
Abbildung 2 Verzeichnisbaum .....	16

# **1 Einleitung**

## **1.1 Überblick**

Das Ziel der vorliegenden A-Trust Zertifizierungsrichtlinie besteht darin, die Umsetzung der Ausgabe, Administration und Anwendung von trust|sign Zertifikaten derart festzulegen, dass eine sichere und zuverlässige Durchführung der angebotenen trust|sign Zertifizierungsdienstleistungen sowie der Anwendung der ausgebenen Zertifikate gewährleistet ist.

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

Die Gliederung dieses Dokuments orientiert sich an dem internationalen Standard für Zertifizierungsrichtlinien (RFC 2527 - Internet X.509 Public Key Infrastructures, Certificate Policy and Certification Practices Framework) der Internet Society.

## **1.2 Dokumentidentifikation**

Name der Zertifizierungsrichtlinie:	trust sign Zertifizierungsrichtlinie
Version:	1.0/04.12.2001
Object Identifier:	<b>1.2.040.0.17</b> (A-Trust) <b>.2</b> (CPS) <b>.1</b> (trust sign) <b>.1.0</b> (Version) vorliegende Version

## **1.3 Zertifizierungsinfrastruktur und Anwendbarkeit**

### **1.3.1 Zertifizierungsstellen**

Es existiert eine zentrale Zertifizierungsstelle, die die Schlüssel der Signatoren sowie die Widerruflisten für Zertifikate signiert. Die A-Trust stellt qualifizierte Zertifikate

(gemäß SigG) aus, die auf einer sicheren Signaturerstellungseinheit, der trust|sign Karte, basieren.

### **1.3.2 Registrierungsstellen**

In den Registrierungsstellen führen Registration Officers die anwenderrelevanten Arbeiten durch. Diese Aufgaben umfassen neben der sicheren Identifizierung auch die Bearbeitung der Anwenderdaten und die Weiterleitung von Informationen an die übergeordnete Zertifizierungsstelle. Die Aushändigung der Karte erfolgt in der Registrierungsstelle. Sollte der Signator sein Passwort für Widerruf oder Sperrhebung vergessen haben, so erhält er diese Information in der RA.

### **1.3.3 Widerrufsdienst**

Die Anwender können sich bei dem Verlust ihrer Karte oder zu einer Sperre ihres Zertifikats telefonisch bzw. über Fax an den Widerrufsdienst wenden und das Zertifikat widerrufen lassen.

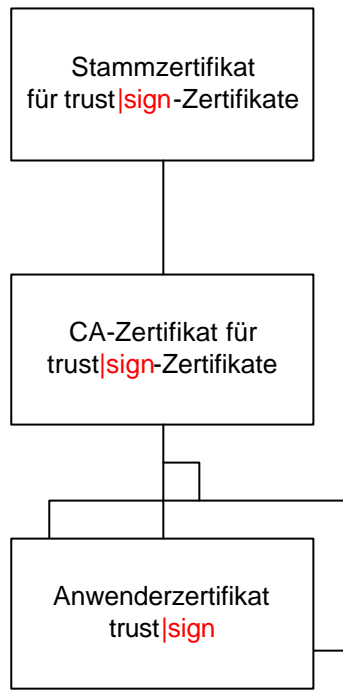
### **1.3.4 Anwender**

Unter „Anwender“ sind die Personen zusammengefasst, die trust|sign Zertifikate von A-Trust erhalten (Zertifikatsinhaber bzw. Signatoren), oder welche trust|sign Zertifikate nutzen bzw. den Zertifikatsangaben trauen (Signaturempfänger).

### **1.3.5 Anwendbarkeit**

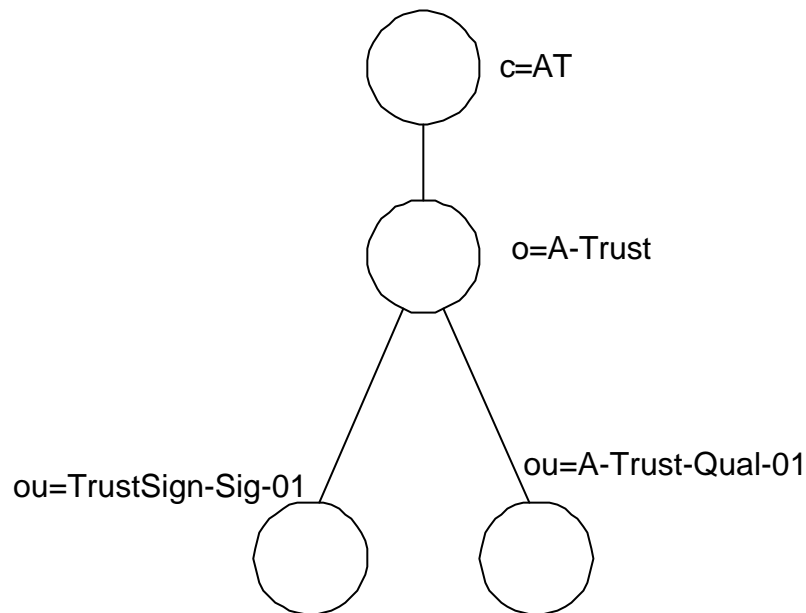
Dieses Dokument ist relevant für die Zertifizierungsstelle, die angeschlossenen Registrierungsstellen, Dienstleistungen der Zertifizierungs- und Registrierungsstelle und die Anwender. Der zertifizierte Signaturschlüssel des Signators darf ausschließlich für das Erstellen von Signaturen genutzt werden.

### 1.3.6 Zertifizierungshierarchie



**Abbildung 1 Zertifizierungshierarchie**

### 1.3.7 A-Trust Verzeichnisbaum



**Abbildung 2 Verzeichnisbaum**

Das Zertifikat des Schlüssels A-Trust-Qual-01 ist das Stammzertifikat von A-Trust.

Mit A-Trust-Qual-01 werden die CA-Zertifikate für trust|sign signiert.

Die Zertifikate der Zertifikatsinhaber von trust|sign-Zertifikaten werden mit dem CA-Schlüssel TrustSign-Sig-01 signiert.

## 1.4 Ansprechpartner und Kontaktstellen

### 1.4.1 Organisation zur Verwaltung dieses Dokuments

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



## 1.4.2 Kontaktperson

Kontaktinformationen für trust|sign Zertifikate der A-Trust erhält man auf folgenden Wegen:

- Auf der Homepage der A-Trust:  
www.A-Trust.at
- Bei der Infohotline des Call Centers:  
Telefonnummer: 0900 833 201
- In jeder Registrierungsstelle der A-Trust und
- auf schriftliche Anfrage an:  
A-Trust  
Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH  
Landstraßer Hauptstraße 5  
A-1030 Wien

## 1.4.3 Verantwortlicher für die Anerkennung anderer Policies

Die A-Trust übernimmt die Entscheidung über die Anerkennung anderer Policies.

## **2 Generelle Bestimmungen**

### **2.1 Verpflichtungen**

#### **2.1.1 Verpflichtungen der Zertifizierungsstellen**

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

- Die Zertifikate für Signatoren werden im Einklang mit der Zertifizierungsrichtlinie erstellt und können gesperrt, widerrufen oder verlängert werden
- Die Zertifizierungsstelle arbeitet im Einklang mit dem der Aufsichtsbehörde vorgelegten Sicherheits- und Zertifizierungskonzept.
- Die Zertifizierungsstelle beschäftigt ausschließlich qualifiziertes Personal.
- Die Zertifizierungsstelle kommt ihrer Informationspflicht hinsichtlich Signatoren 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 Signatoren und zum Signieren der Widerrufslisten.  
Anmerkung: Es gibt auch private Schlüssel für andere Zwecke. In diesem Dokument werden nur die privaten Schlüssel für die Ausstellung von Zertifikaten und Widerrufslisten behandelt.
- Die Zertifizierungsstelle veröffentlicht alle ausgestellten Zertifikate (sofern die Ausstellung vom Inhaber gewünscht ist), alle widerrufenen und alle gesperrten Zertifikate. Bei Widerruf und Sperre eines Zertifikats wird der betroffene Signator schriftlich benachrichtigt. Dem Signator steht bei der Antragsstellung die Option frei, die Veröffentlichung seines Zertifikats zu unterdrücken. Es ist dann nicht öffentlich abfragbar, wird aber bei einer Sperre oder einem Widerruf in die Widerrufsliste aufgenommen.

## 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.
- Die Registrierungsstellen übergeben die trust|sign Karte ausschließlich an den Signator persönlich. A-Trust stellt dem Signator insbesondere folgende Dokumente elektronisch zur Verfügung:
  - Vertragsbedingungen,
  - Entgeltbestimmungen sowie
  - Certification Practice Statement, Certificate Policy und die Belehrungen für den Signator.

## 2.1.3 Verpflichtungen der Zertifikatsinhaber

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

- Die Signatoren verpflichten sich, die Allgemeinen Geschäftsbedingungen zusammen mit der trust|sign Policy, der Zertifizierungsrichtlinie und den Entgeltbestimmungen von A-Trust als Grundlage für den abgeschlossenen Vertrag anzuerkennen.
- Der Signator ist für die Richtigkeit der Angaben verantwortlich, die er bei der Registrierung macht und wirkt gemäß den in der Zertifizierungsrichtlinie angegebenen Verfahren zur Identitätsfeststellung und Authentikation mit.
- Der Signator ist verpflichtet, seinen privaten Schlüssel angemessen zu schützen. Dies umfasst insbesondere keinen Zugriff durch unautorisierte Personen auf die trust|sign Karte zuzulassen und die Aktivierungsdaten (PIN) des privaten Schlüssels nicht weiterzugeben. Dazu gehört weiters die Ver-

wendung eines von A-Trust auf ihrer Homepage empfohlenen Kartenlesegeräts.

- Falls nötig initiiert der Signator unverzüglich die Sperre oder den Widerruf seines Zertifikats. Wird die Sperre nicht nach einem vorgegebenen Zeitraum aufgehoben, so erfolgt automatisch ein Widerruf des Zertifikats.
- Der Signator setzt sein Zertifikat nur zu dem im Zertifikat angegebenen Zweck ein. Maßgeblich hierfür sind die zum Zeitpunkt der Ausstellung des Zertifikats gültige Zertifizierungsrichtlinie und die zugehörige Policy.
- Der Signator wird hinreichend darüber informiert, dass für die Erstellung sicherer Signaturen nur solche technischen Komponenten und Verfahren einzusetzen sind, die von der A-Trust veröffentlicht werden.

Der Signator ist verpflichtet, die jeweiligen nationalen Ausfuhrbestimmungen sowie etwaige nationale Nutzungsbeschränkungen bei einer Verwendung im Ausland zu beachten.

## **2.1.4 Verpflichtungen der Zertifikatsnutzer**

Die Zertifikatsnutzer von trust|sign Zertifikaten (Signaturempfänger) verpflichten sich, vor der Akzeptanz folgende Prüfungen durchzuführen:

- Der Zertifikatsnutzer prüft die digitale Signatur.
- Der Zertifikatsnutzer prüft die Gültigkeit des Zertifikats.
- Die Zertifikatsnutzer prüft, ob das Zertifikat zweckgemäß (d.h. für die Erstellung einer Signatur) eingesetzt wurde.

## **2.1.5 Verpflichtungen der Verzeichnisdienste**

Der Verzeichnisdienst veröffentlicht in regelmäßigen Abständen

- die ausgestellten Zertifikate, die zur Veröffentlichung freigegeben sind, sowie Listen der
- gesperrten und
- widerrufenen Zertifikate.

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

## **2.2 Haftung**

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

### **2.2.1 Haftung der Zertifizierungsstelle**

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

- die 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 sowie ein Widerrufsdienst verfügbar ist,
- die Anforderungen des SigG § 7 erfüllt und für die Erzeugung und Speicherung von Signaturerstellungsdaten technische Komponenten und Verfahren nach SigG § 18 verwendet werden,
- sie die X.509-Standards einhält,
- die Abläufe, die in der gegenständlichen Zertifizierungsrichtlinie beschrieben sind, einhält.

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.

Kann ein Geschädigter nachweisen, dass A-Trust Verpflichtungen oder gesetzliche Bestimmungen missachtet hat, so wird vermutet, dass der Schaden dadurch eingetreten ist (gemäß SigG §23 (3)).

A-Trust haftet nicht, wenn sie nachweist, dass sie und ihre Mitarbeiter an der Verletzung ihrer Verpflichtungen kein Verschulden trifft (gemäß SigG §23 (3)).

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

Die Zertifizierungsstelle haftet für die Registrierungsstellen.

## **2.2.2 Haftung der Registrierungsstelle**

A-Trust haftet für die Tätigkeiten der Registrierungsstellen laut Sicherheits- und Zertifizierungskonzept.

## **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 der A-Trust und dem Signator geschlossene Vertrag unterliegt dem österreichischen Recht und richtet sich nach SigG und SigV. Im Verhältnis zu aus-

ländischen Signatoren wird die Anwendung des UN-Kaufrechts ausdrücklich ausgeschlossen.

## **2.4.2 Trennbarkeit der Bestimmungen, Fortbestehen von Ansprüchen, Vereinigung (Fusion), Kündigung**

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

Änderungen der Allgemeinen Geschäftsbedingungen wie der Zertifizierungsrichtlinie werden dem Signator vor der Zertifikatserneuerung schriftlich mitgeteilt. Ändert A-Trust die Allgemeinen Geschäftsbedingungen, so hat der Signator jederzeit die Möglichkeit zu kündigen. Widerspricht der Signator 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 der Entgeltregelung. Alle Entgelte, die nicht im Grundentgelt enthalten sind, werden mit der Nutzung der jeweiligen Leistung fällig.

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

Das vereinbarte Nutzungsentgelt ist jährlich jeweils am ersten Tag des neuen Jahres zu zahlen. Die Zahlungsverpflichtung entsteht am ersten Tag der betriebsfähigen Bereitstellung und das Entgelt ist im voraus zu bezahlen.

## **2.5.2 Abrufen von Zertifikaten**

Der Abruf von trust|sign Zertifikaten über den Verzeichnisdienst der A-Trust ist kostenfrei.

## **2.5.3 Sperre oder Widerruf von Zertifikaten**

Die Sperre oder der Widerruf eines Zertifikats ist kostenfrei.

## **2.5.4 Abrufen von Statusinformationen**

Der Zugang zu Widerruflisten und Statusinformationen ist gebührenfrei.

## **2.5.5 Gebühren für weitere Dienste**

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

## **2.5.6 Richtlinien für Gebührenrückerstattung**

Der Signator hat keinen Anspruch auf Gebührenrückerstattung. Im Falle einer Kündigung des Vertrags hat der Signator das Entgelt bis zum Ende der Abrechnungsperiode (Ende des Kalenderjahres) zu entrichten.

## **2.6 Bekanntmachung und Verzeichnisdienste**

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

Bekanntmachungen:	<a href="http://www.A-TRUST.at/">www.A-TRUST.at/</a>
Verzeichnisdienst:	<a href="http://ldap.A-TRUST.at/">ldap.A-TRUST.at/</a>
Widerrufliste:	<a href="http://ldap.A-TRUST.at/">ldap.A-TRUST.at/</a>
OCSP:	<a href="http://ocsp.A-TRUST.at/">ocsp.A-TRUST.at/</a>

**Tabelle 1 Homepage und Verzeichnisse**



Der Inhalt dieses Abschnitts entspricht Forderung aus SigV §15 (1) Ziffer 17.

## **2.6.1 A-Trust Stammzertifikat**

Das A-Trust Stammzertifikat ist unter

<http://www.a-trust.at/certs/A-Trust-Qual-01.cer>

zu finden.

Über den entsprechenden Menüpunkt auf der A-Trust Homepage oder direkt unter <http://www.a-trust.at/certs/A-Trust-Qual-01.crt> kann der Download des Stammzertifikats erfolgen.

## **2.6.2 A-Trust CA-Zertifikat**

Das benötigte A-Trust CA-Zertifikat ist unter

<http://www.a-trust.at/certs/TrustSign-Sig-01.cer>

zu finden.

Über die A-Trust Homepage kann der Download des CA-Zertifikats erfolgen.

## **2.6.3 Widerrufsinformationen**

Verteilungspunkte für die Zertifikatssperr- und –widerrufslisten (CRLs):

<ldap://ldap.a-trust.at/ou=TrustSign-SIG-01,o=A-Trust,c=AT?certificaterevocationlist?>

Darüberhinaus kann die aktuelle CRL von der A-Trust Homepage per Download bezogen werden.

Außerdem stellt A-Trust eine sichere Möglichkeit für den Download der Sperrliste über https zur Verfügung.

## **2.6.4 Suche nach einem Zertifikat**

Für die Suche nach einem bestimmten Zertifikat (Suchkriterien sind wahlweise Nachname, Vorname oder E-Mailadresse ) und den Download eines gefundenen Zertifikats steht auf der A-Trust Homepage ein Formular zur Verfügung.

## **2.6.5 Veröffentlichung von Informationen der Zertifizierungsstelle**

Die Zertifizierungsstelle veröffentlicht

- die jeweils gültige Zertifizierungsrichtlinie,
- die jeweils gültige Certificate Policy,
- die gültige Entgeltregelung,
- die Ergebnisse der Audits durch die Aufsichtsbehörden,
- interne Auditinformationen, sofern die Sicherheit der A-Trust nicht gefährdet ist,
- das Zertifikat der Zertifizierungsstelle,
- die Allgemeinen Geschäftsbedingungen,
- die Belehrungen für den Signator, die Information über die zu verwendenden Komponenten und Verfahren und
- 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 Signatoren 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 Zertifikats-erneuerung und
- 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 Email
- Optional: Briefsendung
- Optional: Printmedien oder TV

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

## **2.6.6 Frequenz der Aktualisierung**

Eine Aktualisierung der Zertifizierungsrichtlinie erfolgt gemäß Kapitel 8.

## **2.6.7 Zugriffskontrollen**

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

## **2.6.8 Verzeichnisse**

Folgende Verzeichnisse werden von der Zertifizierungsstelle unterhalten:

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

## **2.7 Audit**

### **2.7.1 Häufigkeit des Audits**

Das erstmalige Audit zur Akkreditierung der Zertifizierungsstelle erfolgt bei Aufnahme des Betriebs.

Danach werden Audits in regelmäßigen Abständen durch die Aufsichtsbehörde durchgeführt.

Darüber hinaus werden jährlich interne Revisionen und Audits durchgeführt.

Audits werden stichprobenhaft in allen A-Trust Liegenschaften und Registrierungsstellen durchgeführt.

### **2.7.2 Identität bzw. Anforderungen an den Auditor**

Die Aufsichtsbehörde bestimmt den Auditor der externen Audits und bedient sich für die Durchführung der Bestätigungsstelle.

Interne Audits werden im Rahmen der Revision durch externe Auditoren durchgeführt.

### **2.7.3 Beziehungen zwischen Auditor und zu untersuchender Partei**

Die Aufsichtsbehörde bestimmt den Auditor der externen Audits. Von A-Trust beauftragte Audits werden von externen Beratern, welche über die notwendige Qualifikation verfügen, durchgeführt.

### **2.7.4 Aspekte des Audits**

Der Auditor überprüft, ob die Zertifizierungsstelle gemäß der Angaben in der Zertifizierungsrichtlinie und dem Sicherheits- und Zertifizierungskonzept arbeitet. Dies gilt ebenfalls für die zu untersuchenden Liegenschaften. Der Auditor versichert

sich des sachgemäßen Einsatzes und der Angemessenheit der kryptographischen Komponenten.

### **2.7.5 Handlungen nach unzureichendem Ergebnis**

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

- Das Zertifikat der Zertifizierungsstelle muss widerrufen werden, und der Betrieb wird eingestellt.
- Der Zertifizierungsstelle wird eine Frist zur Behebung der beanstandeten Mängel eingeräumt, sie bleibt aber weiterhin mit Auflagen versehen in Betrieb.

### **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 vom Signator bekannt gegebenen Daten vertraulich im Sinne des Datenschutzgesetzes zu behandeln. Die Daten, die bei der Anmeldung angegeben werden, werden ausschließlich für die Dienstleistungen der Zertifizierungsstelle benutzt. Bei der Verwendung von Pseudonymen durch den Signator muss die A-Trust den ihr bekannten korrekten und vollständigen Namen des Signators an berechnigte 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 Sperren und Widerrufen**

Gründe, die zur Sperre oder zu einem Widerruf führen, werden im Verzeichnis- und Widerrufsdienst veröffentlicht.

## **2.8.4 Offenbarung an Behörden im Rahmen gesetzlicher Pflichten**

Die A-Trust gibt die persönlichen Daten des Signators nur auf Verlangen an laut SigG berechnigte Personen weiter (gemäß SigG §11).

## **2.8.5 Offenbarung im Rahmen zivilrechtlicher Auskunftspflichten**

Die A-Trust gibt die persönlichen Daten des Signators nur auf Verlangen an laut SigG berechnigte Personen weiter (gemäß SigG §11).

## **2.8.6 Weitere Gründe zur Freigabe von vertraulichen Informationen**

Die A-Trust gibt die persönlichen Daten des Signators nur auf Verlangen an laut SigG berechnigte Personen weiter (gemäß SigG §11).

## **2.9 Urheberrechte und Eigentumsrechte**

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

- Sicherheits- und Zertifizierungskonzept,
- Zertifizierungsrichtlinie,
- Certificate Policy.

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

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

Die Urheber- und Eigentumsrechte der folgenden Schlüssel liegen bei dem Signator:

- Privater Schlüssel des Signators sowie
- Öffentlicher Schlüssel des Signators.

## **3 Identifizierung und Authentisierung**

### **3.1 Erstregistrierung**

Der Inhalt dieses Abschnitts entspricht Forderung aus SigV §15 (1) Ziffer 4.

#### **3.1.1 Namenstypen**

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

- Name für das trust|sign Zertifikat: Nachname und Vorname sind erforderlich. Es kann alternativ auch ein Pseudonym gewählt werden. Der korrekte und vollständige Name muss der Registrierungsstelle und Zertifizierungsstelle auch bei Verwendung eines Pseudonyms bekannt sein.
- Die Angabe der postalischen Adresse ist erforderlich.
- Die Angabe der Meldeadresse ist optional.
- Auf der Kartenoberfläche der trust|sign Karte stehen zwei Zeilen für Informationen zur Verfügung. Die erste Zeile ist erforderlich, die zweite Zeile ist optional.
- Die Angabe einer Email-Adresse ist optional und wird, wenn vorhanden, in die Zertifikatserweiterungen aufgenommen.

Der Inhalt dieses Abschnitts entspricht Forderung aus SigV §15 (1) Ziffer 5.

#### **3.1.2 Anforderungen an Namen**

Der Name des Signators muss entsprechend dem bei der Registrierung vorgelegten amtlichen Lichtbildausweis erfasst werden.

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

Gemäß §8 (4) SigG darf ein verwendetes Pseudonym weder anstößig noch offensichtlich zur Verwechslung mit Namen oder Kennzeichen geeignet sein.



Der Inhalt dieses Abschnitts entspricht Forderung aus SigV §15 (1) Ziffer 5.

### **3.1.3 Regeln zur Interpretation unterschiedlicher Namensformen**

Keine Bestimmungen.

### **3.1.4 Eindeutigkeit von Namen**

Jeder Signator erhält eine 12-stellige Identifikationsnummer (Cardholder Identification Number, abgekürzt CIN). Diese Nummer ist ein Teil des eindeutigen Namens des Signators und ermöglicht die eindeutige und unveränderliche Zuordnung zu einem Signator.

### **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 mit der der Besitz des geheimen Schlüssels bewiesen wird**

Die Karte wird mit einem generierten Schlüsselpaar für das Signieren an den Signator persönlich übergeben. Somit ist kein Beweis des Besitzes eines zum öffentlichen Schlüssel gehörenden privaten Schlüssels erforderlich.

### **3.1.8 Authentisierung von Organisationen**

Keine Bestimmungen.

### **3.1.9 Authentisierung von Individuen**

Die Angaben des Antragstellers werden bei der Abholung der Karte in der Registrierungsstelle durch den Registration Officer überprüft. Der Antragsteller beweist seine Identität durch das Vorlegen eines gültigen, amtlichen Lichtbildausweises. Dabei sind nur ein Personalausweis, ein Reisepass, eine Identitätskarte oder ein Führerschein zulässig. Für Ausländer werden nur gültige Reisepässe in englischer Sprache oder beglaubigte Abschriften zugelassen.

### **3.2 Erneute Registrierung / Re-Zertifizierung**

Der Signator kann eine neue oder auch eine Zusatzkarte beantragen. Der Vorgang verläuft analog zur Erstregistrierung. Dabei sind allfällige Änderungen in den personenbezogenen Daten anzugeben. Die Identifikationsnummer des Karteninhabers wird dabei nicht verändert.

### **3.3 Erneute Registrierung nach Widerruf**

Nach dem Widerruf eines Zertifikates kann der Signator eine neue trust|sign Karte beantragen. Der Vorgang entspricht den Abläufen einer erneuten Registrierung / Re-Zertifizierung.

### **3.4 Sperr- und Widerrufs Antrag**

Sperren und Widerrufe werden entsprechend Abschnitt 4.4 gehandhabt. Der Signator kann sein Zertifikat per Telefon oder Fax sowohl sperren als auch widerrufen lassen.

Dazu muss der Signator zumindest seinen Namen, die Seriennummer bzw. Kartennummer seines Zertifikates und das Passwort angeben.

Sollte er dazu nicht in der Lage sein, ist eine Sperre nur mit folgenden Angaben möglich:

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

Eine Sperre kann innerhalb von drei Werktagen wieder aufgehoben werden.

Wenn das Passwort für einen Widerruf vergessen wurde, muss der Signator sein Passwort in der Registrierungsstelle erfragen. Dazu muss er sich mit einem amtlichen Lichtbildausweis identifizieren.

Der Inhalt dieses Abschnitts entspricht Forderung aus SigV §15 (1) Ziffer 17.

## **4 Betriebliche Anforderungen**

### **4.1 Antrag auf Ausstellung von Zertifikaten**

Der Antrag kann persönlich, per Telefon oder in schriftlicher Form (Brief, Email, Fax) erfolgen. Die Registrierungsstelle entscheidet über die Art und Weise der Antragsbereitstellung für den Kunden. Dabei kann es sich um ein Papier- oder aber auch ein Internet-Formular handeln.

Der Antragsteller erhält

- die PIN-Daten sowie
- den Antrag auf Ausstellung eines qualifizierten Zertifikats laut SigG.

Der Inhalt dieses Abschnitts entspricht Forderung aus SigV §15 (1) Ziffer 4.

### **4.2 Herausgabe von Zertifikaten**

Die mit den Schlüsseln versehene trust|sign Karte wird mit einer Folie versiegelt und an die vom Antragsteller angegebene Registrierungsstelle weitergeleitet. Der Antragsteller selbst erhält auf postalischem Weg einen Brief mit der Initial-PIN und dem von ihm festgelegten Passwort für die Sperre, die Sperraufhebung und den Widerruf des Zertifikats. Zusätzlich wird ihm das Antragsformular auf Ausstellung eines qualifizierten Zertifikats zugeschickt.

Für die Ausgabe der Karte an den Antragsteller muss dieser persönlich in der von ihm angegebenen Registrierungsstelle vorstellig werden. Der Registration Officer darf die Karte erst herausgeben, wenn

- er die Identität des Antragstellers anhand eines gültigen, amtlichen Lichtbildausweises (Personalausweis, Reisepass, Identitätskarte oder Führerschein) überprüft hat,
- der Antragsteller den Antrag auf Ausstellung eines qualifizierten Zertifikats mit seinen Antragsdaten auf Korrektheit überprüft und mit seiner Unterschrift versehen hat,
- der Antragsteller den Erhalt des Briefes mit PIN und Passwort bestätigt hat,
- der Antragsteller über die Sicherheitsrichtlinien belehrt wurde und dies mit seiner Unterschrift bestätigt hat, sowie

- die Allgemeinen Geschäftsbedingungen akzeptiert hat.

### **4.3 Akzeptanz von Zertifikaten**

Für die Ausgabe der Karte durch den Registration Officer muss der Antragsteller persönlich in der von ihm angegebenen Registrierungsstelle vorsprechen. Er hat die im Abschnitt 4.2 aufgeführten Schritte zu unternehmen, um die Karte zu erhalten.

### **4.4 Sperren und Widerrufen von Zertifikaten**

trust|sign Zertifikate können vorübergehend gesperrt werden. Diese Sperre kann auch in einen endgültigen Widerruf umgewandelt werden. Ebenso ist ein sofortiger und permanenter Widerruf des Zertifikats möglich.

#### **4.4.1 Gründe für einen Widerruf**

Der Widerruf eines trust|sign Zertifikats wird erforderlich, wenn

- Angaben im Zertifikat nicht mehr korrekt sind,
- der Signator seine Karte verloren hat bzw. sie wegen Funktionsuntüchtigkeit nicht mehr einsetzen kann,
- Verdacht auf eine Kompromittierung besteht bzw. eine Kompromittierung vorliegt,
- der Zertifizierungsstelle ein wesentlicher Verstoß des Signators gegen diese Richtlinien oder die Allgemeinen Geschäftsbedingungen bekannt wird,
- die Frist einer Aufhebung einer Sperre abläuft,
- das Vertragsverhältnis beendet wird oder
- die eingesetzten Algorithmen nicht mehr den Sicherheitserwartungen entsprechen und dadurch eine sichere Anwendung nicht mehr gegeben wäre.

#### **4.4.2 Wer kann einen Widerruf anordnen**

Ein Widerruf eines trust|sign Zertifikats kann bei dem Vorliegen eines Grundes nach 4.4.1 angeordnet werden durch:

- den betreffenden Signator,
- die Zertifizierungsstelle selbst und
- jeder, der das Passwort für den Widerruf kennt.

#### **4.4.3 Prozedur für einen Widerrufs Antrag**

Ein Widerruf kann durch den Signator vorgenommen werden. Dies kann wie folgt geschehen:

- Der Signator wendet sich per Telefon an den Widerrufsdienst.
- Der Signator veranlasst den Widerruf per Fax.
- Bei Vergessen des Passworts besucht der Signator eine Registrierungsstelle und wendet sich an einen Registration Officer, um das Passwort zu erfragen. Danach ruft er beim Widerrufsdienst an.

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

- Telefonat: Der Signator kann jederzeit einen Widerruf per Telefon vornehmen. Die Authentikation erfolgt nur über das Sperr- und Widerruf-Passwort, welches der Antragsteller bei der Antragsausfüllung selbst festgelegt hat. Das Telefonat wird auf Band gespeichert und gemäß SigV §16 (2) mindestens 33 Jahre archiviert.

Die für einen Widerruf benötigten Informationen lassen sich wie folgt zusammenfassen:

- Persönliche Daten (vollständiger Name, Geburtstag und -ort),
- Passwort,
- Identifikationsnummer des Signators oder Kartenummer oder
- Seriennummer des Zertifikats.

- Fax: Der Signator kann jederzeit einen Widerruf per Fax vornehmen. Das Fax muss das Sperr- und Widerruf-Passwort sowie die vollständige Seriennummer oder die Kartenummer des zu widerrufenden Zertifikats beinhalten. Das Fax wird aufbewahrt und gemäß SigV §16 (2) mindestens 33 Jahre archiviert.
- Besuch in einer Registrierungsstelle: Der Signator benötigt dazu einen gültigen, amtlichen Lichtbildausweis. Der RO teilt dem Signator die Zertifikatsnummer und das Passwort mit, womit der Signator den Widerruf beim Widerrufsdienst veranlassen kann.

Die Angabe des Widerrufsgrundes (Verlust der Karte, Defekt der Karte, Änderung von Daten im Zertifikat, etc.) muss auf jeden Fall erfolgen.

#### **4.4.4 Frist bis zur Bekanntgabe des Widerrufs**

Die Aktualisierung der Widerrufsliste erfolgt während der Geschäftszeiten spätestens innerhalb von drei Stunden ab bekannt werden des Widerrufsgrundes. Der Widerrufsdienst ist jederzeit (d. h. 7 Tage pro Woche jeweils 24 Stunden) erreichbar.

#### **4.4.5 Gründe für eine Sperre**

Die Sperre ist ein temporärer Widerruf des Zertifikats. Sie kann bei Verdacht auf einen Defekt, eine Manipulation sowie den Verlust von Karte oder Passwort eingesetzt werden. Im Gegensatz zu einem Widerruf kann eine Sperre innerhalb einer festgelegten Frist auch wieder aufgehoben werden. Nach drei Werktagen wird eine Sperre durch die Zertifizierungsstelle in einen Widerruf umgewandelt.

#### **4.4.6 Wer kann eine Sperre anordnen und aufheben**

Die bevollmächtigten Personen für eine Sperre und deren Aufhebung sind:

- der Signator und
- jeder, der das Passwort für Sperre und Widerruf kennt.

#### 4.4.7 Prozedur für einen Sperrantrag

Eine Sperre kann durch den Signator vorgenommen werden. Dies kann wie folgt vorgenommen werden:

- Der Signator wendet sich per Telefon an den Widerrufsdienst.
- Der Signator veranlasst die Sperre per Fax.

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

- **Telefonat:** Der Signator kann jederzeit ein Sperren per Telefon vornehmen. Die Authentikation erfolgt über das Sperr- und Widerruf-Passwort, welches der Antragsteller bei der Antragsausfüllung selbst festgelegt hat. Des weiteren wird die eindeutige Seriennummer des Zertifikats, die Kartenummer oder die Identifikationsnummer des Signators benötigt. Das Telefonat wird auf Band gespeichert und gemäß SigV §16 (2) mindestens 33 Jahre archiviert. Die für eine Sperre benötigten Informationen lassen sich wie folgt zusammenfassen:
  - Identifikationsnummer des Signators oder
  - Kartenummer oder
  - Seriennummer des Zertifikats
  - Passwort

Sollte der Signator sein Sperr- und Widerruf-Passwort vergessen haben und somit eine Authentisierung nicht möglich sein, müssen weitere Daten herangezogen werden. Diese sind:

- der vollständige Name,
- das Pseudonym (falls verwendet),
- das Geburtsdatum und
- der Geburtsort.
- **Fax:** Der Signator kann jederzeit eine Sperre per Fax vornehmen. Das Fax muss das Sperr- und Widerrufs-Passwort sowie die vollständige, eindeutige Seriennummer des zu sperrenden Zertifikats oder die Kartenummer oder die Identifikationsnummer des Signators beinhalten. Das Fax wird aufbewahrt und gemäß SigV §16 (2) mindestens 33 Jahre archiviert.



#### **4.4.8 Sperraufhebung**

Innerhalb von drei Werktagen kann der Signator die Sperre des Zertifikats wieder aufheben. Dazu muss er die Sperraufhebung bei dem Widerrufsdienst telefonisch oder per Fax beantragen.

Für die Identifikation muss er sein Passwort angeben. Die Identifikation durch Angaben wie Name, Geburtsdatum und –ort ist nicht zulässig. Sollte der Signator das Passwort vergessen haben, so kann er sein Passwort und die Zertifikatsnummer/Kartenummer auch in der RA erfragen, wobei er sich mit einem gültigen, amtlichen Lichtbildausweis identifizieren muss.

Weitere benötigte Daten sind die Zertifikats- bzw. Kartenummer oder die Identifikationsnummer des Signators.

Das aufgezeichnete Telefonat bzw. das eingegangene Fax wird gemäß SigV §16 (2) mindestens 33 Jahre archiviert.

#### **4.4.9 Frist bis zur Bekanntgabe der Sperre bzw. Sperraufhebung**

Die Sperren werden in der Widerrufsliste eingetragen, bei einer Sperraufhebung sind die betreffenden Sperren in der nächsten Widerrufsliste, die nach der Aufhebung ausgestellt wird, nicht mehr enthalten.

Die Aktualisierung der Widerrufsliste erfolgt während der Geschäftszeiten spätestens innerhalb von drei Stunden ab bekannt werden des Widerrufsgrundes. Der Widerrufsdienst ist 24 Stunden erreichbar.

#### **4.4.10 Grenzen einer Sperrperiode**

Die Sperre eines Zertifikates kann innerhalb von drei Werktagen wieder aufgehoben werden. Andernfalls wird sie durch den Widerrufsdienst in einen Widerruf umgewandelt.

#### **4.4.11 Aktualisierungsfrequenz der Widerrufsliste**

Die aktuelle Update-Frequenz der Widerrufsliste ist im Internet über die Web-Seite der A-Trust abrufbar (siehe Abschnitt 2.6).

#### **4.4.12 Anforderungen an die Überprüfung durch Widerrufslisten**

Das Überprüfen der Gültigkeit von Zertifikaten liegt in der Verantwortung der Zertifikatsnutzer. Der Inhalt eines trust|sign Zertifikats kann nur dann als authentisch gelten, wenn sich der Zertifikatsnutzer von der Gültigkeit des Zertifikats überzeugt hat.

Für eine positive Gültigkeitsüberprüfung ist es erforderlich, dass

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

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

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

#### **4.4.13 Möglichkeiten zur on-line Statusabfrage**

Es wird ein OCSP-Dienst über das Internet angeboten.

#### **4.4.14 Anforderungen an die Statusabfrage**

Ein Zertifikatsnutzer sollte die Authentizität der Auskunft des Verzeichnisdiensts durch die Prüfung der in der Antwort enthaltenen Signatur verifizieren. Des weiteren

ist der in der Auskunft enthaltene Zeitpunkt, auf den sich der Status bezieht, mit dem fraglichen Prüfzeitpunkt zu vergleichen.

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

#### **4.4.15 Weitere Verfahren zur Bekanntgabe von Widerruf**

Keine Bestimmungen.

#### **4.4.16 Anforderungen an die Überprüfung der weiteren Verfahren zur Bekanntgabe von Widerruf**

Keine Bestimmungen.

#### **4.4.17 Spezielle Verfahren bei Kompromittierung von privaten Schlüsseln**

Beim Verlust der trust|sign Karte lässt der Signator diese sperren. Sollte zugleich auch die PIN nicht mehr verfügbar oder sicher sein, führt der Signator einen Widerruf durch.

### **4.5 Protokollierung sicherheitsrelevanter Ereignisse**

#### **4.5.1 Protokollierte Ereignisse**

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

- Ab- und Anschalten von Systemen,
- Änderungen der Hardwarekonfiguration,

- Einrichtung oder Schließung von Accounts,
- Änderungen bei der Rollenaufteilung,
- Änderung der Softwarekonfiguration (Installation oder Update von Software),

Weiterhin werden alle mit den Systemen durchgeführten Transaktionen zusammen mit Transaktionstyp, Zeitpunkt und Informationen darüber, ob die Transaktion abgeschlossen oder abgebrochen wurde und wer die Transaktion veranlasst hat, protokolliert. Folgende Transaktionstypen sind insbesondere aufzuzeichnen:

- Zertifizierungsanträge,
- Schlüsselerzeugungen,
- Zertifikatserstellungen,
- Veröffentlichung von Zertifikaten und Widerrufslisten,
- Sperr- und Widerrufsanträge,
- Ausgeführte Sperren 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 den Signator,
- Bestätigung der Belehrung über die Sicherheitsrichtlinien durch den Registration Officer,
- Akzeptanzerklärung der Allgemeinen Geschäftsbedingungen und der Entgeltbestimmungen durch den Signator oder auch
- Änderungen an den personenbezogenen Signatordaten.

## **4.5.2 Frequenz der Überprüfung der Protokolldateien**

Die Protokolle werden im Zuge der Revision auf verdächtige Vorkommnisse untersucht.

### **4.5.3 Aufbewahrungszeitraum der Protokolldateien**

Sicherheitsrelevante Protokolldateien werden mind. 33 Jahre aufbewahrt. Protokolldateien, die benötigt werden, um nachträglich Aussagen über die Gültigkeit von Zertifikaten zu treffen, werden archiviert. Dies gilt besonders für Daten zur Veröffentlichung von Zertifikaten und Widerrufslisten sowie Eingang und Bearbeitung von Sperranträgen. 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 die A-Trust über eine Benachrichtigung von betroffenen Anwendern.

### **4.5.7 Bewertungen zur Angreifbarkeit**

Keine Bestimmungen.

## **4.6 Archivierung**

### **4.6.1 Archivierte Daten**

Archiviert werden:

- Persönliche Signatordaten, die zur Zertifizierung verwendet wurden,
- Zertifizierungsanträge,
- Alle von der Zertifizierungsstelle ausgestellten Zertifikate (Zertifikate der Zertifizierungsstelle und Dienste, Cross-Zertifikate und Zertifikate der Signatoren),
- Sperr- 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 Schlüsselwechsel der Zertifizierungsstelle.

Zusätzlich werden die Anträge auf Ausstellung des Zertifikats, die Registrierungsunterlagen und die Kopie des gültigen, amtlichen Lichtbildausweises für den in Abschnitt 4.6.2 genannten Zeitraum aufbewahrt.

### **4.6.2 Aufbewahrungszeiten**

Die Aufbewahrungszeiten richten sich nach dem Signaturgesetz und betragen mindestens 33 Jahre.

Für die einzelnen Aufbewahrungszeiten sind folgende Aspekte zu berücksichtigen:

- Die Daten müssen mindestens so lange aufbewahrt werden, wie sie für die Wiederherstellung bei Ausfall von Systemkomponenten im Anwendungszeitraum benötigt werden.
- Insbesondere bei Anwendung digitaler Signaturen sind die Daten mindestens so lange aufzubewahren, wie die digital signierten Dokumente nachprüfbar gehalten 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.

### **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 der archivierenden Einheit vor Modifikationen geschützt.

Die Zugangs- und Zugriffskontrollen räumt nur zwei autorisierten Personen aus dem Zuständigkeitsbereich gleichzeitig den Zutritt in das Archiv ein.

### **4.6.4 Anforderungen, die Daten mit Zeitstempeln zu versehen**

Alle Zertifikatsanträge sind mit einem Zeitstempel zu versehen. Dies betrifft insbesondere die Sperr- und Widerrufsansprüche 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 im A-Trust System 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 dann 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 auch bei Unterbrechungen oder Einstellung der Tätigkeit der Zertifizierungsstelle über den festgelegten Archivierungszeitraum bestehen bleibt.

## **4.7 Schlüsselwechsel von CA- und Root-Schlüssel**

Ein Schlüsselwechsel erfolgt je Zertifikatstyp nach einer festgelegten Zeitspanne. Zusätzlich können außerplanmäßige Schlüsselwechsel bei einem Widerruf der Zertifikate, dem Ausfall eines Hardware Security Moduls oder gar einer Kompromittierung von Schlüsseln erforderlich werden.

Die Instanzen wechseln regelmäßig ihren Schlüssel. Dies sollte vor dem Ablauf der im zugehörigen Zertifikat festgelegten Gültigkeitsdauer geschehen. Rechtzeitig vor einem Schlüsselwechsel wird dieser auf der Web-Seite (siehe Abschnitt 2.6.5) angekündigt. Die Gültigkeitsdauer der Zertifikate ist Kapitel 6.3 zu entnehmen.

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

Um sich von der Authentizität des Zertifikats der A-Trust Root zu überzeugen hat der Signator die Möglichkeit der Abfrage des in den Medien (Wiener Zeitung) oder auf der A-Trust-Homepage veröffentlichten Fingerprints.

Mit dem 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. 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.



## **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 könnte, so werden die entsprechenden Komponenten umgehend aus dem Betrieb genommen.

Bei Zertifikaten sind die betroffenen Signatoren zu informieren. Es erfolgt eine unmittelbare Sperre 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 eine weitere Verbreitung zu verhindern. Die Wiederaufnahme des Dienstes ist mit der Veröffentlichung der neuen Widerrufsliste verbunden. In Abhängigkeit der Fehler und der Ausfallzeit der Verzeichnisdienste werden die Anwender informiert.

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

### **4.8.2 Widerruf von Zertifikaten zu Zertifizierungsstellen- und Dienste-Schlüsseln**

Zertifikate der Zertifizierungsstelle werden in den folgenden Fällen widerrufen:

- bei Kompromittierung oder Verdacht auf Kompromittierung der entsprechenden Schlüssel,
- wenn die eingesetzten Algorithmen nicht mehr den Sicherheitserwartungen 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.

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 Signatoren rechtzeitig über den bevorstehenden Widerruf informiert. Ein ungeplanter Widerruf erfordert eine umgehende Informierung der Signatoren. 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 deaktiviert.

#### **4.8.2.1 Widerruf von Zertifikaten der Dienste**

Werden Zertifikate der Dienste der Zertifizierungsstelle widerrufen, so werden die Dienste ohne gültigen Schlüssel umgehend aus dem Betrieb genommen. Dadurch wird verhindert, dass die Anwender Dienste nutzen, deren Signaturen 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.

#### **4.8.2.2 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.

Signatoren, deren Zertifikate von dem Widerruf betroffen sind, erhalten neue Schlüssel mit neuen Zertifikaten nach den entsprechenden Richtlinien dieses Dokuments. Die Zertifizierung erfolgt dabei mit einem neuen Schlüssel der Zertifizierungsstelle.

##### **4.8.2.2.1 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 dem regulären Wechsel unterscheidet:

- Eine rechtzeitige Informierung der Signatoren über den Schlüsselwechsel ist bei einem unmittelbaren Widerruf nicht möglich. Die Signatoren werden im Zusammenhang mit der Widerrufsinformation auch umgehend über den Schlüsselwechsel informiert.
- Es findet keine Crosszertifizierung mit dem ungültigen Zertifikat statt. Die Signatoren 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.

#### **4.8.2.2 Widerruf von Crosszertifikaten**

Wird ein Zertifikat der Zertifizierungsstelle widerrufen, so werden auch alle dazu erstellten Crosszertifikate widerrufen. Dies gilt auch für Crosszertifikate, die zu anderen Zertifizierungsstellen ausgestellt wurden. Dies gilt insbesondere dann, wenn die Sicherheitsanforderungen durch diese Zertifizierungsstelle nicht mehr erfüllt sind.

#### **4.8.3 Schlüsselkompromittierung bzw. Verdacht auf Schlüsselkompromittierung**

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

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

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

#### **4.8.4 Sicherheitsvorkehrungen nach Katastrophen**

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

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

#### **4.9 Einstellung der Tätigkeit der Zertifizierungsstelle**

Einstellung der Tätigkeit bedeutet, dass die kompletten Dienstleistungen (Ausnahme: Zugriff auf archivierte Daten) 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 Inhaber 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 Zertifikatsinhaber werden vom Widerruf ihres Zertifikates informiert.

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

A-Trust trägt dafür Sorge, dass die CRLs der eingestellten Zertifizierungsstelle auch nach der Beendigung den Benutzern öffentlich und authentisch zur Verfügung

stehen. Eine darüber hinausgehende Übertragung der Verpflichtung an Drittparteien ist nicht notwendig.

## **5 Physische, verfahrensorientierte und personelle Sicherheitsvorkehrungen**

### **5.1 Physische Sicherheitsvorkehrungen**

#### **5.1.1 Standort und örtliche Gegebenheiten**

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

Dienstleistung	Adresse
Firmensitz	A-Trust Landstraßer Hauptstraße 5 A-1030 Wien
Registrierung	Von der A-Trust autorisierte Organisationen, wie z. B. Banken. Die Adressen sind auf der Web-Seite von A-Trust <a href="http://www.a-trust.at">www.a-trust.at</a> veröffentlicht.
Zertifizierung PIN-Briefe-Versand	Siemens Rechenzentrum Siemensstr. 88-92 A-1211 Wien  Ausfallrechenzentrum: Siemens Rechenzentrum Dietrichgasse 27-29 A-1030 Wien
Kartenproduktion Personalisierung	Austria Card Lamezanstr. 4-8 A-1232 Wien
Widerrufsdienst	T-Systems Hofmühlgasse 3-5 A-1060 Wien Telefonnummer: 59903 3072 bzw. 90337 3072 Faxnummer: 59903 3890 bzw. 90337 3890
Call Center	T-Systems Hofmühlgasse 3-5 A-1060 Wien Telefonnummer: 0900 833 201 bzw. 90337 3085 oder 59903 3071

**Tabelle 2 Örtlichkeiten**

## **5.1.2 Zugangskontrollen**

Der Zugang zu allen technischen Komponenten im Rechenzentrum ist nur durch einen von 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 die Notstromversorgung durch ein Diesellaggregat.

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 eines Rechenzentrums der Siemens AG.



## **5.1.6 Datenträger**

Als Datenträger werden folgende Medien eingesetzt:

- Papier
- CD-ROMs
- Magnetbänder
- Festplatten

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

## **5.1.7 Müllentsorgung**

Die Daten auf den elektronischen Datenträger werden sachgemäß vernichtet und die Datenträger dann einer Spezialfirma zur sachgerechten Entsorgung übergeben.

Papierdatenträger werden in vorhandenen Aktenvernichtern entsorgt oder einer Spezialfirma zur sachgemäßen Entsorgung übergeben.

## **5.1.8 Redundante Auslegung**

Der gesamte Betrieb im Rechenzentrum ist redundant ausgelegt, so dass eine Hochverfügbarkeit (7x24 Stunden) des Rechenzentrumsbetriebs erreicht werden kann.

## **5.2 Verfahrensorientierte Sicherheitsvorkehrungen**

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

### **5.2.1 Funktionen der A-Trust**

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

**Tabelle 3 Übergeordnete Rollen der A-Trust**

## 5.2.2 Sicherheitskritische Funktionen

<b>Rolle</b>	<b>Verantwortung</b>
Sicherheitsbeauftragter	Beschreibung siehe Tabelle Übergeordnete Rollen
Revision	Beschreibung siehe Tabelle Übergeordnete Rollen
Datenschutz	Beschreibung siehe Tabelle Übergeordnete Rollen
Security Officer (SO)	Verantwortlichkeit für die Generierung und Zertifizierung der Schlüssel von A-Trust und Sperre dieser Zertifikate Verwaltung der Hardware Security Module Vergabe der RO- und RCA-Berechtigung Ansprechpartner für sicherheitsrelevante Fragen Beaufsichtigung der Einhaltung der im CPS festgelegten Vorgehensweisen
Sicherheitssystem administrator	Zutritt in die Hochsicherheitszone Beaufsichtigung von Systemadministrator und Systemoperator
Initialisierer	Initialisieren der Karten auf der Initialisierungsanlage
Personalisierer	Personalisieren der Karten auf der Personalisierungsanlage
Revocation Center Agent (RCA), Mitarbeiter im Widerrufsdienst	Ansprechpartner für die Zertifikatsinhaber hinsichtlich der Annahme von Anträgen für Sperre, Widerruf und Aufhebung von Sperren Durchführung der Umwandlung einer Sperre in einen Widerruf
Registration Officer (RO), Mitarbeiter der Registrierungsstelle	Entgegennahme von Zertifikatsanträgen, Änderungsanträgen und Nachdruckaufträgen. Identifikation von Zertifikatswerbern im Rahmen der Registrierung und der Bekanntgabe des Widerrufspassworts Belehrung der Zertifikatsinhaber

**Tabelle 4 Sicherheitsrelevante Rollen**

### 5.2.3 Sonstige (nicht sicherheitskritische) Funktionen

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

**Tabelle 5 Nicht sicherheitsrelevante Rollen**

### 5.2.4 Anzahl erforderlicher Personen für sicherheitsrelevante Tätigkeiten

Die folgende Tabelle stellt sicherheitsrelevante Tätigkeiten dar und ordnet diesen die dafür zuständigen Rollen zu. Weiterhin wird aufgezeigt, ob für diese Tätigkeit das Vieraugenprinzip notwendig ist.

Tätigkeit	Personen	Vieraugenprinzip notwendig
Registrierung und Identifizierung von Zertifikatswerbern	RO	Nein
Initialisierung der Karten	Kartenproduzent-Initialisierer	Nein
Personalisierung der Karten	Kartenproduzent-Personalisierer	Nein
Sperren von Anwenderzertifikaten	RCA, RO	Nein
Widerrufen von Anwenderzertifikaten	RCA, RO	Nein
Aufheben einer Sperre von Anwenderzertifikaten	RCA, RO	Nein

<b>Tätigkeit</b>	<b>Personen</b>	<b>Vieraugen- prinzip notwendig</b>
Umwandeln einer Sperre in einen Widerruf	RCA	Nein
Erzeugung der Schlüssel der CA und Schlüsselwechsel	SO	Ja
Aktivierung der Schlüssel	SO	Ja
Zertifizierung für CA (inkl. Cross-zertifikate)	SO	Ja
Widerruf von Zertifikaten der CA (inkl. Crosszertifikate)	SO	Ja
Vergabe der Berechtigungen für RO und RCA	SO	Ja
Ab- und Anschalten von Komponenten, insbesondere Verzeichnisdiensten	Sicherheitssystem-administrator	Ja
Austausch von Hardware-Komponenten	Sicherheitssystem-administrator, Systemadministrator	Ja
Austausch von Software-Komponenten	Sicherheitssystem-administrator, Systemadministrator	Ja
Überprüfung von Protokolldateien auf verdächtige Vorkommnisse	Auditor	Nein
Überprüfung der Protokolldateien auf Manipulation sowie anschließende Anfertigung bzw. Lagerung des Backups	Auditor, Sicherheitssystem-administrator	Nein
Qualitätsprüfung der verwendeten Schlüssellängen und Parameter zur Schlüsselerzeugung	SO	Nein
Wartung oder Austausch eines kryptographischen Moduls	SO, Sicherheitssystem-administrator	Ja
Genehmigung zur Zertifizierung von Schlüsseln anderer Zertifizierungsstellen (Crosszertifizierung)	Sicherheits-beauftragter	Nein

## **Tabelle 6 Anzahl erforderlicher Personen**

### **5.2.5 Identifikation und Authentikation 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**

Für das von A-Trust beschäftigte Personal werden die Anforderungen aus SigG und SigV eingehalten.

Insbesondere erfüllt das Personal alle notwendigen Anforderungen hinsichtlich Vertrauenswürdigkeit, Integrität, Zuverlässigkeit und Fachkunde.

Gemäß SigV §10 (5) ist ein ausreichendes Fachwissen in den Bereichen:

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

erforderlich.

### **5.3.2 Überprüfung des Personals (z. B. Strafregisterauszug)**

Gemäß SigV §10 (4) dürfen im Rahmen der bereitgestellten Signatur- und Zertifizierungsdienste keine Personen beschäftigt werden, die wegen einer mit Vorsatz begangenen strafbaren Handlung zu einer Freiheitsstrafe von mehr als einem Jahr oder wegen strafbarer Handlungen gegen das Vermögen oder gegen die Zuverlässigkeit von Urkunden und Beweiszeichen zu einer Freiheitsstrafe von mehr als drei Monaten verurteilt wurden. Verurteilungen, die nach den Bestimmungen des Tilgungsgesetzes 1972 getilgt sind oder der beschränkten Auskunft unterliegen, bleiben außer Betracht.

Die Zuverlässigkeit des Personals wird in Abständen von zumindest zwei Jahren überprüft.

### **5.3.3 Anforderungen an die Schulung**

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

### **5.3.4 Anforderungen und Häufigkeit von Schulungswiederholungen**

Die Schulungen finden in regelmäßigen Abständen insbesondere bei der Einführung neuer technischer Systeme, Software oder Sicherheitssystemen 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 gem. den Bestimmungen des Österreich. Datenschutzgesetzes zur Geheimhaltung verpflichtet.

### **5.3.8 An das Personal auszuhändigende Dokumente**

An das Personal werden 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 Signatoren**

Die Schlüsselgenerierung erfolgt im Hochsicherheitsbereich des Kartenherstellers. Die Schlüssel werden in trust|sign Karten erzeugt, auf welche anschließend die persönlichen Daten des zukünftigen Zertifikatsinhabers aufgebracht werden. Ein Zertifikat für das Signaturschlüsselpaar wird noch nicht erstellt. Dies geschieht erst auf Veranlassung der Registrierungsstelle, nachdem der Signator zuverlässig identifiziert und authentifiziert wurde.

##### **6.1.1.2 Schlüssel der Zertifizierungsstelle**

Die Schlüssel der Zertifizierungsstelle werden in dem 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 Mitarbeitern und muss von der Geschäftsführung der A-Trust angeordnet werden.

#### **6.1.2 Auslieferung privater Schlüssel**

Der private Signaturschlüssel wird in der trust|sign Karte an den Signator ausgeliefert. Der Signator versichert sich bei der Übergabe der trust|sign Karte in der RA, dass die die Karte versiegelnde Folie nicht beschädigt ist.

Ein Auslesen des privaten Signaturschlüssels aus der Chipkarte ist nicht möglich.

Der private Signaturschlüssel kann nur durch die korrekte Eingabe der Identifikationsdaten (PIN) benutzt werden. Das Wissen über die PIN besitzt nur der Signator.

### **6.1.3 Auslieferung öffentlicher Schlüssel an Zertifikatsaussteller**

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

### **6.1.4 Auslieferung öffentlicher Schlüssel von der Zertifizierungsstelle an die Signatoren**

Der öffentliche Schlüssel der A-Trust Root wird jedem Signator mit seiner Chipkarte sicher ausgeliefert.

Zusätzlich werden das Zertifikat des Schlüssels der A-Trust Root sowie aller A-Trust Zertifizierungsstellen in einem Verzeichnis im Internet veröffentlicht, damit es allgemein zugänglich ist und alle Zertifikatsnutzer Zertifikate dagegen prüfen können.

Das selbst signierte Zertifikat der A-Trust Root wird außerdem in einer Ausgabe der Wiener Zeitung veröffentlicht.

### **6.1.5 Schlüssellängen**

Die Schlüssel der A-Trust Root und aller A-Trust Zertifizierungsstellen entsprechen einer Länge von zur Zeit 2048 Bit (RSA-Schlüssel).

Der von A-Trust zur Erstellung der Signatur über die Zertifikate verwendete Hash-Algorithmus ist SHA-1.

Die Schlüssel der Signatoren entsprechen einer Länge von zur Zeit 1024 Bit (RSA-Schlüssel).

Als Hash-Algorithmus wird den Zertifikatsinhabern die Verwendung von SHA-1 bzw. RIPEMD-160 empfohlen.

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

Die Schlüsselerzeugung erfolgt unter Einsatz eines physikalischen Zufallszahlengenerators, der auf einer physikalischen Rauschquelle basiert und das Primärauschen kryptographisch nachbehandelt.

Die Primfaktoren  $p$  und  $q$  von  $n$  werden so gewählt, dass:

$$\log_2(n) = \log_2(p) + \log_2(q) > 1023$$

und

$$0,5 < |\log_2(p) - \log_2(q)| < 30$$

gilt.

Der öffentliche Exponent  $e$  wird zufällig gewählt.

## 6.1.7 Qualitätsprüfung der Parameter

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

## 6.1.8 Hardware/Software Schlüsselerzeugung

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

Die Schlüssel der Signatoren werden im Chip der trust|sign Karte 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“ bzw. „extKeyUsage“ angegeben.

### **6.1.9.1 Verwendung der Schlüssel der A-Trust Root-CA**

Die A-Trust Root-Zertifizierungsstelle besitzt ein selbstsigniertes Zertifikat, das zum Signieren der CA-Zertifikate und Widerrufslisten verwendet wird.

keyUsage:

- keyCertSign und
- cRLSign

### **6.1.9.2 Verwendung der Schlüssel der A-Trust Zertifizierungsstellen**

Die Schlüssel der A-Trust Zertifizierungsstelle werden ausschließlich zum Signieren von Zertifikaten und Widerrufslisten eingesetzt.

Deshalb werden die Bits

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

gesetzt.

### **6.1.9.3 Verwendung des Schlüssels des Signators**

Der Schlüssel des Signators dient zur Erstellung einer digitalen Signatur.

Deshalb werden die Bits

- nonRepudiation und
- digitalSignature

gesetzt.

Weiters wird extendedKeyUsage auf EmailProtection gesetzt.

## **6.2 Schutz der privaten Schlüssel**

### **6.2.1 Standards des kryptographischen Moduls**

#### **6.2.1.1 Schlüssel der Zertifizierungsstelle**

Als kryptographische Module werden Hardware Security Module eingesetzt.

Der private Schlüssel A-Trust Root dient zur Signatur der Zertifikate der A-Trust Zertifizierungsstellen. Er wird nur in einer gesicherten Umgebung eingesetzt.

Die Schlüssel einer A-Trust Zertifizierungsstelle dienen zur Signatur von Zertifikaten, Widerruflisten und Crosszertifikaten. Er wird nur in einer sicheren Umgebung eingesetzt.

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

#### **6.2.1.2 Schlüssel der Signatoren**

Die Schlüssel der Signatoren werden auf einer gesetzeskonformen Chipkarte, der trust|sign Karte, gespeichert. Bei der trust|sign Karte handelt es sich um eine von A-SIT nach §18(5) [SigG] bescheinigte Smartcard, welche eine sichere Signaturerstellungseinheit darstellt und die Erzeugung und Speicherung der Signaturerstellungsdaten und die Erstellung sicherer elektronischer Signaturen ermöglicht (siehe [A-SIT-Karte]).

Die trust|sign Karte unterstützt Hash-Verfahren. Weitere Informationen dazu sind auf der A-Trust Homepage unter „empfohlene Komponenten und Verfahren“ nachzulesen.

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

Private Schlüssel befinden sich entweder in einem Hardware Security Modul (Schlüssel der Zertifizierungsstelle) oder auf einer Chipkarte (Schlüssel der Signatoren).

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

Für Signaturschlüssel ist ausschließlich die Kontrolle einer einzelnen Person gefordert.

### **6.2.3 Hinterlegung privater Schlüssel**

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

### **6.2.4 Backup privater Schlüssel**

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

### **6.2.5 Archivierung privater Schlüssel**

Eine Archivierung privater Schlüssel findet nicht statt.

### **6.2.6 Einbringung privater Schlüssel in das kryptographische Modul**

Die eingesetzte kryptographische Hardware ist so beschaffen, dass die privaten Schlüssel nur innerhalb dieses Mediums generiert werden. Somit ist eine Einbringung von außen nicht erforderlich.

#### **6.2.6.1 Schlüssel der Zertifizierungsstelle**

Die privaten Schlüssel der Zertifizierungsstelle zum Signieren von Zertifikaten und Widerruflisten werden in einem Hardware Security Modul erzeugt und dort gespeichert. Die Anwendung erfolgt ebenfalls direkt im Hardware Security Modul.

### **6.2.6.2 Schlüssel der Signatoren**

Die privaten Signaturschlüssel der Signatoren werden direkt in der trust|sign Karte generiert und sind vor dem Auslesen geschützt.

### **6.2.7 Methode zur Freischaltung / Aktivierung privater Schlüssel**

Die Nutzung bzw. Aktivierung der privaten Schlüssel der Zertifizierungsstelle ist durch eine Benutzerauthentikation gesichert.

Die Schlüssel der Signatoren werden durch die korrekte Eingabe einer PIN aktiviert. Diese PIN ist jedes Mal vor der Erstellung einer Signatur einzugeben. Nach jeweils drei aufeinanderfolgenden Fehlversuchen ist die PIN gesperrt.

### **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. Private Schlüssel, die nicht mehr genutzt werden, werden mit einer geeigneten Funktion im Hardware Security Modul deaktiviert.

Die privaten Schlüssel der Signatoren werden deaktiviert, wenn eine vorgegebene Anzahl von Fehlversuchen zur PIN-Eingabe überschritten wird.

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

Die auf dem Chip der trust|sign Karte befindlichen Schlüssel der Signatoren werden durch die Zerstörung der Karte vernichtet.

## **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 ge-

sperrt werden, ohne dass die ihm untergeordneten Zertifikate dadurch ihre Gültigkeit verlieren.

Solange der Zertifizierungsschlüssel noch als sicher gilt, kann eine Erneuerung vorgenommen werden.

Für die Zertifikate gelten die folgenden Gültigkeitsdauern:

Zertifikatstyp	Gültigkeitsdauer (Jahre)
A-Trust Root-CA	3
A-Trust Zertifizierungsstelle	3
Signatorschlüssel	3

**Tabelle 7 Gültigkeitsdauer von Zertifikaten**

## **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 Vier-Augen-Prinzip 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 Signatoren**

Die Signatoren aktivieren ihren privaten Schlüssel über eine PIN.



Die Initial (bzw. Transport)-PIN wird in einem HSM erzeugt. Die Signatoren erhalten diese mit der Benachrichtigung, dass ihre trust|sign Karte zur Abholung bereit liegt. Mit dieser PIN kann noch keine Signatur durchgeführt werden. Die Eingabe der Initial-PIN fordert den Signator zur Änderung in eine PIN auf. Erst unter Authentikation mit dieser PIN ist eine Signatur möglich.

Der Signator kann innerhalb einer bestimmten Frist nach Erhalt des PIN- und Passwort-Kuverts einen Nachdruck beantragen.

## **6.4.2 Schutz der Aktivierungsdaten**

### **6.4.2.1 Aktivierungsdaten für Schlüssel der Zertifizierungsstelle**

Die Mitarbeiter, 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 Signatoren**

Die Chipkarte verhindert das Auslesen der PIN.

Die Initial-PIN, welche im PIN-Brief an den Signator versandt wird, ermöglicht noch keine Signaturausführung. Mit Hilfe dieser Initial-PIN muss der Signator seine persönliche PIN für die Durchführung der Signatur individuell wählen und kann danach Signaturen durchführen. Lehnt das System die Eingabe der im Brief abgedruckten Initial-PIN ab, so ist der Signator verpflichtet, dies der Zertifizierungsstelle zu melden.

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

### **6.4.3.1 Aktivierungsdaten für Schlüssel der Zertifizierungsstelle**

Die Schlüssel der Zertifizierungsstelle, welche sich in Hardware-Security Modulen befinden, werden von zwei Security Officers im Vier-Augen-Prinzip aktiviert. Die einmal aktivierten Schlüssel sind so lange aktiv bis sie deaktiviert werden.

### **6.4.3.2 Aktivierungsdaten für Schlüssel der Signatoren**

Die Länge der PIN beträgt sechs bis acht Ziffern. Für jede digitale Signatur ist diese PIN vom Signator einzugeben.

Die PIN kann nicht auf die Initial-PIN zurückgeändert werden, da diese nur aus vier Stellen besteht und daher für die Signaturerstellung ungeeignet ist.

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

## **6.6.2 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
- Mitarbeiter werden vor der Programmnutzung auf die Verwendung geschult
- Handbücher müssen in ausreichender Zahl zur Verfügung stehen
- Original-Software-Versionen werden sicher aufbewahrt
- Ggf. werden Sicherungskopien von Software angelegt
- Unerlaubte Zugriffe auf Software z. B. zur Erstellung von Raubkopien müssen verhindert werden.
- Regelungen für den Betrieb werden erlassen (Durchführung von Datensicherungen, Wechsel von Passwörtern)

## **6.6.3 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 kryptographischen Moduls**

Wartungsarbeiten finden ausschließlich im Vier-Augen-Prinzip 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**

Die von A-Trust für trust|sign verwendeten Zertifikate sind X.509 V3 Zertifikate.

### 7.1.1 A-Trust CA-Zertifikate

Attribut	Inhalt	Erläuterung
Version	v3(2)	Die Versionsnummer wird auf „2“ gesetzt, um ein X.509 Zertifikat der Version 3 anzuzeigen
Seriennummer	Seriennummer des Zertifikats	Eindeutig innerhalb der A-Trust Zertifizierungsinfrastruktur
Algorithmus	SHA-1	Für die Signatur über das Zertifikat verwendeter Algorithmus
Aussteller des Zertifikats	CN = A-Trust-Qual-nn OU = A-Trust-Qual-nn O = A-Trust C = AT	-nn bezeichnet die Version der CA, die die Signatur über das Zertifikat erstellt hat
Gültig von Gültig bis	Beginn und Ende der Gültigkeit des Zertifikats	Der Gültigkeitszeitraum beträgt höchstens drei Jahre
Zertifikatsinhaber	CN = TrustSign-Sig-nn OU = TrustSign-Sig-nn O = A-Trust C = AT	-nn bezeichnet die Version der CA, die den zertifizierten Schlüssel besitzt
Öffentlicher Schlüssel	RSA 2048 Bit	Öffentlicher Schlüssel des Signators

**Tabelle 8 Profil für CA-Zertifikat**

## 7.1.2 Zertifikate für Signatoren

Attribut	Inhalt	Erläuterung
Version	v3(2)	Die Versionsnummer wird auf „2“ gesetzt, um ein X.509 Zertifikat der Version 3 anzuzeigen
Seriennummer	Seriennummer des Zertifikats	Eindeutig innerhalb der A-Trust Zertifizierungsinfrastruktur
Algorithmus	SHA-1	Für die Signatur über das Zertifikat verwendeter Algorithmus
Aussteller des Zertifikats	CN = TrustSign-Sig-nn OU = TrustSign-Sig-nn O = A-Trust C = AT	-nn bezeichnet die Version der CA, die die Signatur über das Zertifikat erstellt hat
Gültig von Gültig bis	Beginn und Ende der Gültigkeit des Zertifikats	Der Gültigkeitszeitraum beträgt höchstens drei Jahre
Zertifikatsinhaber	C = CountryName T = Title SN = SurName G = GivenName CN = CommonName Seriennummer = SerialNumber	CountryName: AT etc. Title: Titel (Dr. etc.) SurName: Zuname GivenName: Vorname CommonName: entweder Vorname + Zuname oder Pseudonym Titel, Zuname, Vorname entfallen bei Verwendung eines Pseudonyms SerialNumber: eindeutige Identifikationsnummer des Signators (CIN)
Öffentlicher Schlüssel	RSA 1024 Bit	Öffentlicher Schlüssel des Signators

**Tabelle 9 Profil für trust|sign Zertifikat**

### 7.1.3 Erweiterungen (certificate extensions)

In den Zertifikaten der A-Trust CAs werden die folgenden Erweiterungen gemäß X.509 V3 und PKIX verwendet:

Erweiterung	Zertifikatstyp		Klassifikation	
	Root	CA	kritisch	Nicht kritisch
<b>Standard-erweiterungen</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
qc-Statement	Ja	Ja	X	

**Tabelle 10 Erweiterungen (CA-Zertifikate)**

Die Verwendung von Erweiterungen in Signator-Zertifikaten wird in der folgenden Tabelle dargestellt:



Erweiterung	Im Zertifikat vorhanden	Klassifikation	
		kritisch	Nicht kritisch
<b>Standarderweiterungen</b>			
authorityKeyIdentifier	Ja		X
subjectKeyIdentifier	Ja		X
keyUsage	Ja	X	
extKeyUsage	Ja		X
certificatePolicies	Ja		X
subjectAltName	Optional		X
basicConstraints	Ja		X
cRLDistributionPoints	Ja		X
subjectDirectoryAttributes	Optional		X
<b>Private Extensions</b>			
authorityInfoAccess	Ja		X
qc-Statement	Ja	X	

**Tabelle 11 Erweiterungen (trust|sign Zertifikat)**

Die Erweiterung subjectDirectoryAttributes enthält bei trust|sign Zertifikaten optional das Geburtsdatum des Signators.

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

## 7.1.4 Namensformen

Die Verwendung von Namensfeldern erfolgt gemäß der Bestimmungen in Abschnitt 3.1.1.

## 7.1.5 Identifikation der Policy

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

Die Erweiterung certificatePolicies im Zertifikat wird mit

- OID 0.4.0.1456.1.1 gem. [ETSI]  
itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(1456)  
policy-identifiers(1) qcp-public-with-sscd (1)

und mit

- OID 1.2.040.0.17.1.1 gem. [Policy]  
1.2.040.0.17 (A-Trust).1 (Policy).1 (trust|sign).1.0 (Version) vorliegende  
Version

codiert.

## 7.1.6 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.

## **8 Administration dieser Spezifikation**

### **8.1 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 Signatoren erfordern, benötigen eine Anpassung der OID der Certificate Policies und der URI der Zertifizierungsrichtlinie und damit eine generelle Bekanntmachung gegenüber den Signatoren. Dies sind insbesondere Änderungen, die

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

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

### **8.2 Verfahren zur Publizierung und Bekanntgabe**

Eine Bekanntgabe von Änderungen wird mit einem Vorlauf von 2 Monaten vorgenommen. Nach einer Änderung können weiterhin alte Versionen der Zertifizierungsrichtlinie und der Certificate Policy - wie in Abschnitt 2.6. beschrieben – abgerufen werden.

### **8.3 Genehmigung und Eignung einer Zertifizierungsrichtlinie**

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

## 9 Anhang

### A **Glossar**

Aktivierungsdaten	Daten, die zur Aktivierung der Schlüssel benötigt werden (PIN).
Anwender	Person, die die Dienstleistungen der Zertifizierungsstelle der A-Trust nutzt. Anwender sind sowohl Zertifikatsinhaber als auch Zertifikatsnutzer.
Audit	Von externen Personen durchgeführte Sicherheitsüberprüfung.
CA (Certification Authority), Zertifizierungsdiensteanbieter	Eine Person oder Stelle, die Zertifikate ausstellt oder anderweitige elektronische Signaturdienste öffentlich anbieten darf.
CA-Schlüssel	Schlüssel der CA, die zur Ausstellung von Zertifikaten und dem Unterschreiben von Widerrufslisten (Zertifizierung) verwendet werden.
Certification Policy, Policy	Ein Regelwerk, das den Einsatzbereich eines Zertifikates für eine bestimmte Benutzergruppe und/oder Anwendungsklasse festhält.
Certification Practice Statement, CPS, Zertifizierungsrichtlinie	Aussagen über die bei der Ausstellung von Zertifikaten von einem Zertifizierungsdiensteanbieter eingehaltene Vorgehensweise
Dienste (CA-Dienste)	Überbegriff für angebotene Dienstleistungen wie Verzeichnisdienst, Statusauskunft und Zeitstempeldienst
Dienste-Schlüssel	Schlüssel eines Dienstes (z. B. Signaturschlüssel zur Signatur von Statusauskünften)
Digitale Signatur	Elektronische Signatur, die mit Hilfe von Verfahren der asymmetrischen Kryptographie erzeugt wird.
E-Mail	Electronic Mail; Nachrichten, die in digitaler Form über computerbasierte Kommunikationswege versandt oder empfangen werden.

Elektronische Signatur	Eine Signatur in digitaler Form, die in Daten enthalten ist, Daten beigefügt wird oder logisch mit ihnen verknüpft ist und von einem Unterzeichner verwendet wird, um zu bestätigen, dass er den Inhalt dieser Daten billigt. Sie ist so mit den Daten verknüpft, dass eine nachträgliche Veränderung der Daten offenkundig wird.
Gültigkeitsmodell	Modell nach dem die Prüfung der Gültigkeit von Zertifikaten und Signaturen vorgenommen wird.
Hardware Security Modul, HSM	Elektronisches System zur sicheren Speicherung von Schlüsseln und zur Berechnung und Verifizierung von Signaturen.
Integrität (von Daten)	Ein Zustand, in dem Daten weder von Unbefugten verändert noch zerstört wurden.
Kettenmodell	<i>Gültigkeitsmodell</i> 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 Schlüsselpaars. 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 Teil eines Schlüsselpaars, der zum digitalen Signieren sowie zum Entschlüsseln von Nachrichten/Dokumenten erforderlich ist und geheim gehalten werden muss.

Public-Key Infrastructure, PKI	Ein kryptographisches System, das ein Paar von durch einen mathematischen Algorithmus verbundenen Schlüsseln benutzt. Der öffentliche Teil dieses Schlüsselpaars kann jedermann zugänglich gemacht werden, der Informationen verschlüsseln oder eine digitale Signatur prüfen will, der geheime Teil wird von seinem Besitzer sicher bewahrt und kann Daten entschlüsseln oder eine digitale Signatur erstellen.
Qualifiziertes Zertifikat	Zertifikat, welches den Bestimmungen des § 5 des Österr. Signaturgesetzes entspricht.
Registrierungsstelle, Registration Authority, RA	Eine vertrauenswürdige Einrichtung, welche die Überprüfung der Identität der Zertifikatsbewerber im Namen des Zertifizierungsdiensteanbieters unter Berücksichtigung der Zertifizierungsrichtlinien durchführt und selbst keine Zertifikate ausstellt.
RFC	Request for Comments, Artikel über Standards und Protokolle im Internet. Neue Standards werden zunächst vorgeschlagen und zur Diskussion gestellt (daher "mit der Bitte um Stellungnahme"). Erst nachdem sie ausdiskutiert und für gut befunden worden sind, werden sie unter einer RFC-Nummer veröffentlicht.
Root-CA	Die Root-CA ist die oberste CA in der Zertifizierungshierarchie der A-Trust. Sie stellt die Zertifikate für die nachgeordneten CAs aus.
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.
Signator	Eine Person, die eine elektronische Signatur erstellt, Zertifikatsinhaber
Signaturerstellungsdaten	Signaturerstellungsdaten sind einmalige Daten wie Codes oder private Signaturschlüssel, die von dem Signator zur Erstellung einer elektronischen Signatur verwendet werden.

Signaturprüfdaten	Signaturprüfdaten sind Daten wie Codes oder öffentliche Signaturschlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden.
Sperre	Eine Sperre ist ein zeitlich begrenztes vorübergehendes Aussetzen der Gültigkeit eines Zertifikats der trust sign-Karte.
Statusauskunft	Dienst, bei dem die Anwender Auskunft über den aktuellen Status (gültig oder gesperrt) eines Zertifikates abrufen können.
trust sign-Karte	Eine Prozessorchipkarte, die geheime Schlüssel des Karteninhabers enthält und zur Erstellung und Verifizierung digitaler Signaturen dient.
URI	Uniform Resource Identifier, spezifiziert eine bestimmte Datei auf einem bestimmten Server, Oberbegriff für URL (Uniform Resource Locator) und URN (Universal Resource Name).
Verifizierung (einer digitalen Signatur)	Feststellung, dass eine digitale Signatur mit dem privaten Schlüssel, der zu dem in einem gültigen Zertifikat beinhalteten öffentlichen Schlüssel gehört, erstellt wurde und die Nachricht sich nach der Signatur nicht verändert hat.
Verzeichnis (-dienst)	Dienst, bei dem die Anwender Zertifikate der CA oder anderer Anwender sowie CRLs abrufen können. Der Zugriff wird über LDAP realisiert.
Widerruf	Der irreversible Vorgang der vorzeitigen Beendigung der Gültigkeit eines Zertifikats ab einem bestimmten Zeitpunkt.
X.509	Der ITU-Standard für Zertifikate. X.509 v3 beschreibt Zertifikate, die mit verschiedenen Zertifikats-erweiterungen erstellt werden können
Zeitstempel	Digitale Signatur von digitalen Daten und einem Zeitpunkt. Mit Hilfe eines Zeitstempels kann nachgewiesen werden, dass digitale Dokumente zu einem bestimmten Zeitpunkt existiert haben. Um Manipulationen zu verhindern, soll der Zeitstempel nur von einer vertrauenswürdigen Instanz (z. B. Zertifizierungsstelle) ausgestellt werden.
Zertifikatsinhaber	Anwender, dessen Schlüssel und persönliche Daten im Zertifikat der A-Trust festgehalten sind. Auch Signator genannt.



Zertifikatsnutzer, Signaturempfänger	Anwender, der Zertifikate über die Schlüssel und Daten anderer nutzt, um Signaturen zu prüfen.
Zertifikats-Widerrufsliste, CRL	Eine digital signierte Datenstruktur, die widerrufen und gesperrte Zertifikate anführt, welche von einem bestimmten Zertifizierungsdiensteanbieter ausgestellt wurden.

## B Referenzen

[Policy]	Certificate Policy für qualifizierte trust sign Zertifikate, Version 1.0
[ETSI]	Policy requirements for certification authorities issuing qualified certificates – ETSI TS 101 456, V1.1.1 (2000-12)
[SigG]	Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG). BGBl. I Nr. 190/1999 (NR: GP XX RV 1999 AB 2065 S. 180. BR: AB 6065 S. 657.)
[SigV]	Verordnung zum Signaturgesetz, BGBl II 2000/30, 02. 02. 2000
[SigRL]	Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, 13. 12. 1999
[DSG]	Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000). BGBl. I Nr. 165/1999 (NR: GP XX RV 1613 AB 2028 S. 179. BR: 5992 AB 6034 S. 657.)
[FIPS 140-1]	FIPS PUB 140-1, Security Requirements For Cryptographic Modules, 1994 January 11
[RFC2527]	RFC 2527, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, March 1999
[A-SIT-Karte]	A-SIT Bescheinigung nach §18(5) SigG: Smart Card mit Chip Philips Smart Card Controller P8WE5032V0G und Betriebssystem STARCOS SPK 2.3 und Digital Signature Application TrustSign, 22.10.2001