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

a.trust

Certification Practice Statement für einfache Zertifikate a·sign Company Root

Version: 1.0.2

Datum: 10.12.2004

Inhaltsverzeichnis

1 Einleitung 11
1.1 Überblick 11
1.2 Dokumentidentifikation 11
1.3 Zertifizierungsinfrastruktur und Anwendbarkeit 12
1.3.1 Zertifizierungsstellen 12
1.3.2 Registrierungsstellen 12
1.3.3 Widerrufsdienst 12
1.3.4 Anwender 12
1.3.5 Anwendbarkeit 12
1.3.6 Zertifizierungshierarchie 14
1.3.7 a.trust Verzeichnisbaum 14
1.4 Ansprechpartner und Kontaktstellen 15
1.4.1 Organisation zur Verwaltung dieses Dokuments 15
1.4.2 Kontaktinformation 15
1.4.3 Verantwortlichkeit für die Anerkennung anderer Policies 16
2 Generelle Bestimmungen 17
2.1 Verpflichtungen 17
2.1.1 Verpflichtungen der Zertifizierungsstellen 17
2.1.2 Verpflichtungen der Registrierungsstellen 17
2.1.3 Verpflichtungen der Zertifikatsinhaber 18
2.1.4 Verpflichtungen der Zertifikatsnutzer 19
2.1.5 Verpflichtungen der Verzeichnisdienste 19
2.2 Haftung 20

2.2.1 Haftung der Zertifizierungsstelle 20
2.2.2 Haftung der Registrierungsstelle 20
2.3 Auslegung und (gerichtliche) Durchsetzung 21
2.3.1 Zugrunde liegende Gesetzesbestimmungen 21
2.3.2 Trennbarkeit der Bestimmungen, Fortbestehen von Ansprüchen, Fusion, Kündigung 21
2.4 Gebühren 21
2.4.1 Ausgabe und Erneuerung von Zertifikaten 21
2.4.2 Abrufen von Zertifikaten 22
2.4.3 Widerruf von Zertifikaten 22
2.4.4 Abrufen von Statusinformationen 22
2.4.5 Richtlinien für Gebührenrückerstattung 22
2.5 Bekanntmachung und Verzeichnisdienste 22
2.5.1 Web-Seiten und Verzeichnisse 22
2.5.2 a.trust Stammzertifikat 23
2.5.3 a.trust CA-Zertifikat 23
2.5.4 Widerrufsinformationen 23
2.5.5 Veröffentlichung von Informationen der Zertifizierungsstelle 24
2.5.6 Frequenz der Aktualisierung 25
2.5.7 Zugriffskontrollen 25
2.5.8 Verzeichnisse 25
2.6 Interne Prüfung (Audit) 26
2.6.1 Häufigkeit des Audits 26
2.6.2 Identität bzw. Anforderungen an den Auditor 26
2.6.3 Beziehungen zwischen Auditor und zu untersuchender Partei 26

2.6.4 Aspekte des Audits 26
2.6.5 Handlungen nach unzureichendem Ergebnis 26
2.6.6 Bekanntgabe der Ergebnisse 27
2.7 Vertraulichkeit 27
2.7.1 Vertraulich eingestufte Informationen 27
2.7.2 Nicht vertraulich eingestufte Informationen 27
2.7.3 Offenlegung von Informationen zu Zertifikatswiderruf 27
2.7.4 Offenbarung an Behörden im Rahmen gesetzlicher Pflichten 27
2.7.5 Offenbarung im Rahmen zivilrechtlicher Auskunftspflichten 28
2.7.6 Weitere Gründe zur Freigabe von vertraulichen Informationen 28
2.8 Urheberrechte und Eigentumsrechte 28
3 Identifizierung und Authentisierung 29
3.1 Erstregistrierung 29
3.1.1 Namenstypen 29
3.1.2 Eindeutigkeit der Namen 29
3.1.3 Methode zum Beweis des Besitzes des geheimen Schlüssels 29
3.1.4 Authentisierung von Organisationen 30
3.1.5 Authentisierung von Individuen 30
3.2 Erneute Registrierung/Rezertifizierung 30
3.3 Erneute Registrierung nach Widerruf 31
3.4 Widerrufsantrag 31
4 Betriebliche Anforderungen 32
4.1 Antrag auf Ausstellung von Zertifikaten 32
4.2 Herausgabe und Akzeptanz von Zertifikaten 32
4.3 Widerruf 32

4.3.1 Gründe für einen Widerruf 32
4.3.2 Wer kann einen Widerruf anordnen 33
4.3.3 Prozedur für einen Widerrufsantrag 33
4.3.4 Frist bis zur Bekanntgabe des Widerrufs 34
4.3.5 Aktualisierungsfrequenz der Widerrufsliste 34
4.3.6 Anforderungen an die Überprüfung durch Widerrufslisten 34
4.3.7 Möglichkeiten zur online Statusabfrage 35
4.3.8 Anforderungen an die Statusabfrage 35
4.3.9 Spezielle Verfahren bei Kompromittierung 35
4.4 Protokollierung sicherheitsrelevanter Ereignisse 35
4.4.1 Protokollierte Ereignisse 35
4.4.2 Frequenz der Überprüfung der Protokolldateien 36
4.4.3 Aufbewahrungszeitraum der Protokolldateien 36
4.4.4 Schutz der Protokolldateien 37
4.4.5 Protokollierungssystem (intern/extern) 37
4.4.6 Benachrichtigung beim Auftreten sicherheitskritischer Ereignisse 37
4.5 Archivierung 37
4.5.1 Archivierte Daten 37
4.5.2 Aufbewahrungszeiten 38
4.5.3 Schutzvorkehrungen 38
4.5.4 Anforderungen, die Daten mit Zeitstempeln zu versehen 38
4.5.5 System zur Erfassung der Archivierungsdaten (intern / extern) 39
4.5.6 Prozeduren zum Abrufen und Überprüfen von Daten 39
4.6 Schlüsselwechsel von CA-Schlüsseln 39
4.7 Kompromittierung und Notfallplan 40

4.7.1 Rechner, Software und/oder Daten sind korrumpiert 40
4.7.2 Widerruf von Zertifikaten zu Zertifizierungsstellen- und Dienste-Schlüsseln 40
4.7.3 Schlüsselkompromittierung bzw. Verdacht auf Schlüsselkompromittierung 42
4.7.4 Sicherheitsvorkehrungen nach Katastrophen 42
4.8 Einstellung der Tätigkeit der Zertifizierungsstelle 43
5 Physische, verfahrensorientierte und personelle Sicherheitsvorkehrungen . 44
5.1 Physische Sicherheitsvorkehrungen 44
5.1.1 Standort und örtliche Gegebenheiten 44
5.1.2 Zugangskontrollen 44
5.1.3 Stromversorgung und Klimaanlage 45
5.1.4 Wasserschäden 45
5.1.5 Feuer 45
5.1.6 Datenträger 45
5.1.7 Müllentsorgung 46
5.1.8 Redundante Auslegung 46
5.2 Verfahrensorientierte Sicherheitsvorkehrungen 46
5.2.1 Funktionen der a.trust 47
5.2.2 Sicherheitskritische Funktionen 47
5.2.3 Sonstige (nicht sicherheitskritische) Funktionen 48
5.2.4 Anzahl erforderlicher Personen für sicherheitsrelevante Tätigkeiten 49
5.2.5 Identifikation und Authentisierung der Rollen 50
5.3 Personelle Sicherheitsvorkehrungen 50
5.3.1 Anforderungen an das Personal 50
5.3.2 Überprüfung des Personals 51
5.3.3 Anforderungen an die Schulung 51

5.3.4 Anforderungen und Häufigkeit von Schulungswiederholungen 51
5.3.5 Sanktionen für unautorisierte Handlungen 51
5.3.6 Anforderungen an Vertragsvereinbarungen mit dem Personal 51
5.3.7 An das Personal auszuhändigende Dokumente 52
6 Technische Sicherheitsvorkehrungen 53
6.1 Schlüsselgenerierung und Installation 53
6.1.1 Schlüsselgenerierung 53
6.1.2 Auslieferung privater Schlüssel an Zertifikatsinhaber 53
6.1.3 Auslieferung öffentlicher Schlüssel an die Zertifikatsinhaber 54
6.1.4 Schlüssellängen 54
6.1.5 Parameter zur Schlüsselerzeugung 55
6.1.6 Qualitätsprüfung der Parameter 55
6.1.7 Hardware/Software Schlüsselerzeugung 55
6.1.8 Verwendungszweck der Schlüssel (nach X.509 v3 key usage Feld) 55
6.2 Schutz der privaten Schlüssel 56
6.2.1 Schutz des Schlüssels der Zertifizierungsstelle 56
6.2.2 Schutz der Schlüssel der Zertifikatsinhaber 57
6.2.3 Aktivierung privater Schlüssel durch mehrere Personen 57
6.2.4 Hinterlegung privater Schlüssel 57
6.2.5 Backup privater Schlüssel 57
6.2.6 Archivierung privater Schlüssel 57
6.2.7 Einbringung privater Schlüssel in das kryptographische Modul 58
6.2.8 Methode zur Deaktivierung privater Schlüssel 58
6.3 Weitere Aspekte zum Schlüsselmanagement 58
6.3.1 Archivierung öffentlicher Schlüssel 58

6.3.2 Verwendungszeitraum öffentlicher und privater Schlüssel 58
6.4 Aktivierungsdaten 59
6.4.1 Erzeugung und Installation der Aktivierungsdaten (PINs) für Zertifizierungsschlüssel 59
6.4.2 Schutz der Aktivierungsdaten 59
6.5 Lebenszyklus der Sicherheitsvorkehrungen 60
6.5.1 Systementwicklung 60
6.5.2 Sicherheitsmanagement 60
6.5.3 Bewertung 60
6.6 Vorkehrungen zur Netzwerksicherheit 60
6.7 Vorkehrungen zur Wartung (Analyse) des kryptographischen Moduls 60
7 Profile von Zertifikaten und Widerrufslisten 61
7.1 Zertifikatsprofile 61
7.1.1 CA-Zertifikat a.sign Company Root 61
7.1.2 Zertifikate für Zertifikatsinhaber 62
7.1.3 Erweiterungen (certificate extensions) 63
7.2 Profil der Widerrufsliste 64
7.2.1 Versionsnummern 64
7.2.2 a.trust CRL und CRL Entry Extensions 64
8 Administration dieser Spezifikation 65
8.1 Prozeduren zur Änderung dieses Dokuments 65
8.2 Verfahren zur Publizierung und Bekanntgabe 65
8.3 Genehmigung und Eignung einer Zertifizierungsrichtlinie 66
9 Anhang 67

Tabellenverzeichnis

Tabelle 1 a.trust Homepage und Verzeichnisdienste 22

Tabelle 2 Standorte 44

Tabelle 3 Funktionen der a.trust 47

Tabelle 4 Sicherheitskritische Funktionen 48

Tabelle 5 Sonstige Funktionen 48

Tabelle 6 Anzahl erforderlicher Personen 50

Tabelle 7 Gültigkeitsdauer von Zertifikaten 59

Tabelle 8 Profil für CA-Zertifikat 62

Tabelle 9 Profil für a.sign Company Root 62

Tabelle 10 Erweiterungen Qual Root CA und a.sign Company Root CA 63

Tabelle 11 Erweiterungen (Signatorzertifikat) 63

Abbildungsverzeichnis

Abbildung 1 Zertifizierungshierarchie 14

Abbildung 2 a.trust Verzeichnisbaum 14

1 Einleitung

1.1 Überblick

Das Ziel der vorliegenden Zertifizierungsrichtlinie besteht darin, die Umsetzung der Ausgabe, Administration und Anwendung von a.sign Company Root Zertifikaten derart festzulegen, dass eine sichere und zuverlässige Durchführung der angebotenen Zertifizierungsdienstleistungen sowie der Anwendung der ausgegebenen Zertifikate gewährleistet ist.

Die Zertifizierungsrichtlinie gibt Auskunft über die Praktiken der Zertifizierungsstelle zur Ausgabe von a.sign Company Root Zertifikaten. Sie dient dazu, die Vorgangsweise intern zu fixieren und den Anwendern die Vorgehensweise der Zertifizierungsstelle zu erläutern. Somit können sich die Anwender auch 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:	a.trust Certification Practice Statement für einfache Zertifikate a.sign Company Root
Version:	1.0.2/10.12.2004
Object Identifier:	**1.2.040.0.17** (a.trust) **.2** (CPS) **.15** (a.sign Company Root Zertifikate) **.1.0.2** (Version) vorliegende Version

1.3 Zertifizierungsinfrastruktur und Anwendbarkeit

1.3.1 Zertifizierungsstellen

Es existiert eine zentrale Zertifizierungsstelle, die die Schlüssel für die Zertifikatsinhaber sowie die Widerrufslisten zu diesen Zertifikaten signiert.

1.3.2 Registrierungsstellen

In den Registrierungsstellen führen Registration Officers (ROs) die anwenderrelevanten Arbeiten durch. Diese Aufgaben umfassen neben der Identifizierung auch die Bearbeitung der Zertifikatsinhaberdaten und die Weiterleitung von Informationen an die übergeordnete Zertifizierungsstelle.

1.3.3 Widerrufsdienst

Die Zertifikatsinhaber können sich zum Zweck der Durchführung des Widerrufs ihres Zertifikats an den Widerrufsdienst wenden.

1.3.4 Anwender

Unter „Anwender“ sind einerseits die Zertifikatsinhaber zu verstehen, deren öffentlicher Schlüssel mit dem a.sign Company Root Zertifikat der a.trust zertifiziert ist und andererseits jene Personen, die diese Zertifikate nutzen bzw. auf die Korrektheit der Zertifikatsangaben vertrauen.

1.3.5 Anwendbarkeit

Dieses Dokument ist relevant für die Zertifizierungsstelle und die Registrierungsstelle, wie auch die Dienstleistungen der Zertifizierungs- und Registrierungsstelle und für die Anwender.

Die folgenden Zertifikate unterliegen dieser Zertifizierungsrichtlinie:

- a.sign Company Root Zertifikat, mit dem das Zertifikat des Zertifikatsinhabers (Unternehmens) ausgestellt wird,
- Zertifikate, die mit dem privaten Schlüssel des a.sign Company Root Zertifikats signiert wurden und den Zertifikatsinhabern zur Signatur von Benutzerzertifikaten dienen.

Die Registrierung, Ausstellung und sämtliche Sicherheitsmaßnahmen betreffend Zertifikate für Endbenutzer, sowie organisatorische, personelle und qualitätssichernde Maßnahmen der unter a.sign Company Root angesiedelten CA des Zertifikatsinhabers werden im Detail in dessen Certificate Policy, Certification Practice Statement und Sicherheitskonzept beschrieben.

Die Generierung der Schlüssel der Zertifikatsinhaber wird von diesen selbst in sicherer Weise vorgenommen. Dazu ist ein nach allgemeinen Prüfungskriterien wie z. B. ITSEC, Common Criteria for Information Technology Security Evaluation oder FIPS 140-1 etc. evaluiertes und zertifiziertes bzw. von einer Bestätigungsstelle (z. B. A-SIT) bestätigtes/bescheinigtes Hardware Security Modul zu verwenden. Der Besitz des Hardware Security Moduls muss a.trust bei der Zertifikatsbestellung durch Vorlage von Verträgen oder Rechnungen nachgewiesen werden. Die Zertifizierungsunterlagen müssen der Registrierungsstelle vorgelegt werden und der Zertifikatswerber muss a.trust auf deren Verlangen eine Einsichtnahme in die Verwendung des Hardware Security Moduls vor Ort ermöglichen.

1.3.6 Zertifizierungshierarchie

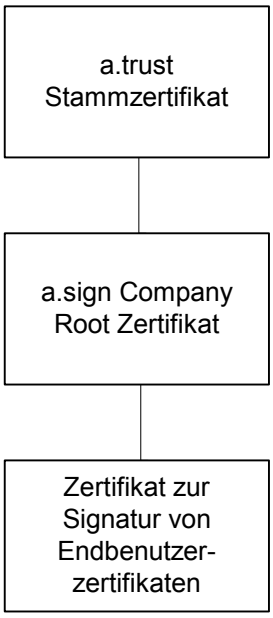

Abbildung 1 Zertifizierungshierarchie

1.3.7 a.trust Verzeichnisbaum

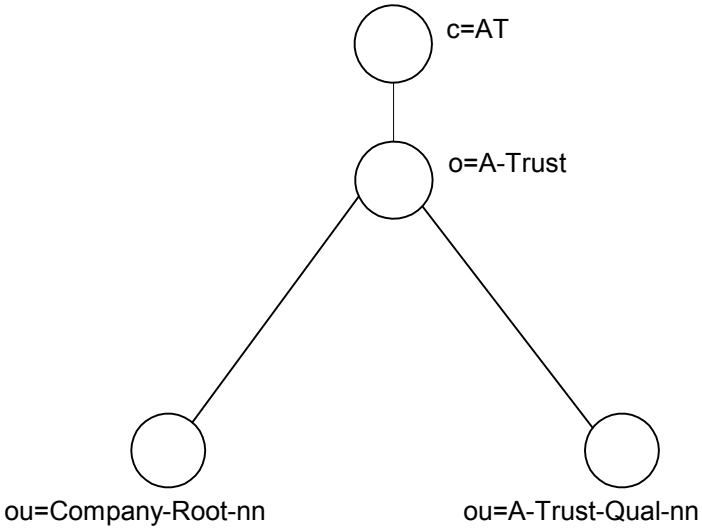

Abbildung 2 a.trust Verzeichnisbaum

Das Zertifikat des Schlüssels A-Trust-Qual-nn ist das a.trust Stammzertifikat, wobei -nn die Version der Root-CA bezeichnet, welche mit dem zugehörigen geheimen Schlüssel digitale Signaturen erstellt.

Mit A-Trust-Qual-nn ab Version 02 wird das a.sign Company Root Zertifikat und die zugehörige CRL signiert.

Für Zertifikate, die zu einem früheren Zeitpunkt (vor Inbetriebnahme der CA-Version 02) ausgestellt wurden, ist die Root-CA A-Trust-nQual-01 gültig.

Der private Schlüssel des a.sign Company Root Zertifikats Company-Root-nn signiert die Zertifikate der Zertifikatsinhaber und die zugehörige CRL.

1.4 Ansprechpartner und Kontaktstellen

1.4.1 Organisation zur Verwaltung dieses Dokuments

a.trust ist für die Organisation und Verwaltung der Zertifizierungsrichtlinie verantwortlich.

1.4.2 Kontaktinformation

Kontaktinformationen zu a.sign Company Root Zertifikaten erhält man auf folgenden Wegen:

- Auf der Homepage von a.trust:
  http://www.a-trust.at/
- bei der Informationshotline des Call Centers:
  Telefonnummer siehe Homepage
- in ausgewählten Registrierungsstellen der a.trust (Kontaktinformationen siehe Homepage) und
- auf schriftliche Anfrage an:
  A-Trust
  Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH.
  Landstraßer Hauptstraße 5
  A-1030 Wien

1.4.3 Verantwortlichkeit für die Anerkennung anderer Policies

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 dieser Zertifizierungsrichtlinie, die sich insbesondere auf die folgenden Aspekte erstreckt:

- Die Zertifikate der Zertifikatsinhaber, welche von a.sign Company Root zertifiziert werden, werden im Einklang mit dieser Zertifizierungsrichtlinie erstellt und können widerrufen oder erneuert (Verlängerung der Gültigkeitsdauer) werden.
- Die Zertifizierungsstelle arbeitet im Einklang mit dem der Aufsichtsbehörde vorgelegten Sicherheits- und Zertifizierungskonzept.
- Die Zertifizierungsstelle beschäftigt Personal mit angemessener Qualifikation.
- Die Zertifizierungsstelle kommt ihrer Informationspflicht hinsichtlich Zertifikatsinhaber 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 a.sign Company Root erfolgt ausschließlich zum Signieren der Zertifikate der Zertifikatsinhaber und zum Signieren der zugehörigen Widerrufsliste.
- Die Zertifizierungsstelle veröffentlicht alle ausgestellten Zertifikate sowie alle widerrufenen Zertifikate.

2.1.2 Verpflichtungen der Registrierungsstellen

Die Registrierungsstellen der a.trust befolgen die Regelungen dieser Zertifizierungsrichtlinie, die sich insbesondere auf die folgenden Aspekte erstrecken:

- Die Registrierungsstellen arbeiten im Einklang mit dem der Aufsichtsbehörde vorgelegten Sicherheits- und Zertifizierungskonzept.

- Die Registrierungsstellen stellen die Einhaltung der Identifikations- und Authentikationsmechanismen sicher, die in dieser Zertifizierungsrichtlinie beschrieben sind.
- Die Registrierungsstellen beschäftigen Personal mit angemessener Qualifikation.
- Die Registrierungsstelle übermittelt das von a.sign Company Root ausgestellte Zertifikat in elektronischer Form an den Zertifikatsinhaber. a.trust stellt dem Zertifikatsinhaber insbesondere folgende Dokumente elektronisch zur Verfügung:
  - Vertragsbedingungen,
  - Entgeltbestimmungen sowie
  - Certificate Policy, Certification Practice Statement.

2.1.3 Verpflichtungen der Zertifikatsinhaber

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

- Die Zertifikatsinhaber verpflichten sich, die gegenständliche Zertifizierungsrichtlinie zusammen mit der zutreffenden Certificate Policy als Grundlage für den abgeschlossenen Vertrag anzuerkennen.
- Die Certificate Policy und das Certification Practice Statement für die von ihm ausgestellten Benutzerzertifikate erstellt der Zertifikatsinhaber und er ist für ihre Aktualisierung und Veröffentlichung verantwortlich.
- Der Inhaber des von a.sign Company Root ausgestellten Zertifikates ist verpflichtet, nur die Hardware, die bei der Antragstellung an a.trust mitgeteilt bzw. deren Verwendung nachgewiesen wurde, zur Erzeugung und Aufbewahrung des privaten Schlüssels zu verwenden. Sind Änderungen beabsichtigt, muss er a.trust umgehend benachrichtigen.
- Der Inhaber des von a.sign Company Root ausgestellten Zertifikates ist für die Richtigkeit der Angaben verantwortlich, die er bei der Registrierung macht und wirkt gemäß den in dieser Zertifizierungsrichtlinie angegebenen Verfahren zur Identitätsfeststellung und Authentifizierung mit.

- Der Zertifikatsinhaber ist verpflichtet, seinen privaten Schlüssel angemessen zu schützen. Dies umfasst insbesondere keinen Zugriff durch unautorisierte Personen auf den privaten Schlüssel zuzulassen und die Aktivierungsdaten des privaten Schlüssels (PIN) nicht weiterzugeben.

- Falls nötig, initiiert der Zertifikatsinhaber unverzüglich den Widerruf seines Zertifikats.

- Der Zertifikatsinhaber setzt sein Zertifikat nur zur Signatur von Benutzerzertifikaten und der dazu gehörigen CRLs ein.

- Der Inhaber des von a.sign Company Root ausgestellten Zertifikates ist verpflichtet, die jeweiligen nationalen Ausfuhrbestimmungen sowie etwaige nationale Nutzungsbeschränkungen bei einer Verwendung im Ausland zu beachten.

- Der Inhaber des von a.sign Company Root ausgestellten Zertifikates legt a.trust ein Sicherheits- und ein Betriebskonzept und arbeitet im Einklang mit diesen Dokumenten.

- Er beschäftigt Personal mit angemessener Qualifikation.

- Der Inhaber Inhaber des von a.sign Company Root ausgestellten Zertifikates kommt seiner Informationspflicht hinsichtlich Signatoren, Aufsichtsbehörden und a.trust nach.

2.1.4 Verpflichtungen der Zertifikatsnutzer

Die Zertifikatsnutzer verpflichten sich, vor der Akzeptanz eines Zertifikats folgende Prüfungen durchzuführen:

- Der Zertifikatsnutzer prüft die Gültigkeit des Zertifikats.

- Die Zertifikatsnutzer überprüft, ob das Zertifikat zweckgemäß eingesetzt wurde.

2.1.5 Verpflichtungen der Verzeichnisdienste

Der Verzeichnisdienst veröffentlicht in regelmäßigen Abständen Listen mit

- ausgestellten Zertifikaten und

- widerrufenen Zertifikaten.

Der Verzeichnisdienst ist verpflichtet, diese Listen in regelmäßigen Abständen zu aktualisieren und hochverfügbar zu halten. Die aktuelle Update-Frequenz der Widerrufsliste ist im Internet über die Web-Seite von a.trust abrufbar.

2.2 Haftung

Die Allgemeinen Geschäftsbedingungen bilden zusammen mit der Zertifizierungsrichtlinie, der Certificate 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

- das Zertifikat bei Vorliegen der Voraussetzungen (siehe Kapitel 4.3.1) unverzüglich widerrufen wird und ein Widerrufsdienst verfügbar ist,
- sie die Anforderungen des Signaturgesetzes an Anbieter von Zertifizierungsdiensten erfüllt,
- sie die X.509-Standards einhält,
- sich an die Abläufe hält, die in der gegenständlichen Zertifizierungsrichtlinie beschrieben sind.

Kann ein Geschädigter nachweisen, dass a.trust Verpflichtungen oder gesetzliche Bestimmungen missachtet hat, so wird vermutet, dass der Schaden dadurch eingetreten ist. a.trust haftet nicht, wenn sie nachweist, dass sie und ihre Mitarbeiter an der Verletzung ihrer Verpflichtungen kein Verschulden trifft. a.trust haftet nicht für entgangenen Gewinn, Folgeschäden oder ideellen Schaden des Nutzers.

a.trust haftet für Zertifizierungsstellen (Inhaber der von von a.sign Company Root ausgestellten Zertifikate), die in ihrem Namen Zertifikate ausstellen.

2.2.2 Haftung der Registrierungsstelle

Die Zertifizierungsstelle haftet für die Registrierungsstelle.

2.3 Auslegung und (gerichtliche) Durchsetzung

2.3.1 Zugrunde liegende Gesetzesbestimmungen

Der zwischen a.trust und dem Zertifikatsinhaber geschlossene Vertrag unterliegt dem österreichischen Recht und richtet sich nach [SigG] und [SigV]. Im Verhältnis zu ausländischen Zertifikatsinhabern wird die Anwendung des UN-Kaufrechts ausdrücklich ausgeschlossen.

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

a.trust ist berechtigt, Rechte und Pflichten aus dem bestehenden Vertrag auf Dritte zu übertragen. Dem Zertifikatsinhaber entsteht dadurch kein besonderes Kündigungsrecht, solange der Dritte die Rechte und Pflichten des Vertrags wahrnimmt.

Änderungen der Allgemeinen Geschäftsbedingungen werden dem Zertifikatsinhaber vor der Zertifikatserneuerung schriftlich mitgeteilt. Ändert a.trust die Allgemeinen Geschäftsbedingungen, so hat der Zertifikatsinhaber die Möglichkeit zu kündigen. Widerspricht er den geänderten Allgemeinen Geschäftsbedingungen nicht binnen eines Monats, so gelten diese als akzeptiert.

2.4 Gebühren

Die aktuell gültigen Gebühren finden sich in der Entgeltregelung. Alle Entgelte, die nicht im Grundentgelt enthalten sind, werden mit der Nutzung der jeweiligen Leistung fällig.

2.4.1 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.

2.4.2 Abrufen von Zertifikaten

Der Abruf des a.sign Company Root Zertifikates und der von ihm ausgestellten Zertifikate über den Verzeichnisdienst ist kostenfrei.

2.4.3 Widerruf von Zertifikaten

Der Widerruf eines Zertifikats ist kostenfrei.

2.4.4 Abrufen von Statusinformationen

Der Zugang zu Widerrufslisten und Statusinformationen ist gebührenfrei.

2.4.5 Richtlinien für Gebührenrückerstattung

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

2.5 Bekanntmachung und Verzeichnisdienste

2.5.1 Web-Seiten und Verzeichnisse

a.trust stellt die folgende Web-Seite und Verzeichnisse bereit:

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

Tabelle 1 a.trust Homepage und Verzeichnisdienste

2.5.2 a.trust Stammzertifikat

Das a.trust Stammzertifikat ist unter

- http://www.a-trust.at/certs/A-Trust-Qual-nnx.crt
  (-nn ist 02 oder höher) oder unter
- http://www.a-trust.at/certs/A-Trust-nQual-01x.crt

zu finden.

Erläuterung: -nn ist die Versionsnummer der Root-CA: erhöht wird bei Generierung eines neuen Schlüssels und Veränderung des Distinguished Name;
-x bezeichnet die Version des Zertifikats: erhöht wird bei Ausstellung eines neuen Zertifikats mit unverändertem DN, unabhängig, ob ein neuer Schlüssel generiert wird, bei einer neuen CA-Version (nn + 1) wird immer mit –a begonnen;
Beispiel: A-Trust-Qual-02a.crt.

Das Stammzertifikat A-Trust-nQual-01 wird zur Validierung/CRL-Erstellung von früher (vor Inbetriebnahme von CA-Version 02) ausgestellten Zertifikaten verwendet.

Über den entsprechenden Menüpunkt auf der a.trust Homepage oder direkt unter dem oben angeführten Link kann der Download des Stammzertifikats erfolgen.

2.5.3 a.trust CA-Zertifikat

Das benötigte CA-Zertifikat ist unter

- http://www.a-trust.at/certs/a-sign-Company-Root-nnx.crt

zu finden (die Bedeutung von -nnx ist in Abschnitt 2.5.2 beschrieben).

Über die Homepage kann der Download der CA-Zertifikate erfolgen.

2.5.4 Widerrufsinformationen

Verteilungspunkt für die Zertifikatswiderrufsliste (CRL) der a.sign Company Root Zertifikate ab CA-Version 02:

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

Für Zertifikate, die unter der CA-Version 01 ausgestellt wurden, gilt folgender Verteilungspunkt:

- ldap://ldap.a-trust.at/ou=Company-Root-01,o=A-Trust,c=AT?certificaterevocationlist?

Darüberhinaus kann die aktuelle von a.trust ausgestellte CRL von der Homepage per Download bezogen werden.

2.5.5 Veröffentlichung von Informationen der Zertifizierungsstelle

a.trust veröffentlicht auf ihrer Homepage http://www.a-trust.at/:

- die jeweils gültige Zertifizierungsrichtlinie (CPS),
- die jeweils gültige Certificate Policy,
- die gültige Entgeltregelung,
- interne Auditinformationen, sofern die Sicherheit der Dienste nicht gefährdet ist,
- das Zertifikat der Zertifizierungsstelle,
- die Allgemeinen Geschäftsbedingungen und
- eine Liste mit Kontaktstellen bzw. Registrierungsstellen.

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

Die Zertifikatsinhaber werden zusätzlich informiert bei:

- 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),
- wesentlichen Änderungen der Zertifizierungsrichtlinie und
- Einstellung der Tätigkeit der Zertifizierungsstelle.

a.trust stellt alle Informationen wie folgt bereit:

- auf der Web-Seite
- optional: in einem elektronischen Newsletter per E-Mail
- optional: Briefsendung
- optional: Printmedien oder TV

Informationen, die nur einzelne Zertifikatsinhaber betreffen, werden diesen direkt zugestellt. Ist eine Vielzahl von Zertifikatsinhabern betroffen, wird eine der o. a. Alternativen ausgewählt.

2.5.6 Frequenz der Aktualisierung

Eine Aktualisierung der Zertifizierungsrichtlinie erfolgt gemäß Kapitel 8.

2.5.7 Zugriffskontrollen

Zugriffskontrollen stellen sicher, dass die Anwender nur lesenden Zugriff auf die Veröffentlichungen von 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.

2.5.8 Verzeichnisse

Folgende Verzeichnisse werden von a.trust unterhalten:

- Ein öffentlich zugängliches Verzeichnis, welches die Zertifikate der Zertifizierungsstellen und Widerrufslisten, sowie die Zertifikate der Zertifikatsinhaber enthält.
- Eine öffentliche Web-Seite, auf der diese Zertifizierungsrichtlinie abrufbar und den Anwendern weitere allgemeine Informationen zugänglich sind.

2.6 Interne Prüfung (Audit)

2.6.1 Häufigkeit des Audits

Jährlich werden interne Revisionen und Audits durchgeführt. Sie werden in Form von Stichproben in allen a.trust Liegenschaften und Registrierungsstellen durchgeführt.

2.6.2 Identität bzw. Anforderungen an den Auditor

Interne Audits werden im Rahmen der Revision durchgeführt.

2.6.3 Beziehungen zwischen Auditor und zu untersuchender Partei

a.trust bestimmt einen Auditor, der die Zertifizierungsdienste überprüft und darüber hinaus keine sicherheitskritische Funktion übernimmt. Die Registrierungsstelle und anderen Liegenschaften werden ebenfalls von dem durch a.trust bestellten Auditor oder durch die eigene interne Revision überprüft.

2.6.4 Aspekte des Audits

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

2.6.5 Handlungen nach unzureichendem Ergebnis

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

- Widerruf des entsprechenden Zertifikats bzw. Einstellung des Betriebs der überprüften Einheit der Zertifizierungsinfrastruktur,

- der überprüften Einheit der Zertifizierungsinfrastruktur wird eine Frist zur Beseitigung der Schwachstellen eingeräumt.

2.6.6 Bekanntgabe der Ergebnisse

a.trust veröffentlicht die Informationen aus dem Audit, sofern dadurch nicht die Sicherheit gefährdet wird.

2.7 Vertraulichkeit

2.7.1 Vertraulich eingestufte Informationen

a.trust verpflichtet sich, die vom Zertifikatsinhaber 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.

2.7.2 Nicht vertraulich eingestufte Informationen

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

2.7.3 Offenlegung von Informationen zu Zertifikatswiderruf

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

2.7.4 Offenbarung an Behörden im Rahmen gesetzlicher Pflichten

a.trust gibt Daten des Zertifikatsinhabers nur mit dessen ausdrücklichem Einverständnis oder auf Verlangen an gesetzlich berechtigte Behörden weiter.

2.7.5 Offenbarung im Rahmen zivilrechtlicher Auskunftspflichten

Wird wie in Abschnitt 2.7.4 behandelt.

2.7.6 Weitere Gründe zur Freigabe von vertraulichen Informationen

Wird wie in Abschnitt 2.7.4 behandelt.

2.8 Urheberrechte und Eigentumsrechte

Die Urheber- und Eigentumsrechte an den folgenden Dokumenten liegen bei a.trust:

- Zertifizierungsrichtlinie,
- Certificate Policy,
- AGB und
- Entgeltbestimmungen.

Die Urheber- und Eigentumsrechte an den folgenden Schlüsseln und Zertifikaten liegen bei a.trust:

- Private Schlüssel des Zertifizierungsdiensteanbieters,
- Öffentliche Schlüssel des Zertifizierungsdiensteanbieters und
- Zertifikat der Zertifizierungsstelle.

Die Urheber- und Eigentumsrechte der folgenden Schlüssel liegen beim Zertifikatsinhaber:

- Privater Schlüssel des Zertifikatsinhabers sowie
- Öffentlicher Schlüssel des Zertifikatsinhabers.

3 Identifizierung und Authentisierung

3.1 Erstregistrierung

3.1.1 Namenstypen

Die benötigten Angaben eines Antragstellers sind die folgenden:

- Name für das Zertifikat (Common Name):
  wird vom Antragsteller gewählt
- Organisationsname (OrganizationName):
  der Name der Organisation (vollständiger Name z. B. lt. Firmenbucheintrag oder vom Antragsteller gewählte Abkürzung) ist erforderlich.
- Organisationsuntereinheit (OrganizationalUnit):
  optional, wird vom Antragsteller bei Bedarf gewählt.
- Land (Country):
  Das Land des Sitzes der Organisation wird ebenfalls in den eindeutigen Namen des Antragstellers aufgenommen.

3.1.2 Eindeutigkeit der Namen

Der Name des Zertifikatsinhabers (Attribut subject des Zertifikats) ist durch die Kombination der in Abschnitt 3.1.1 genannten Attribute eindeutig gestaltet.

3.1.3 Methode zum Beweis des Besitzes des geheimen Schlüssels

Das beantragende Unternehmen generiert das Schlüsselpaar mit einem zertifizierten Hardware Security Modul in einem Arbeitsschritt zusammen mit der Erstellung des Zertifikatsrequests, welcher im Anschluss an a.trust übermittelt wird. Somit ist gesichert, dass der zum zertifizierten öffentlichen Schlüssel gehörige private Schlüssel sich im Besitz des Antragstellers befindet.

3.1.4 Authentisierung von Organisationen

Für die Bestellung eines von a.sign Company Root ausgestellten Zertifikats muss die bestellende Organisation überprüft werden. Wenn sie eine ins österreichische Firmenbuch bzw. ins European Business Register (EBR) eingetragene Firma ist, so erfolgt die Überprüfung durch die Registrierungsstelle mittels Online-Abfrage des Firmenbuchs bzw. des EBR. Die Firmenbuch- bzw. EBR-Nummer muss in diesem Fall bei der Antragstellung angegeben werden. Es kann auch vom Unternehmen ein Firmenbuchauszug an die Registrierungsstelle übermittelt werden.

Wenn die Antrag stellende Organisation kein registriertes Unternehmen ist, dann erfolgt die Überprüfung mittels Vorlage einer Kopie eines Dokumentes, aus welchem hervorgeht, dass die Organisation tatsächlich existiert. Das kann ein aktueller (nicht älter als drei Monate) Auszug aus einem zuständigen amtlichen Register bzw. vergleichbare Dokumente sein. Darüber hinaus kann die Überprüfung auch anhand von Datenbanken vertrauenswürdiger Dritter erfolgen.

3.1.5 Authentisierung von Individuen

Die Personen, die bei der Beantragung eines von a.sign Company Root ausgestellten Zertifikats überprüft werden, sind ein technischer Verantwortlicher und eine zeichnungsberechtigte Person (rechtlich-organisatorisch Verantwortlicher). Von beiden muss eine Ausweiskopie eines gültigen, amtlichen Lichtbildausweises an a.trust übermittelt werden. Dabei sind Personalausweis, Reisepass, Identitätskarte oder Führerschein zulässig. Für Ausländer werden nur gültige Reisepässe in deutscher oder englischer Sprache oder beglaubigte Abschriften zugelassen.

Wenn die zeichnungsberechtigte Person nicht im Firmenbuch oder EBR genannt ist oder kein Eintrag in ein solches Register existiert, dann muss die Organisation zusätzlich einen Nachweis über die Zeichnungsberechtigung an a.trust übermitteln.

3.2 Erneute Registrierung/Rezertifizierung

Mit der Bestellung eines von a.sign Company Root ausgestellten Zertifikats wird ein unbefristeter Vertrag mit a.trust abgeschlossen. Daher wird automatisch vor Ablauf der Gültigkeitsdauer der Zertifikatsinhaber benachrichtigt und gebeten, einen neuen Zertifikatsantrag an die Registrierungsstelle zu senden. Ob ein neuer Schlüssel generiert wird, bleibt dem Signator selbst überlassen, allerdings empfiehlt a.trust den Zertifikatsinhabern, die Möglichkeit des Schlüsselwechsels zu nützen.

Die Existenz der Organisation wird von der Registrierungsstelle anlässlich der Verlängerung erneut überprüft.

3.3 Erneute Registrierung nach Widerruf

Nach dem Widerruf eines Zertifikates kann der Zertifikatsinhaber ein neues Zertifikat beantragen. Der Vorgang entspricht dem Ablauf der Registrierung.

3.4 Widerrufsantrag

Widerrufe werden entsprechend Abschnitt 4.3 gehandhabt.

Der Widerruf erfolgt durch einen Telefonanruf beim zuständigen Widerrufsdienst. Beim Widerruf muss das bei der Antragstellung selbst gewählte Passwort für den Widerruf angegeben werden.

Wenn das Passwort vergessen wurde, kann der Widerruf mit einem firmenmäßig gezeichneten Einschreiben beantragt werden.

4 Betriebliche Anforderungen

4.1 Antrag auf Ausstellung von Zertifikaten

Der Antrag auf Ausstellung eines Zertifikats erfolgt durch Kontaktaufnahme mit der zuständigen Registrierungsstelle (Informationen dazu befinden sich auf der a.trust Homepage). Die Ausweiskopien, den Zertifizierungsreport oder die Bestätigung/Bescheinigung kann der Antragsteller per Fax an die Registrierungsstelle senden.

4.2 Herausgabe und Akzeptanz von Zertifikaten

Das von a.sign Company Root fertig ausgestellte Zertifikat wird dem Zertifikats-inhaber auf elektronischem Weg zur Verfügung gestellt.

4.3 Widerruf

Auf Antrag des Zertifikatsinhabers ist ein rascher und permanenter Widerruf möglich.

4.3.1 Gründe für einen Widerruf

Der Widerruf eines von a.sign Company Root ausgestellten Zertifikates wird erforderlich, wenn

- sich Angaben im Zertifikat geändert haben,
- der private Schlüssel nicht mehr verwendet werden kann (z. B. durch einen Defekt/Ausfall des Hardware Security Moduls),
- Verdacht auf eine Kompromittierung besteht (wenn z. B. ein Unbefugter Zugriff auf den HSM, in dem sich der private Schlüssel befindet, hatte) bzw. eine Kompromittierung vorliegt,
- a.trust davon Kenntnis erhält, dass der Inhaber des Zertifikates den privaten Schlüssel in einer anderen als der a.trust bekannt gegebenen bzw. nachgewiesenen Hardware-Einheit erzeugt oder aufbewahrt,

- der Zertifizierungsstelle ein wesentlicher Verstoß des Zertifikatsinhabers gegen diese Richtlinien oder die Allgemeinen Geschäftsbedingungen bekannt wird,
- das Vertragsverhältnis beendet wird,
- die eingesetzten Algorithmen nicht mehr den Sicherheitserwartungen entsprechen.

4.3.2 Wer kann einen Widerruf anordnen

Ein Widerruf kann angeordnet werden durch:

- eine Person, der das Passwort für den Widerruf bekannt ist (Zertifikatsinhaber) oder
- die Zertifizierungsstelle der a.trust.

4.3.3 Prozedur für einen Widerrufsantrag

Ein Widerruf kann durch den Inhaber des von a.sign Company Root ausgestellten Zertifikates per Telefon vorgenommen werden. Die aktuellen Telefonnummern des Widerrufsdienstes sind der Homepage zu entnehmen.

Dabei ergeben sich einige Anforderungen an den Ablauf. Diese werden nachfolgend angeführt:

- Für den Widerruf eines Zertifikats ist die Angabe des Passworts für den Widerruf verpflichtend.
- Der Grund für den Widerruf (Kompromittierung des privaten Schlüssels, Auflösung des Vertrages etc.) muss dem Mitarbeiter des Widerrufsdienstes mitgeteilt werden.

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

- Passwort für den Widerruf: obligatorisch
- Zertifikatsdaten (Name, Organisationsname, etc.)
  obligatorisch

Wenn beim Widerruf das Passwort nicht genannt werden kann, so kann der Widerruf per Einschreiben mit firmenmäßiger Zeichnung erfolgen.

4.3.4 Frist bis zur Bekanntgabe des Widerrufs

Die Aktualisierung der Widerrufsdienste muss lt. Österr. Signaturgesetz spätestens innerhalb von drei Stunden ab Kenntnis des Widerrufsgrundes erfolgen.

Die Informationen über die Erreichbarkeit des Widerrufsdienstes sind der a.trust Homepage zu entnehmen.

4.3.5 Aktualisierungsfrequenz der Widerrufsliste

Die aktuelle Update-Frequenz der Widerrufsliste ist im Internet über die Web-Seite von a.trust abrufbar.

4.3.6 Anforderungen an die Überprüfung durch Widerrufslisten

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

Für eine positive Gültigkeitsüberprüfung ist erforderlich, dass

- das Zertifikat mit dem auf einem gültigen Zertifikat der Zertifizierungsstelle beruhenden Schlüssel signiert wurde und
- sich das Zertifikat nicht in der aktuellen Widerrufsliste befindet.

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

Die von dem Nutzer lokal gespeicherten Zertifikate sollten vor ihrer Verwendung gegen eine aktuelle Widerrufsliste geprüft werden. Sofern keine erfolgreiche Gültigkeitsprüfung vorgenommen werden kann (beispielsweise aus technischen Gründen), sollten keine Zertifikate akzeptiert werden. Das Risiko für die Akzeptanz eines solchen Zertifikats trägt jedenfalls der Zertifikatsnutzer.

4.3.7 Möglichkeiten zur online Statusabfrage

Es wird ein OCSP-Dienst über das Internet angeboten.

4.3.8 Anforderungen an die Statusabfrage

Ein Zertifikatsnutzer sollte die Authentizität der Auskunft des Verzeichnisdiensts durch die Prüfung der in der Antwort enthaltenen Signatur verifizieren. Desweiteren 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. Das Risiko für die Akzeptanz eines solchen Zertifikats trägt jedenfalls der Zertifikatsnutzer.

4.3.9 Spezielle Verfahren bei Kompromittierung

Wenn der Verdacht auf Kompromittierung eines privaten Schlüssels besteht, muss der Zertifikatsinhaber einen Widerruf beantragen.

4.4 Protokollierung sicherheitsrelevanter Ereignisse

4.4.1 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 Berechtigungen,
- Änderungen bei der Rollenaufteilung (siehe Abschnitt 5.2),
- 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,
- Widerrufsanträge,
- Ausgeführte Widerrufe sowie
- Schlüsselwechsel.

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

- Akzeptanzerklärung der Allgemeinen Geschäftsbedingungen und der Entgeltbestimmungen durch den Zertifikatswerber oder auch
- Änderungen an den Daten des Zertifikatsinhabers.

4.4.2 Frequenz der Überprüfung der Protokolldateien

Die Protokolle werden an jedem Arbeitstag einmal auf verdächtige Vorkommnisse untersucht.

4.4.3 Aufbewahrungszeitraum der Protokolldateien

Sicherheitsrelevante Protokolldateien werden über die gesetzliche Frist hinaus aufbewahrt. Protokolldateien, die benötigt werden, um nachträglich Aussagen über die Gültigkeit von Zertifikaten zu treffen, werden archiviert. Dies gilt besonders für Daten zur Veröffentlichung von Zertifikaten und Widerrufslisten sowie Eingang und Bearbeitung von Widerrufsanträgen. Der Zeitraum der Aufbewahrung von archivierten Protokolldateien ist in Abschnitt 4.5.2 festgelegt.

4.4.4 Schutz der Protokolldateien

Die Protokolldateien werden an unterschiedlichen Standorten erstellt und aufbewahrt. Sie sind nur autorisiertem Personal zugänglich zu machen.

Die Protokolldateien werden mittels digitaler Signatur vor Modifikationen geschützt.

4.4.5 Protokollierungssystem (intern/extern)

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

4.4.6 Benachrichtigung beim Auftreten sicherheitskritischer Ereignisse

Bei einem Verdacht auf das Eintreten eines sicherheitskritischen Ereignisses entscheidet a.trust über eine Benachrichtigung von betroffenen Anwendern.

4.5 Archivierung

4.5.1 Archivierte Daten

Archiviert werden:

- Daten des Zertifikatsinhabers, die zur Zertifizierung verwendet wurden,
- Zertifizierungsanträge,
- alle von der Zertifizierungsstelle ausgestellten Zertifikate (Zertifikate der Zertifizierungsstelle und Zertifikate der Zertifikatsinhaber),
- Widerrufanträge mit Datum und Uhrzeit des Eintreffens (inklusive entsprechender Protokolldateien),
- alle ausgestellten Widerrufslisten,
- Datum und Uhrzeit der Veröffentlichung der Zertifikate und Widerrufslisten (inklusive entsprechender Protokolldateien) und
- Datum und Uhrzeit von Schlüsselwechseln der Zertifizierungsstelle.

4.5.2 Aufbewahrungszeiten

Die Aufbewahrungszeit beträgt mindestens sieben Jahre. Es 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 müssen.
- Zu berücksichtigen ist auch die technische Kompatibilität. Dies gilt insbesondere für Soft- und Hardware, deren Veränderung eine Nachprüfung von Dokumenten nicht mehr möglich macht.

4.5.3 Schutzvorkehrungen

Das Archiv befindet sich in gesicherten Räumlichkeiten. Der Zugriff ist nur autorisierten Personen gestattet.

Elektronische Dokumente sind durch digitale Signaturen der archivierenden Einheit vor Modifikationen geschützt.

Die Zugangs- und Zugriffskontrolle räumt nur zwei autorisierten Personen aus dem Zuständigkeitsbereich gleichzeitig den Zutritt und das Recht für Änderungen im Archiv ein.

4.5.4 Anforderungen, die Daten mit Zeitstempeln zu versehen

Alle Zertifikatsanträge, Widerrufsanträge und Änderungen an den Widerrufslisten sind mit einem Zeitstempel zu versehen.

4.5.5 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.

4.5.6 Prozeduren zum Abrufen und Überprüfen von Daten

Anwender sollten die Möglichkeit haben, archivierte Informationen, die sie direkt betreffen, oder die sie zur Überprüfung von Signaturen benötigen, abzurufen. Dies ist mit einem entsprechenden Aufwand seitens der Zertifizierungsstelle verbunden und geschieht unter bestimmten, hier anzugebenden, Voraussetzungen.

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.

4.6 Schlüsselwechsel von CA-Schlüsseln

Ein Schlüsselwechsel von CA- und Root-Schlüsseln erfolgt im Zusammenhang mit dem Ausfall eines Hardware Security Moduls, wenn die verwendeten Schlüssellängen bzw. Algorithmen nicht mehr den Sicherheitserwartungen entsprechen sollten oder aber im Falle einer Kompromittierung von Schlüsseln. In letzterem Fall ist unbedingt ein Widerruf der betroffenen Zertifikate erforderlich.

Die Zertifizierungsstellen erneuern außerdem regelmäßig ihre Zertifikate. Dies sollte vor dem Ablauf der im Zertifikat festgelegten Gültigkeitsdauer geschehen. Die Gültigkeitsdauer der Zertifikate ist dem Abschnitt 6.3.2 zu entnehmen. Der Überprüfer eines Zertifikats erhält das neue Zertifikat über den Verzeichnisdienst. Er kann über die Auflösung der Zertifikatskette die Gültigkeit des Zertifikats überprüfen.

Mit einem Schlüsselwechsel verliert der alte Schlüssel seine aktive Gültigkeit. D. h. der private Schlüssel wird nicht weiter für die Zertifizierung eingesetzt. Ab diesem Zeitpunkt wird nur noch der neue Schlüssel für das Signieren von Zertifikaten verwendet. Das Zertifikat zu dem alten Schlüssel wird nur, falls erforderlich, widerrufen

(Kompromittierung). Wurde der alte Schlüssel nicht widerrufen, kann er bis zum Ablauf der im Zertifikat festgelegten Gültigkeitsdauer zum Nachprüfen von Zertifikaten eingesetzt werden.

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

4.7 Kompromittierung und Notfallplan

4.7.1 Rechner, Software und/oder Daten sind korrumpiert

Werden innerhalb des Systems fehlerhafte oder manipulierte Rechner, Software oder Daten entdeckt, die Auswirkungen auf die Sicherheit des Systems und dessen Dienste haben könnten, so werden die entsprechenden Komponenten umgehend aus dem Betrieb genommen.

Bei Zertifikaten sind die betroffenen Zertifikatsinhaber zu informieren. Es erfolgt ein unmittelbarer Widerruf der betroffenen Zertifikate, falls sich im Zertifikat fehlerhafte Angaben befinden.

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 nicht weiterhin unkorrekte Daten zu publizieren. 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.

4.7.2 Widerruf von Zertifikaten zu Zertifizierungsstellen- und Dienste-Schlüsseln

Zertifikate der Zertifizierungsstelle werden widerrufen:

- bei Kompromittierung oder Verdacht auf Kompromittierung der entsprechenden Schlüssel,
- wenn die eingesetzten Algorithmen nicht mehr den Sicherheitserwartungen entsprechen und dadurch eine sichere Anwendung nicht mehr gegeben wäre,
- 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 4.7.3 zu berücksichtigen. Bei Widerruf des Zertifikats wegen Einstellung der Tätigkeit der Zertifizierungsstelle ist Abschnitt 4.8 zu beachten.

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

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

4.7.2.1 Widerruf des Zertifikats der Zertifizierungsstelle

Wird ein Zertifikat der Zertifizierungsstelle widerrufen, so müssen dadurch alle unter diesem Zertifikat ausgestellten Zertifikate ebenfalls 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.

Zertifikatsinhaber, deren Zertifikate von dem Widerruf betroffen sind, erhalten neue Zertifikate. Die Zertifizierung erfolgt dabei mit einem neuen Schlüssel der Zertifizierungsstelle.

4.7.2.2 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 4.6 durchgeführt, die sich aber in folgenden Punkten von dem regulären Wechsel unterscheiden:

- Eine rechtzeitige Information der Zertifikatsinhaber über den Schlüsselwechsel ist bei einem unmittelbaren Widerruf nicht möglich. Die Zertifikatsinhaber werden im Zusammenhang mit der Widerrufsinformation auch über den Schlüsselwechsel informiert.

- Die Schlüssel zu widerrufenen Zertifikaten sind ungültig und werden nicht weiter eingesetzt.

4.7.2.3 Widerruf von Crosszertifikaten

Wird ein Zertifikat der Zertifizierungsstelle widerrufen, so werden ggf. auch alle dazu ausgestellten 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.

4.7.3 Schlüsselkompromittierung bzw. Verdacht auf Schlüsselkompromittierung

Wird in der Zertifizierungsstelle eine Kompromittierung von CA-Schlüsseln 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 erfolgen das Abschalten des Verzeichnisdienstes und die Einstellung der Statusauskünfte, um falsche oder ungültige Aussagen durch diese Dienste zu verhindern.

- Verteilung neuer, gültiger Zertifikate an die Anwender.

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

4.7.4 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 Ver-

fahren, wie Widerruf oder das Anbieten von Informationen über E-Mail oder Web-Seite nicht möglich sind, dann werden verstärkt alternative Verfahren wie der Postweg zur Verbreitung der notwendigen Informationen eingesetzt.

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

4.8 Einstellung der Tätigkeit der Zertifizierungsstelle

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

Die Einstellung der Tätigkeit wird mindestens drei Monate zuvor allen betroffenen Einheiten und Personenkreisen mitgeteilt. Dies gilt insbesondere für die Benachrichtigung der Aufsichtsstelle und die Inhaber von gültigen Zertifikaten.

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.

5 Physische, verfahrensorientierte und personelle Sicherheitsvorkehrungen

5.1 Physische Sicherheitsvorkehrungen

5.1.1 Standort und örtliche Gegebenheiten

Die Dienstleistungen, die von a.trust oder in ihrem Namen durchgeführt werden, finden an den folgenden Örtlichkeiten statt:

Dienstleistung	Adresse
Firmensitz	A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH. Landstraßer Hauptstraße 5 A-1030 Wien
Registrierung Widerrufsdienst	Die Registrierungsstellen und den Widerrufsdienst finden Sie auf der Web-Seite der a.trust http://www.a-trust.at/ veröffentlicht.

Tabelle 2 Standorte

5.1.2 Zugangskontrollen

Der Zugang zu allen technischen Komponenten im Rechenzentrum ist nur durch einen vom Betreiber 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 a.trust 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 der a.trust die Notstromversorgung durch ein Dieselaggregat.

Die Örtlichkeiten, in denen technische Komponenten der a.trust oder eines anderen Betreibers im Namen der a.trust untergebracht sind, verfügen alle über eine angemessene Klimaanlage.

5.1.4 Wasserschäden

Die Örtlichkeiten, in denen technische Komponenten der a.trust oder eines anderen Betreibers im Namen 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 a.trust 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
- Magnetbänder
- Festplatten
- DVDs
- WORMs

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

5.1.7 Müllentsorgung

Die Daten auf den elektronischen Datenträgern werden sachgemäß vernichtet und die Datenträger dann 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 a.trust Rechenzentrum ist redundant ausgelegt, so dass eine Hochverfügbarkeit (7 x 24 Stunden) des Rechenzentrumsbetriebs erreicht werden kann.

5.2 Verfahrensorientierte Sicherheitsvorkehrungen

In diesem Kapitel werden die bei a.trust und den Liegenschaften, in denen Zertifizierungsdienste für a.trust erbracht werden, notwendigen Rollen definiert. Die Aufgaben der Rollen werden kurz beschrieben, die Rollen werden nach ihrer sicherheitstechnischen Relevanz eingeordnet.

5.2.1 Funktionen der a.trust

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

Tabelle 3 Funktionen der a.trust

5.2.2 Sicherheitskritische Funktionen

Rolle	Funktion
Sicherheitsbeauftragter	siehe Tabelle 3
Revision	siehe Tabelle 3
Datenschutz	siehe Tabelle 3

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

Tabelle 4 Sicherheitskritische Funktionen

5.2.3 Sonstige (nicht sicherheitskritische) Funktionen

Rolle	Funktion
Systemadministrator	Administration, Installation, Konfiguration und Wartung der Systeme Wird in sicherheitskritischen Bereichen vom Sicherheitssystemadministrator beaufsichtigt.
Systemoperator	Laufende Systembetreuung, Datensicherung und –wiederherstellung für die täglichen Abläufe
Schulung	siehe Tabelle 3

Tabelle 5 Sonstige Funktionen

5.2.4 Anzahl erforderlicher Personen für sicherheitsrelevante Tätigkeiten

Die folgende Tabelle stellt sicherheitsrelevante Tätigkeiten dar und ordnet diesen die dafür zuständigen Rollen zu. Weiters wird aufgezeigt, ob für diese Tätigkeit das Vieraugenprinzip notwendig ist und ob diese Tätigkeit im Hochsicherheitsbereich des a.trust Rechenzentrums ausgeübt wird.

Tätigkeit	Personen	Vier-augen-prinzip	Hoch-sicher-heit
Registrierung und Identifizierung von Zertifikatswerbern	RO	Nein	Nein
Widerrufen von Anwenderzertifikaten	RCA	Nein	Nein
Erzeugung der Schlüssel für Root-CA und Zertifizierungsstellen sowie Schlüsselwechsel	SO, SO	Ja	Ja
Aktivierung der Schlüssel für Root-CA und Zertifizierungsstellen	SO, SO	Ja	Ja
Zertifizierung für die Root-CA und die Zertifizierungsstellen	SO, SO	Ja	Ja
Widerruf von Zertifikaten der CA	SO, SO	Ja	Ja
Vergabe der Berechtigungen für RO und RCA	SO	Nein	Nein
Inbetriebnahme eines kryptografischen Moduls (Signaturerstellungseinheit der CA)	SO, SO	Ja	Ja
Ab- und Anschalten von Komponenten, insbesondere Verzeichnisdiensten	Sicherheitssystemad-ministrator, Sicher-heitssystemad-ministrator	Ja	Ja
Austausch von Hardware-Komponen-ten	Sicherheitssystemad-ministrator, Sicher-heitssystemad-ministrator	Ja	Ja
Austausch von Software-Komponenten	Sicherheitssystemad-ministrator, Sicher-heitssystemad-ministrator	Ja	Ja

Tätigkeit	Personen	Vier-augen-prinzip	Hoch-sicher-heit
Überprüfung von Protokolldateien auf verdächtige Vorkommnisse	Systemadministrator	Nein	Nein
Überprüfung der Protokolldateien auf Manipulation	Systemadministrator	Nein	Nein
Anfertigung eines Backups der Protokolldateien und Lagerung desselben	Sicherheitssystemadministrator, Sicherheitssystemadministrator	Ja	Ja
Qualitätsprüfung der verwendeten Schlüssellängen und Parameter zur Schlüsselerzeugung	SO	Nein	Nein
Wartung oder Austausch eines kryptographischen Moduls	SO, SO	Ja	Ja

Tabelle 6 Anzahl erforderlicher Personen

5.2.5 Identifikation und Authentisierung 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

Das Personal, das von a.trust beschäftigt wird, erfüllt alle notwendigen Anforderungen hinsichtlich Vertrauenswürdigkeit, Integrität, Zuverlässigkeit und Fachkunde und verfügt über ausreichendes Fachwissen in den Bereichen:

- allgemeine EDV-Ausbildung,
- Sicherheitstechnologie, Kryptographie, elektronische Signatur und Public Key Infrastructure,

- technische Normen, insbesondere Evaluierungsnormen, sowie
- Hard- und Software.

5.3.2 Überprüfung des Personals

Die im Rahmen der Signatur- und Zertifizierungsdienste beschäftigten Personen werden mittels eines Strafregisterauszuges in Abständen von zumindest zwei Jahren auf ihre Zuverlässigkeit überprüft.

5.3.3 Anforderungen an die Schulung

Es finden regelmäßige Schulungen durch kompetentes Personal für die 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 Sicherheitssysteme statt.

5.3.5 Sanktionen für unautorisierte Handlungen

Schwerwiegende Verstöße gegen Sicherheitsvorkehrungen werden disziplinarisch geahndet.

5.3.6 Anforderungen an Vertragsvereinbarungen mit dem Personal

Das Personal ist gemäß Datenschutzgesetz zur Geheimhaltung verpflichtet.

5.3.7 An das Personal auszuhändigende Dokumente

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

- Betriebskonzept,
- Zertifizierungsrichtlinie und
- Schulungsunterlagen.

6 Technische Sicherheitsvorkehrungen

6.1 Schlüsselgenerierung und Installation

6.1.1 Schlüsselgenerierung

6.1.1.1 Schlüssel der Zertifizierungsstelle

Die Schlüssel der a.trust CA werden in einem Hardware Security Modul der Zertifizierungsstelle generiert. Für die geheimen Schlüssel der Zertifizierungsstelle gibt es keine Exportmöglichkeit und auch keine Backups.

Die Erzeugung der Schlüssel in der Zertifizierungsstelle erfolgt immer unter der Aufsicht von zwei befugten a.trust Mitarbeitern und muss von der Geschäftsführung der a.trust angeordnet werden.

6.1.1.2 Schlüssel der Zertifikatsinhaber

Die Schlüssel der von a.sign Company Root ausgestellten Zertifikate werden in einem Hardware Security Modul des Zertifikatsinhabers generiert. Die geheimen Schlüssel dürfen das Hardware Security Modul nicht im Klartext verlassen.

Auch diese Schlüssel müssen im Vieraugenprinzip von zwei befugten Mitarbeitern generiert werden.

a.trust erhält keine Kenntnis dieser privaten Schlüssel. Die Zertifikate werden von der Zertifizierungsstelle der a.trust aufgrund des vom Antragsteller erzeugten PKCS#10-Requests erzeugt.

6.1.2 Auslieferung privater Schlüssel an Zertifikatsinhaber

Eine Auslieferung privater Schlüssel wird nicht durchgeführt, da nur der Zertifikatsinhaber über den privaten Schlüssel verfügt und a.trust keinen Zugriff auf die privaten Schlüssel erhält.

6.1.3 Auslieferung öffentlicher Schlüssel an die Zertifikatsinhaber

6.1.3.1 Öffentliche Schlüssel der Zertifizierungsstelle

Die Zertifikate des Schlüssels der Root-CA sowie der Zertifizierungsstellen werden in einem Verzeichnis im Internet veröffentlicht, sodass sie allgemein zugänglich sind und alle Zertifikatsnutzer Zertifikate dagegen prüfen können.

6.1.3.2 Öffentlicher Schlüssel des Zertifikatsinhabers

Der Zertifikatsinhaber generiert sein Schlüsselpaar selbst in einem HSM und ist daher im Besitz des öffentlichen Schlüssels, das Zertifikat wird im Verzeichnisdienst veröffentlicht.

Zusätzlich zum PKCS#10-Request teilt der technische Verantwortliche dem Mitarbeiter der Registrierungsstelle per Telefon den Hash (SHA1) des öffentlichen Schlüssels mit.

6.1.4 Schlüssellängen

Die Schlüssel der Root-CA und aller Zertifizierungsstellen der a.trust entsprechen einer Länge von zurzeit 2048 Bit (RSA-Schlüssel).

Die Zertifikatswerber müssen als Schlüssellänge mindestens 1024 Bit (RSA-Schlüssel) wählen.

Der von a.trust zur Erstellung der Signatur über Zertifikate verwendete Hash-Algorithmus ist SHA-1. Den Zertifikatsinhabern wird zur Erstellung der Signatur über die Signatorenzertifikate ebenfalls die Verwendung von SHA-1 empfohlen

Die genannten Mindestlängen können sich aufgrund von Algorithmenschwächen oder Anpassung an geänderte gesetzliche Vorgaben ändern.

6.1.5 Parameter zur Schlüsselerzeugung

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

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

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

und

$$0{,}5 < \left|\log_2(p) - \log_2(q)\right| < 30$$

gilt.

Der öffentliche Exponent *e* entspricht der 4. Fermatzahl.

6.1.6 Qualitätsprüfung der Parameter

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

6.1.7 Hardware/Software Schlüsselerzeugung

Die Schlüssel der a.trust Root-CA und der a.sign Company Root-CA a. werden in einem von einer Bestätigungsstelle bestätigten Hardware Security Modul erzeugt und dort auch eingesetzt.

Die Schlüssel der Zertifikatsinhaber werden in einem zertifizierten oder bestätigten/bescheinigten Hardware Security Modul erzeugt. a.trust erhält keine Kenntnis vom privaten Schlüssel des Zertifikatsinhabers.

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

Der Verwendungszweck für den zertifizierten Schlüssel wird in den X.509 v3 Zertifikaten in der Extension „keyUsage“ angegeben (siehe Kapitel 6.1.8.2 und 6.1.8.3).

6.1.8.1 Verwendung der Schlüssel der Root-CA

Die Root-CA besitzt ein selbstsigniertes Zertifikat, welches das Attribut „keyUsage“ nicht enthält.

6.1.8.2 Verwendung der Schlüssel der Zertifizierungsstellen

Die Schlüssel der a.sign company Root Zertifizierungsstelle der a.trust werden ausschließlich zum Signieren von Zertifikaten und Widerrufslisten eingesetzt.

Deshalb werden die Bits

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

gesetzt.

6.1.8.3 Verwendung des Schlüssels des Zertifikatsinhabers

Der Schlüssel des Inhabers eines von a.sign Company Root ausgestellten Zertifikats wird ausschließlich zum Signieren von Zertifikaten und Widerrufslisten für Signatoren benutzt.

Deshalb werden die Bits

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

gesetzt.

6.2 Schutz der privaten Schlüssel

6.2.1 Schutz des Schlüssels der Zertifizierungsstelle

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

Die Schlüssel der a.sign Company Root Zertifizierungsstelle dienen zur Signatur von Zertifikaten und Widerrufslisten. Sie werden nur in einer sicheren Umgebung verwendet.

Für die Speicherung und Anwendung des privaten Schlüssels der Root-CA und der Zertifizierungsstelle für a.sign Company Root Zertifikate werden nur Hardware Security Module eingesetzt, die einen angemessenen physikalischen Zugriffsschutz auf diese Schlüssel bieten. Für die Speicherung und Anwendung der privaten Schlüssel wird der angemessene Zugriffsschutz mittels PIN gewährleistet.

6.2.2 Schutz der Schlüssel der Zertifikatsinhaber

Die Schlüssel der Zertifikatsinhaber befinden sich in einem zertifizierten oder bestätigten/bescheinigten Hardware Security Modul und werden gegen unberechtigte Nutzung mittels einer PIN abgesichert.

6.2.3 Aktivierung privater Schlüssel durch mehrere Personen

Für die Aktivierung des Schlüssels der a.trust Root-CA, der a.trust Zertifizierungsstelle a.sign Company Root oder des Zertifikatsinhabers ist Vieraugenprinzip erforderlich. Eine einzelne Person darf nicht über die Mittel verfügen, einen dieser privaten Schlüssel zu nutzen.

6.2.4 Hinterlegung privater Schlüssel

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

6.2.5 Backup privater Schlüssel

Für private Schlüssel der Root-CA und der a.sign Company Root Zertifizierungsstelle sowie des Zertifikatsinhabers gibt es kein Backup.

6.2.6 Archivierung privater Schlüssel

Private Schlüssel zur Signatur von Zertifikaten und CRLs werden nicht archiviert.

6.2.7 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. Die Anwendung erfolgt ebenfalls direkt im Hardware Security Modul. Die Nutzung bzw. Aktivierung dieser privaten Schlüssel ist durch eine Benutzerauthentikation gesichert.

6.2.8 Methode zur Deaktivierung privater Schlüssel

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

6.3 Weitere Aspekte zum Schlüsselmanagement

6.3.1 Archivierung öffentlicher Schlüssel

Siehe Abschnitt 4.6.

6.3.2 Verwendungszeitraum öffentlicher und privater Schlüssel

Als Gültigkeitsmodell wird das Kettenmodell eingesetzt. Zur Überprüfung der Gültigkeit eines Zertifikats wird die übergeordnete Instanz herangezogen. Dabei muss das übergeordnete Zertifikat nur zum Zeitpunkt der Ausstellung des zu überprüfenden Zertifikats gültig gewesen sein. Solange ein Zertifizierungsschüssel noch als sicher gilt, kann eine Rezertifizierung (Verlängerung/Zertifikatserneuerung) vorgenommen werden.

Für die Zertifikate gelten die folgenden (maximalen) Gültigkeitsdauern (in Jahren). Kürzere Gültigkeitsperioden können gewählt werden, wenn die Sicherheit der Algorithmen nicht für die gesamte Dauer gewährleistet ist:

Zertifikatstyp	Gültigkeitsdauer
a.trust Root-CA	10

Zertifikatstyp	Gültigkeitsdauer
a.signt Company Root CA	10
Zertifikatsinhaber	10

Tabelle 7 Gültigkeitsdauer von Zertifikaten

6.4 Aktivierungsdaten

6.4.1 Erzeugung und Installation der Aktivierungsdaten (PINs) für Zertifizierungsschlüssel

Die Schlüssel der Root-CA und der a.sign Company Root Zertifizierungsstelle können ausschließlich im Vieraugenprinzip durch zwei Beauftragte mit Chipkarte und PIN aktiviert werden. Die Aktivierungsdaten werden direkt im Hardware Security Modul erzeugt. Erzeugte Aktivierungsdaten werden nicht schriftlich festgehalten. Die Chipkarten zur Aktivierung werden in genügender Anzahl erzeugt, damit die Schlüssel der Zertifizierungsstelle nicht durch Zerstörung oder Verlust von Chipkarten unbrauchbar werden.

6.4.2 Schutz der Aktivierungsdaten

6.4.2.1 Aktivierungsdaten für Zertifizierungsschlüssel

Die Mitarbeiter, die über Aktivierungsdaten verfügen, verpflichten sich, diese geheim zu halten (PIN) und sicher aufzubewahren (Chipkarte).

6.4.2.2 Aktivierungsdaten der Zertifikatsinhaber

Die Zertifikatsinhaber sind verpflichtet, ihre Aktivierungsdaten für den geheimen Schlüssel (PIN) nicht weiterzugeben und nicht an für unberechtigte Personen sichtbarer Stelle aufzubewahren.

6.5 Lebenszyklus der Sicherheitsvorkehrungen

6.5.1 Systementwicklung

Die Vorgaben zur Systementwicklung orientieren sich an den Sicherheitsvorgaben von a.trust.

6.5.2 Sicherheitsmanagement

Die Vorgaben zum Sicherheitsmanagement orientieren sich an den Sicherheitsvorgaben von a.trust.

6.5.3 Bewertung

Die Vorgaben zur Bewertung orientieren sich an den Sicherheitsvorgaben von a.trust.

6.6 Vorkehrungen zur Netzwerksicherheit

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

6.7 Vorkehrungen zur Wartung (Analyse) des kryptographischen Moduls

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

7 Profile von Zertifikaten und Widerrufslisten

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

7.1 Zertifikatsprofile

7.1.1 CA-Zertifikat a.sign Company Root

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 = CommonName OU = OrganizationalUnit O = Name C = AT	CommonName, OrganizationalUnit: (für CA-Version 02 und höher): A-Trust-Qual-nn (für CA-Version 01): A-Trust-nQual-01 Name (für CA-Version 02 und höher): A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH (für CA-Version 01): A-Trust
Gültig von Gültig bis	Beginn und Ende der Gültigkeit des Zertifikats	Der Gültigkeitszeitraum beträgt höchstens zehn Jahre
Zertifikatsinhaber	CN = Company-Root-nn OU = Company-Root-nn O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH C = AT	-nn bezeichnet die Generation der CA.

Öffentlicher Schlüssel	RSA 2048 Bit	Öffentlicher Schlüssel des Zertifikats-inhabers (der CA)

Tabelle 8 Profil für CA-Zertifikat

7.1.2 Zertifikate für Zertifikatsinhaber

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 = Company-Root-nn OU = Company-Root-nn O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH C = AT	-nn bezeichnet die Generation der CA.
Gültig von Gültig bis	Beginn und Ende der Gültigkeit des Zertifikats	Der Gültigkeitszeitraum beträgt höchstens zehn Jahre
Zertifikatsinhaber	CN=Common Name O=Organization OU=OrganizationalUnit C=Country	Common Name, Organisation, Organisationsuntereinheit, Country: Inhalt lt. Kapitel 3.1.1
Öffentlicher Schlüssel	mind. RSA 1024 Bit	Öffentlicher Schlüssel des Zertifikats-inhabers

Tabelle 9 Profil für a.sign Company Root

7.1.3 Erweiterungen (certificate extensions)

In den Zertifikaten der Root-CA und der a.sign Company Root werden die folgenden Erweiterungen gemäß X.509 v3 und PKIX verwendet:

Erweiterung	Zertifikatstyp		Klassifikation	
	a.trust Root	CA	kritisch	Nicht kritisch
Standard-erweiterungen				
authorityKeyIdentifier	Nein	Ja		X
subjectKeyIdentifier	Ja	Ja		X
keyUsage	Ja	Ja	X	
subjectAltName	Optional	Optional		X
certificatePolicies	Nein	Ja		X
basicConstraints	Ja	Ja	X	
cRLDistributionPoints	Nein	Ja		X
Private Extensions				
authorityInfoAccess	Nein	Ja		X

Tabelle 10 Erweiterungen Qual Root CA und a.sign Company Root CA

Die Verwendung von Erweiterungen in den von a.sign Company Root ausgestellten Zertifikaten wird in der folgenden Tabelle dargestellt:

Erweiterung	Im Zertifikat vorhanden	Klassifikation	
		kritisch	Nicht kritisch
authorityKeyIdentifier	Ja		X
subjectKeyIdentifier	Ja		X
keyUsage	Ja	X	
subjectAltName	Optional		X
certificatePolicies	Ja		X
basicConstraints	Ja		X
cRLDistributionPoints	Ja		X

Tabelle 11 Erweiterungen (Signatorzertifikat)

Auf die Erweiterung keyusage wird in den Abschnitten 6.1.8.2 und 6.1.8.3 näher eingegangen.

7.2 Profil der Widerrufsliste

7.2.1 Versionsnummern

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

7.2.2 a.trust CRL und CRL Entry Extensions

Für komplette Widerrufslisten werden die nicht kritischen Erweiterungen authorityKeyIdentifier und CRLNumber verwendet.

Wenn Delta-Widerrufslisten ausgestellt werden, besitzen diese 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 Zertifikatsinhaber erfordern, benötigen eine Anpassung der OID und der URI der Zertifizierungsrichtlinie und damit eine generelle Bekanntmachung gegenüber den Zertifikatsinhaber. Dies sind insbesondere Änderungen hinsichtlich

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

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

8.2 Verfahren zur Publizierung und Bekanntgabe

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

8.3 Genehmigung und Eignung einer Zertifizierungsrichtlinie

Diese Zertifizierungsrichtlinie gilt für das Produkt a.sign Company Root. 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 (siehe auch PIN).
Audit	Sicherheitsüberprüfung, Revision
CA (Certification Authority)	Zertifizierungsinstanz; gleichbedeutend mit Zertifizierungsstelle (siehe dort).
CA-Schlüssel	Schlüssel der CA, die zur Ausstellung von Zertifikaten und dem Unterschreiben von Widerrufslisten (Zertifizierung) verwendet werden.
Certificate Policy	Eine eindeutig identifizierte Menge von Regeln, die den Verwendungszweck eines Zertifikats zu einer speziellen Gruppe und/oder Klasse von Applikationen gleicher Sicherheitsanforderungen anzeigt.
Dienste (CA-Dienste)	Überbegriff für angebotene Dienstleistungen wie Verzeichnisdienst, Statusauskunft und Zeitstempeldienst
Gültigkeitsmodell	Modell nach dem die Prüfung der Gültigkeit von Zertifikaten und Signaturen vorgenommen wird.
Kettenmodell	Gültigkeitsmodell nach dem eine gültige Anwendung des Schlüssels dann erfolgt, wenn zum Zeitpunkt der Anwendung das Zertifikat gültig ist und das übergeordnete Zertifikat zum Zeitpunkt der Erstellung des eingesetzten Zertifikats gültig war.
Policy	siehe Certificate Policy
Registrierungsstelle	In der Registrierungsstelle werden Zertifikatsinhaber registriert und identifiziert, bevor sie die Zertifikate erhalten.
Root-CA	Die Root-CA ist die oberste CA in der Zertifizierungshierarchie der a.trust. Sie stellt die Zertifikate für die nachgeordneten CAs aus.
Signaturerstellungsdaten	Signaturerstellungsdaten sind einmalige Daten wie Codes oder private Signaturschlüssel, die von dem Zertifikatsinhaber zur Erstellung einer elektronischen Signatur verwendet werden.
Signaturprüfdaten	Signaturprüfdaten sind Daten wie Codes oder öffentliche Signaturschlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden.

Statusauskunft	Ein Dienst, bei dem die Anwender Auskunft über den aktuellen Status (gültig oder widerrufen) eines Zertifikates abrufen können. Der Zugriff wird über OCSP realisiert, bzw. auch mittels CRLs, die über den Verzeichnisdienst abrufbar sind.
Verzeichnis (-dienst)	Dienst, bei dem die Anwender Zertifikate der CA oder anderer Anwender sowie CRLs abrufen können. Der Zugriff wird über LDAP realisiert.
Widerrufsliste	Liste, in der alle widerrufenen Zertifikate aufgeführt sind und die mit einem Schlüssel der CA signiert ist.
Zeitstempel	Digitale Signatur von 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 Daten im Zertifikat der a.trust festgehalten sind.
Zertifikatsnutzer	Anwender, der Zertifikate der a.trust über die Schlüssel und Daten anderer nutzt, um Signaturen zu prüfen.
Zertifizierungsrichtlinie	Gleichbedeutend mit „Certification Practice Statement“: Richtlinien über die Praktiken der Zertifizierungsstelle zur Ausgabe von Zertifikaten.
Zertifizierungsstelle	Die Zertifizierungsstelle stellt in Zertifikaten die Zuordnung von Zertifikatsinhabern zu Schlüsseln sicher. Zusätzlich übernimmt sie noch weitere Dienstleistungen, wie z. B. das Veröffentlichen von Zertifikaten oder Widerrufslisten.

B Abkürzungsverzeichnis

CA	Certification Authority, gleichbedeutend mit Zertifizierungsstelle
CPS	Certification Practice Statement, gleichbedeutend mit Zertifizierungsrichtlinie
CRL	Certificate Revocation List, gleichbedeutend mit Widerrufsliste
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol, Protokoll für die Statusauskunft
OID	Object Identifier
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PUK	Personal Unblocking Key
RA	Registration Authority, gleichbedeutend mit Registrierungsstelle
RCA	Revocation Center Agent
RFC	Request for Comments
RO	Registration Officer
RSA	Signatur- und Verschlüsselungsverfahren; benannt nach Rivest, Shamir und Adleman
SigG	Österreichisches Signaturgesetz
SigV	Verordnung zum Österreichischen Signaturgesetz
SO	Security Officer
URI	Uniform Resource Identifier

C Referenzdokumente

[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
[RFC2527]	RFC 2527, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, March 1999