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
www.a-trust.at

a.trust

Certification Practice Statement für einfache Zertifikate a.sign government

Version: 1.0

Datum: 11.12.2003

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

1 Einleitung

1.1 Überblick

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

Eine Zertifizierungsrichtlinie gibt Auskunft über die Praktiken der Zertifizierungsstelle zur Ausstellung von a.sign government Zertifikaten. Sie dient dazu, die Praktiken 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 Zertifizierungs-richtlinie:	a.trust Certification Practice Statement für einfache Zertifikate a.sign government
Version:	1.0/11.12.2003
Object Identifier:	**1.2.040.0.17** (a.trust) **.2** (CPS) **.14** (a.sign government) **.1.0** (Version) vorliegende Version

1.3 Zertifizierungsinfrastruktur und Anwendbarkeit

1.3.1 Zertifizierungsstellen

Es existiert eine zentrale Zertifizierungsstelle, die die Schlüssel der Zertifikatsinhaber sowie die Widerrufslisten für Zertifikate signiert. a.trust stellt unter dieser Zertifizierungsrichtlinie

- Softwarezertifikate für Mitarbeiter von Behörden (öffentlichen Verwaltungseinheiten) sowie
- Zertifikate für Signaturdienste von Behörden (Signaturserver, Erstellen von Amtssiegeln)

aus.

1.3.2 Registrierungsstellen

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

1.3.3 Widerrufsdienst

Die Zertifikatsinhaber können sich zum Zweck der Durchführung eines Widerrufs ihres Zertifikats an den Widerrufsdienst wenden und dessen Durchführung veranlassen.

1.3.4 Anwender

Unter „Anwender“ sind einerseits die Personen zu verstehen, welche Zertifikate von a.trust erhalten (Zertifikatsinhaber) und andererseits jene, die Zertifikate nutzen bzw. den Zertifikatsangaben vertrauen. Letztere sind Empfänger von digital signierten Daten einer Behörde oder eines Behördenmitarbeiters.

1.3.5 Anwendbarkeit

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

Die folgenden Anwenderzertifikate unterliegen dieser Zertifizierungsrichtlinie:

- Zertifikate, die nur an Mitarbeiter von Behörden ausgestellt werden und deren private Schlüssel zur Signatur von E-Mails dienen (a.sign government user),

- Zertifikate von Signaturschlüsseln, die von einem Signaturdienst einer Behörde (Signaturserver) zur Erstellung digitaler Signaturen verwendet werden (a.sign government server).

1.3.6 Zertifizierungshierarchie

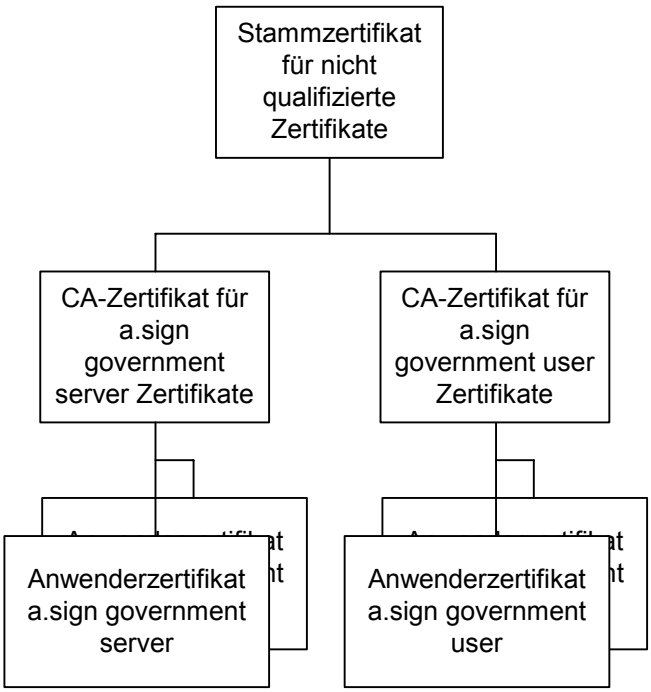

Abbildung 1 Zertifizierungshierarchie

1.3.7 a.trust Verzeichnisbaum

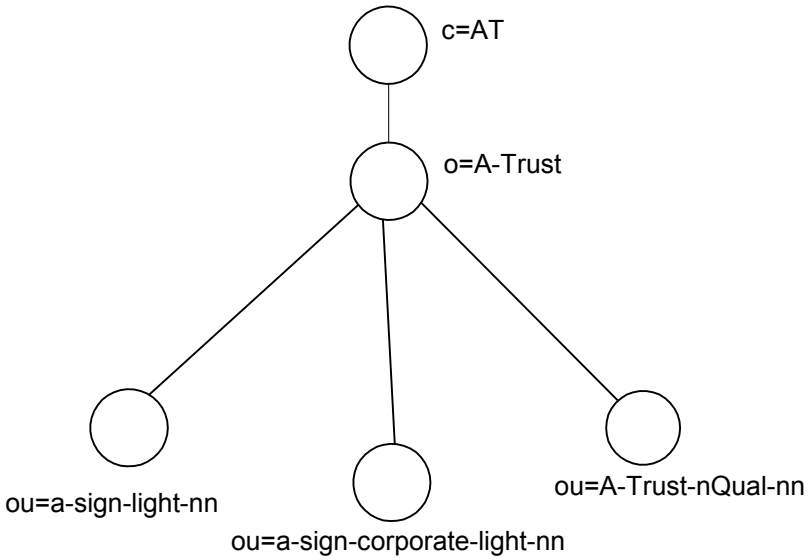

Abbildung 2 a.trust Verzeichnisbaum

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

Mit A-Trust-nQual-nn werden die CA-Zertifikate für nicht qualifizierte Zertifikate und die zugehörigen CRLs signiert.

Die a.sign government server Zertifikate und die zugehörigen CRLs werden mit dem CA-Schlüssel a-sign-corporate-light-nn signiert, die a.sign government user Zertifikate und die zugehörigen CRLs mit dem CA-Schlüssel a-sign-light-nn, wobei -nn die Version der Zertifizierungsstelle bezeichnet, welche mit dem zugehörigen geheimen Schlüssel digitale Signaturen erstellt.

1.4 Ansprechpartner und Kontaktstellen

1.4.1 Organisation zur Verwaltung dieses Dokuments

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

1.4.2 Kontaktinformation

Kontaktinformationen für a.sign government Zertifikate 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 der Registrierungsstelle 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

a.trust übernimmt die Entscheidung über die Anerkennung anderer Policies.

2 Generelle Bestimmungen

2.1 Verpflichtungen

2.1.1 Verpflichtungen der Zertifizierungsstellen

Die Zertifizierungsstelle befolgt die Regelungen dieser Zertifizierungsrichtlinie, die insbesondere die folgenden Aspekte umfasst:

- Die Zertifikate für Zertifikatsinhaber werden im Einklang mit dieser Zertifizierungsrichtlinie erstellt.
- 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 erfolgt ausschließlich zum Signieren der Zertifikate der Zertifikatsinhaber und zum Signieren der Widerrufslisten zu diesen Zertifikaten.
  Anmerkung: Es gibt auch private Schlüssel für andere Zwecke. In dieser Richtlinie werden nur die privaten Schlüssel für die Ausstellung von Zertifikaten und Widerrufslisten behandelt.
- Die Zertifizierungsstelle veröffentlicht alle ausgestellten Zertifikate.

2.1.2 Verpflichtungen der Registrierungsstellen

Die Registrierungsstellen der a.trust befolgen die Regelungen dieser 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 Authentikationsmechanismen sicher, die in dieser Zertifizierungsrichtlinie beschrieben sind.

- Die Registrierungsstellen beschäftigen Personal mit angemessener Qualifikation.

- Die Registrierungsstelle stellt die Zertifikate dem Zertifikatsinhaber in elektronischer Form zur Verfügung.
  Weiters macht a.trust dem Zertifikatsinhaber insbesondere folgende Dokumente elektronisch zugänglich:

  - 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 Allgemeinen Geschäftsbedingungen zusammen mit den Certificate Policies für a.sign government user und a.sign government server, der gegenständlichen Zertifizierungsrichtlinie und den Entgeltbestimmungen von a.trust als Grundlage für den abgeschlossenen Vertrag anzuerkennen.

- Der Zertifikatsinhaber 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 Authentikation mit.

- Der Zertifikatsinhaber ist verpflichtet, seinen privaten Schlüssel angemessen zu schützen. Dies umfasst insbesondere keinen Zugriff durch unautorisierte Personen auf den privaten Schlüssel (auf einem digitalen Medium, wie z. B. Festplatte eines Rechners, gespeichert), zuzulassen und, wenn er für den privaten Schlüssel Aktivierungsdaten (PIN) vergeben hat, diese nicht weiterzugeben.

- Der Zertifikatsinhaber kann jederzeit einen Widerruf veranlassen.

- Der Zertifikatsinhaber setzt sein Zertifikat nur zu dem im Zertifikat angegebenen Zweck ein (siehe hiezu Kapitel 7.1.2.2). Maßgeblich hierfür sind die zum Zeitpunkt der Ausstellung des Zertifikats gültige Zertifizierungsrichtlinie und die zugehörige Policy (a.sign government user bzw. a.sign government server).

- Der Zertifikatsinhaber 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 verpflichten sich, vor der Akzeptanz einer Signatur/eines Zertifikats folgende Prüfungen durchzuführen:

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

2.1.5 Verpflichtungen der Verzeichnisdienste

Der Verzeichnisdienst veröffentlicht die ausgestellten Zertifikate nach ihrer Fertigstellung und in regelmäßigen Abständen Listen mit 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

- die privaten Schlüssel und die ihnen zugeordneten öffentlichen Schlüssel einander bei der Verwendung der von a.trust bereitgestellten oder als geeignet bezeichneten Produkte und Verfahren in komplementärer Weise entsprechen,

- 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,
- 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. 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.

Die Zertifizierungsstelle haftet für die Registrierungsstellen.

2.2.2 Haftung der Registrierungsstelle

Die Zertifizierungsstelle haftet für die Registrierungsstellen.

2.3 Finanzielle Verantwortung

2.3.1 Schadensersatz der beteiligten Parteien

Keine Bestimmungen.

2.3.2 Treuhänderische Beziehungen

Keine Bestimmungen.

2.3.3 Administrative Prozesse

Keine Bestimmungen.

2.4 Auslegung und (gerichtliche) Durchsetzung

2.4.1 Zugrunde liegende Gesetzesbestimmungen

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

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

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

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 gültigen Gebühren finden 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 der Zertifikate über den Verzeichnisdienst ist kostenfrei.

2.5.3 Widerruf von Zertifikaten

Der Widerruf eines Zertifikats ist kostenfrei.

2.5.4 Abrufen von Statusinformationen

Der Zugang zu Widerrufslisten und Statusinformationen ist gebührenfrei.

2.5.5 Richtlinien für Gebührenrückerstattung

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

2.6 Bekanntmachung und Verzeichnisdienste

2.6.1 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:	http://ocsp.a-trust.at/ocsp

Tabelle 1 a.trust Homepage und Verzeichnisdienste

2.6.2 a.trust Stammzertifikat

Das a.trust Stammzertifikat ist unter

http://www.a-trust.at/certs/A-Trust-nQual-nnx.crt

zu finden, wobei -nn die Versionsnummer der Root-CA bezeichnet und x die Generationsbezeichnung des Root-CA-Schlüssels ist (z. B. A-Trust-nQual-01a.crt).

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

2.6.3 CA-Zertifikat

Das jeweils benötigte CA-Zertifikat ist unter

- http://www.a-trust.at/certs/a-sign-corporate-light-nnx.crt
  für a.sign government server Zertifikate bzw.
- http://www.a-trust.at/certs/a-sign-light-nnx.crt
  für a.sign government user Zertifikate

zu finden, wobei -nn die Versionsnummer der Zertifizierungsstelle bezeichnet und x die Generationsbezeichnung des Zertifizierungsschlüssels ist
(z. B. a-sign-light-01a.crt).

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

2.6.4 Widerrufsinformationen

Verteilungspunkte für die Zertifikatswiderrufslisten (CRLs):

- ldap://ldap.a-trust.at/ou=a-sign-corporate-light-nn,o=A-Trust,c=AT?certificaterevocationlist?

- ldap://ldap.a-trust.at/ou=a-sign-light-nn,o=A-Trust,c=AT?certificaterevocationlist?

(-nn bezeichnet die Versionsnummer der a.trust Zertifizierungsstelle, z. B. ou= a-sign-light-01).

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

2.6.5 Suche nach einem Zertifikat

Für die Suche nach einem bestimmten a.sign government user Zertifikat und den Download eines gefundenen Zertifikats steht auf der a.trust Homepage ein Formular zur Eingabe der Suchkriterien zur Verfügung.

2.6.6 Veröffentlichung von Informationen der Zertifizierungsstelle

Die Zertifizierungsstelle veröffentlicht

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

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

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

a.trust stellt alle Informationen wie folgt bereit:

- auf der Web-Seite http://www.a-trust.at/
- 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. Insbesondere im Notfall bieten sich die Printmedien oder TV zur schnellen Bekanntgabe z. B. einer Kompromittierung eines CA-Schlüssels an.

2.6.7 Frequenz der Aktualisierung

Eine Aktualisierung der Zertifizierungsrichtlinie erfolgt gemäß Kapitel 8.

2.6.8 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.

2.6.9 Verzeichnisse

Folgende Verzeichnisse werden von der Zertifizierungsstelle 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 Zertifizierungsrichtlinien abrufbar und den Anwendern weitere allgemeine Informationen zugänglich sind.

2.7 Interne Prüfung (Audit)

2.7.1 Häufigkeit des Audits

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

2.7.2 Identität bzw. Anforderungen an den Auditor

Interne Audits werden im Rahmen der Revision durchgeführt.

2.7.3 Beziehungen zwischen Auditor und zu untersuchender Partei

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

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, welches die folgenden Konsequenzen nach sich zieht:

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

2.7.6 Bekanntgabe der Ergebnisse

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

2.8 Vertraulichkeit

2.8.1 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.

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

2.8.2 Nicht vertraulich eingestufte Informationen

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

2.8.3 Offenlegung von Informationen zu Zertifikatswiderruf

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

2.8.4 Offenbarung an Behörden im Rahmen gesetzlicher Pflichten

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

2.8.5 Offenbarung im Rahmen zivilrechtlicher Auskunftspflichten

Wird wie in Abschnitt 2.8.4 behandelt.

2.8.6 Weitere Gründe zur Freigabe von vertraulichen Informationen

Wird wie in Abschnitt 2.8.4 behandelt.

2.9 Urheberrechte und Eigentumsrechte

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

- Zertifizierungsrichtlinie und
- Certificate Policy.

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 Angaben des Zertifikatsinhabers werden in zwei Kategorien eingeteilt. Dies sind zum einen die erforderlichen und zum anderen die optionalen Angaben.

3.1.1.1 a.sign government server

Es sind folgende Daten aufzunehmen:

- der vollständige Name und die Kontaktinformationen des Organisationsverantwortlichen,
- Kontaktinformationen eines technischen Verantwortlichen, sofern dieser nicht mit dem Organisationsverantwortlichen identisch ist
- Passwort für den Widerruf
- Name des Signaturdienstes oder
  Name des zur Signatur (Amtssiegel) berechtigten Mitarbeiters der Dienststelle
- Name und Sitz der Behörde,
- optional:
  Name der Organisationsuntereinheit (Dienststelle)
- optional:
  Angabe einer näheren Bezeichnung des von der Behörde angebotenen Signaturdienstes (URL)
- optional:
  Verwaltungsbezeichner

3.1.1.2 a.sign government user

Es sind folgende Daten aufzunehmen:

- der vollständige Name des Zertifikatswerbers,
- Organisationszugehörigkeit

- Dienstanschrift, Diensttelefonnummer
- die E-Mailadresse (Domain „gv.at“) des Zertifikatswerbers
- E-Mailadresse des Organisationsverantwortlichen
- ggf. Verwaltungsbezeichner.

Der Name des Zertifikatsinhabers und seine E-Mailadresse (Zertifikatserweiterung) sind zwingende Inhalte des Zertifikats.

3.1.2 Anforderungen an die Namen

Die E-Mailadresse für das a.sign government user Zertifikat muss die Form antragsteller@organisation.gv.at haben.

3.1.3 Regeln zur Interpretation unterschiedlicher Namensformen

Keine Bestimmungen.

3.1.4 Eindeutigkeit der Namen

Jeder Inhaber eines a.sign government user Zertifikats erhält eine zwölf-stellige Identifikationsnummer. Diese Nummer ist ein Teil des eindeutigen Namens des Zertifikatsinhabers und ermöglicht die eindeutige und unveränderliche Zuordnung zu einem Zertifikatsinhaber.
Anmerkung: a.sign government server Zertifikate enthalten diese Nummer ebenfalls, aber hier wird sie nicht zur eindeutigen Identifikation des Namens des Inhabers verwendet.

3.1.5 Anspruch auf Namen und Beilegung von Streitigkeiten

Keine Bestimmungen.

3.1.6 Anerkennung, Bestätigung und Bedeutung von Warenzeichen

Keine Bestimmungen.

3.1.7 Methode zum Beweis des Besitzes des geheimen Schlüssels

3.1.7.1 Generierung durch die Registrierungsstelle

Wird das Schlüsselpaar von der Registrierungsstelle generiert, so wird es zusammen mit dem Zertifikat in verschlüsselter Form per E-Mail an den Antragsteller gesandt. Damit ist gewährleistet, dass der Zertifikatsinhaber im Besitz des privaten Teils des Schlüsselpaars ist. Die Registrierungsstelle löscht das erstellte Schlüsselpaar nach dem Absenden an den Zertifikatsinhaber und gewährleistet damit die Rechte des Zertifikatsinhabers auf die Einzigartigkeit der Schlüsselverwaltung.

3.1.7.2 Generierung durch den Antragsteller

Wird der Schlüssel zu einem a.sign government user Zertifikat im Browser des Antragstellers generiert, so befindet sich der private Schlüssel ausschließlich bei diesem und ein Beweis des Besitzes ist nicht notwendig.

Wird der Schlüssel zu einem Signaturserverzertifikat mittels Software durch den zuständigen technischen Verantwortlichen generiert, so wird gleichzeitig im selben Arbeitsschritt der Zertifikatsrequest an a.trust erstellt. Somit ist sicher gestellt, dass der Antragsteller im Besitz des privaten Schlüssels ist.

3.1.8 Authentisierung von Personen

3.1.8.1 a.sign government user

Der Antrag des Zertifikatswerbers wird von einem Organisationsverantwortlichen der Behörde genehmigt. Somit ist die Berechtigung der Antragstellung aus Behördensicht gegeben.

Weiters gibt der Antragsteller mit der Bestellung seine dienstliche E-Mailadresse und Telefonnummer an. Nach Aufforderung per E-Mail ruft er bei der Registrierungsstelle an, worauf er von dieser zurückgerufen wird. Damit wird die Identität mit dem Antragsteller durch die Registrierungsstelle geprüft.

3.1.8.2 a.sign government server

Der Organisationsverantwortliche der Behörde bzw. der technische Verantwortliche sendet eine Ausweiskopie an die Registrierungsstelle, sodass die Identität der Person überprüft werden kann.

3.2 Erneute Registrierung/Rezertifizierung

Vor der Bestellung eines neuen Zertifikats muss das ursprüngliche Zertifikat widerrufen werden.

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 Zertifikatsinhaber bzw. die Person, der das Widerrufspasswort bekannt ist (Organisationsverantwortlicher), kann das Zertifikat mit telefonischem Antrag beim Widerrufsdienst widerrufen lassen. Zur Durchführung eines Widerrufs muss der Antragsteller das Widerrufspasswort und den Common Name des Zertifikats bzw., wenn nötig, weitere Informationen über das Zertifikat angeben.

4 Betriebliche Anforderungen

4.1 Antrag auf Ausstellung von Zertifikaten

4.1.1 a.sign government user

Zur Zertifikatsanforderung sendet der Zertifikatswerber einen Antrag an a.trust. Der Antrag wird nach Genehmigung von einem Organisationsverantwortlichen an a.trust übermittelt. Die Schlüsselgenerierung kann im Browser des Antragstellers oder durch die Registrierungsstelle der a.trust erfolgen.

4.1.2 a.sign government server

Zur Zertifikatsanforderung wird der Antrag an die Registrierungsstelle übermittelt. Der schriftliche Antrag muss unterzeichnet und mit Behördenstempel versehenen sein. Benötigte Ausweiskopien verantwortlicher Personen sind mitzusenden. Damit ist die Berechtigung zur Zertifikatsausstellung sicher gestellt. Die Schlüsselgenerierung kann vom Antragsteller oder von der Registrierungsstelle der a.trust vorgenommen werden.

4.2 Herausgabe und Akzeptanz von Zertifikaten

4.2.1 Schlüsselgenerierung durch die Registrierungsstelle

Wenn die Generierung von a.trust durchgeführt wird, so läuft die Schlüsselerzeugung wie folgt ab:

Die Registrierungsstelle generiert das Schlüsselpaar und die CA erstellt aufgrund des Zertifikatsrequests der RA das Zertifikat. Sowohl die Schlüssel als auch das Zertifikat werden in einem gemeinsamen PKCS#12-File per E-Mail an den Antragsteller versandt. Das PKCS#12-File ist mit einer von a.trust generierten PIN verschlüsselt. Diese PIN erfährt der Antragsteller per Telefon von der Registrierungsstelle.

4.2.2 Schlüsselgenerierung durch den Browser des Antragstellers

Wenn die Generierung im Browser des Antragstellers durchgeführt wird, so läuft die Schlüsselerzeugung wie folgt ab:

Dem Antragsteller werden nach telefonischer Identifikation durch den RO sowohl der URL als auch die Zugangsberechtigung (12-stellige Identifikationsnummer) für die Schlüsselgenerierung mitgeteilt. Nach dem Aufruf der Seite durch den Antragsteller wird das Schlüsselpaar erzeugt und die öffentliche Komponente an die Zertifizierungsstelle gesandt. Der Antragsteller erhält dann eine E-Mail mit Passwort zur Abholung des Zertifikats und das Zertifikat wird installiert.

4.2.3 Schlüsselgenerierung durch den Antragsteller

Die Generierung des Schlüssels erfolgt mit einer geeigneten Software auf einem Rechner der beantragenden Behörde. Die öffentliche Schlüsselkomponente wird elektronisch an die Registrierungsstelle übermittelt und von dieser zur Zertifizierung an die CA gesandt. Der Antragsteller erhält das Zertifikat elektronisch von der RA.

4.3 Widerruf von Zertifikaten

Zertifikate können sofort und permanent widerrufen werden.

4.3.1 Gründe für einen Widerruf

Der Widerruf eines Zertifikats wird erforderlich, wenn

- sich wesentliche Angaben im Zertifikat geändert haben,
- der private Schlüssel nicht mehr verwendet werden kann (z. B. das Speichermedium ist defekt und keine Sicherung verfügbar),
- Verdacht auf eine Kompromittierung besteht (z. B. ein Unbefugter hatte Zugriff auf den Rechner, auf dem sich der private Schlüssel befindet) bzw. eine Kompromittierung vorliegt,

- 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,
- die Behörde ein in ihren Bereich gehöriges a.sign government Zertifikat widerrufen lassen will.

4.3.2 Wer kann einen Widerruf anordnen

Ein Widerruf eines Zertifikates kann angeordnet werden durch:

- die Person, die das Passwort für den Widerruf kennt (Zertifikatsinhaber bzw. Organisationsverantwortlicher) und
- die Zertifizierungsstelle selbst.

4.3.3 Prozedur für einen Widerrufsantrag

Die Anforderungen an den Ablauf des Widerrufs werden nachfolgend aufgeführt:

- der Antragsteller ruft beim Widerrufsdienst an,
- die Angabe des Passworts ist verpflichtend,
- der Grund für den Widerruf (Kompromittierung des privaten Schlüssel, Änderung von Zertifikatsinhalten, etc.) muss dem Mitarbeiter des Widerrufsdienstes mitgeteilt werden.

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 Erreichbarkeit des Widerrufsdienstes (aktuelle Telefonnummer und Geschäftszeit) ist der a.trust Homepage zu entnehmen.

4.3.5 Aktualisierungsfrequenz der Widerrufsliste

Die aktuelle Update-Frequenz der Widerrufsliste ist 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 (Signaturempfänger). 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 einem auf einem gültigen Zertifikat der Zertifizierungsstelle beruhenden Schlüssel signiert wurde und
- sich das Zertifikat nicht in der aktuellen Widerrufsliste befindet.

Bei einer erhaltenen Signatur ist ferner zu prüfen, ob der Zeitpunkt der Unterschrift im Gültigkeitszeitraum des Zertifikats liegt.

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 Weitere Verfahren zur Bekanntgabe von Widerrufen

Keine Bestimmungen.

4.3.10 Anforderungen an die Überprüfung weiterer Verfahren zur Bekanntgabe von Widerrufen

Keine Bestimmungen.

4.3.11 Spezielle Verfahren bei Kompromittierung von privaten Schlüsseln

Der Zertifikatsinhaber beantragt einen Widerruf, wenn er Grund zur Annahme hat, dass sein auf dem Rechner befindlicher privater Schlüssel kompromittiert wurde oder der Rechner von einem Unbefugten in Betrieb genommen und gleichzeitig die PIN (Aktivierungsdaten des Schlüssels) unberechtigten Personen bekannt wurde.

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.

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.

4.4.7 Bewertungen zur Angreifbarkeit

Keine Bestimmungen.

4.5 Archivierung

4.5.1 Archivierte Daten

Archiviert werden:

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

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.
- 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 sind mit einem Zeitstempel zu versehen. Dies betrifft insbesondere die Widerrufsanträge sowie die Änderungen an den Widerrufslisten.

4.5.5 System zur Erfassung der Archivierungsdaten (intern / extern)

Das System für das Zertifikatsmanagement ist für die Archivierung aller im 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-CA-Schlüsseln erfolgt im Zusammenhang mit dem Ausfall eines Hardware Security Moduls oder wenn die verwendeten Schlüssellängen bzw. Algorithmen nicht mehr den Sicherheitserwartungen entsprechen sollte 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 Kapitel 6.3.2 zu entnehmen. Der Überprüfer eines Zertifikats erhält das neue Zertifikat über den Verzeichnisdienst. Er kann über die Zertifizierungskette 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 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.

4.7.2 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. Diese privaten Schlüssel werden entsprechend Abschnitt 6.2.9 vernichtet.

4.7.2.1 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.

4.7.2.2 Widerruf des Zertifikats der Zertifizierungsstelle

Wird ein Zertifikat der Zertifizierungsstelle wegen Kompromittierung widerrufen, so müssen 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.

Zertifikatsinhaber, 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.

4.7.2.3 Schlüsselwechsel

Nach dem Widerruf des Zertifikats wird der dazugehörige private Schlüssel nicht wieter 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 umgehend über den Schlüsselwechsel informiert.

- Es findet keine Crosszertifizierung mit dem ungültigen Zertifikat statt. Die Zertifikatsinhaber 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.

4.7.2.4 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.

4.7.3 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 erfolgen das Abschalten des Verzeichnisdienstes und die Einstellung 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.

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

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

4.8 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 Widerrufen betroffenen Zertifikatsinhaber werden vom Widerruf ihres Zertifikates informiert.

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

a.trust trägt dafür Sorge, dass die CRLs der eingestellten Zertifizierungsstelle auch nach der Beendigung den Benutzern öffentlich und authentisch zur Verfügung stehen.

5 Physische, verfahrensorientierte und personelle Sicherheitsvorkehrungen

5.1 Physische Sicherheitsvorkehrungen

5.1.1 Standort und örtliche Gegebenheiten

Die Dienstleistungen der a.trust werden in den folgenden Örtlichkeiten vorgenommen:

Dienstleistung	Adresse
Firmensitz	A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH. Landstraßer Hauptstraße 5 A-1030 Wien
Registrierung Widerrufsdienst	Die Registrierungsstellen und den Widerrufsdienst von a.trust 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 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 Dieselaggregat.

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
- 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 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 (7 x 24 Stunden) des Rechenzentrumsbetriebs erreicht werden kann.

5.2 Verfahrensorientierte Sicherheitsvorkehrungen

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

5.2.1 Funktionen der a.trust

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

Tabelle 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 Widerrufsanträgen
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 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

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

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

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

5.3.2 Überprüfung des Personals

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 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 Sicherheitssysteme statt.

5.3.5 Ablauf und Frequenz der Job Rotation

Keine Bestimmungen.

5.3.6 Sanktionen für unautorisierte Handlungen

Schwerwiegende Verstöße gegen Sicherheitsvorkehrungen werden disziplinarisch geahndet.

5.3.7 Anforderungen an Vertragsvereinbarungen mit dem Personal

Das Personal ist gemäß Datenschutzgesetz zur Geheimhaltung verpflichtet.

5.3.8 An das Personal auszuhändigende Dokumente

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

- Betriebskonzept,
- 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 Zertifizierungsstelle 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 aller 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 können in der Software der Registrierungsstelle generiert werden. Der öffentliche Schlüssel wird in einem Zertifikatsantrag an die CA übermittelt. Diese sendet das fertig gestellte Zertifikat an die Registrierungsstelle, die dann das Schlüsselpaar und das Zertifikat zusammen in einem PKCS#12-File an den Antragsteller schickt.

Alternativ generiert der Antragsteller eines a.sign government user Zertifikats den Schlüssel selbst in seinem Browser nach Anstoß über eine personalisierte Web-Seite von a.trust. Es wird ein Zertifikatsrequest (gem. PKCS#10) an a.trust gesandt und das fertig gestellte Zertifikat kann der Antragsteller mit Passwort von der bekannt gegebenen Web-Seite abholen.

Im Falle von a.sign government server Zertifikaten kann der technische Verantwortliche der Behörde den Schlüssel selbst mit Hilfe geeigneter Software generieren und einen PKCS#10-Request an die Registrierungsstelle senden. Zur Abholung des Zertifikats erhält er eine E-Mail, in welcher der Download-Bereich des Zertifikats angegeben ist.

6.1.2 Auslieferung privater Schlüssel an Zertifikatsinhaber

6.1.2.1 Generierung durch die Registrierungsstelle

Der Antragsteller erhält seinen privaten Schlüssel in verschlüsselter Form zugesandt. Der Zugriff auf diesen Schlüssel zum Zweck der Installation im Browser des Signator-PCs ist nur mit einer telefonisch mitgeteilten PIN möglich.

6.1.2.2 Generierung durch den Browser des Antragstellers

Der Antragsteller generiert seinen Schlüssel selbst in seinem Browser und ist daher im Besitz des privaten Schlüssels, weshalb eine Auslieferung nicht notwendig ist.

6.1.2.3 Generierung durch die Software des Antragstellers

Der technische Verantwortliche der Behörde generiert den Schlüssel selbst mit Hilfe geeigneter Software des Servers, auf dem der Signaturdienst betrieben wird, und ist daher im Besitz des privaten Schlüssels. Eine Auslieferung desselben ist nicht notwendig.

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 aller Zertifizierungsstellen werden in einem Verzeichnis im Internet veröffentlicht, damit es allgemein zugänglich ist und alle Zertifikatsnutzer Zertifikate dagegen prüfen können.

6.1.3.2 Öffentlicher Schlüssel des Anwenderzertifikats

Der Zertifikatsinhaber verfügt entweder über den Schlüssel, weil er die Generierung selbst angestoßen bzw. vorgenommen hat oder er erhält die öffentliche Komponente zusammen mit der privaten Komponente in verschlüsselter Form an seine bestätigte E-Mail-Adresse zugesandt.

6.1.4 Schlüssellängen

Die Schlüssel der Root-CA und aller 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, die in der Software der Registrierungsstelle erzeugt werden, entsprechen einer Länge von zur Zeit 1024 Bit (RSA-Schlüssel).

Die Zertifikatswerber, welche die Schlüsselgenerierung selbst mit Software vornehmen oder im Browser anstoßen, müssen als Schlüssellänge 1024 Bit (RSA-Schlüssel) wählen.

Als Hash-Algorithmus wird den Zertifikatsinhabern 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 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.

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

Die Schlüssel für a.sign government Zertifikate werden entweder

- durch die Software der Registrierungsstelle,
- im Browser des Antragstellers oder
- durch eine geeignete Software auf dem Rechner des Antragstellers

erzeugt (Details siehe Kapitel 6.1.1.2).

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 Zertifizierungsstelle werden ausschließlich zum Signieren von Zertifikaten und Widerrufslisten eingesetzt.

Deshalb werden die Bits

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

gesetzt.

6.1.8.3 Verwendung des Schlüssels des Zertifikatsinhabers

Der zum a.sign government user Zertifikat gehörige Schlüssel dient zur persönlichen Signatur von E-Mails, weshalb die Schlüsselverwendung wie folgt lautet:

- digitalSignature
- optional kann die folgende extended keyusage angegeben werden: emailProtection

Der zum a.sign government server Zertifikat gehörige Schlüssel dient zur Signaturerstellung, weshalb die Schlüsselverwendung wie folgt lautet:

- digitalSignature
- optional kann eine extended keyusage angegeben werden:
  - codeSigning
  - timeStamping

6.2 Schutz der privaten Schlüssel

6.2.1 Schutz des Schlüssels der Zertifizierungsstelle

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

Die Schlüssel einer Zertifizierungsstelle dienen zur Signatur von Zertifikaten, Widerrufslisten und Crosszertifikaten. Sie werden nur in einer sicheren Umgebung eingesetzt.

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

6.2.2 Schutz der Schlüssel der Zertifikatsinhaber

Die Schlüssel der Zertifikatsinhaber werden auf dem Rechner des Anwenders gespeichert. Die Verwendung des privaten Schlüssels sollte durch eine PIN abgesichert sein.

6.2.3 Aufteilung privater Schlüssel auf mehrere Personen

Private Schlüssel befinden sich entweder in einem Hardware Security Modul (Schlüssel der Root-CA und der Zertifizierungsstelle) oder auf dem Rechner des Anwenders unter dessen Kontrolle (Schlüssel zu a.sign government Zertifikaten).

Es gilt, dass für die Aktivierung des Schlüssels der Root-CA oder einer Zertifizierungsstelle ein Vier-Augen-Prinzip erforderlich ist. 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 Anwendern.

6.2.5 Backup privater Schlüssel

Für private Schlüssel der Root-CA und der Zertifizierungsstelle gibt es kein Backup.

6.2.6 Archivierung privater Schlüssel

Für private Schlüssel der Root-CA und der Zertifizierungsstelle gibt es keine Archivierung.

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.

6.2.7.1 Schlüssel der Zertifizierungsstelle

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

6.2.7.2 Schlüssel der Zertifikatsinhaber

Der private Schlüssel des Zertifikatsinhabers wird auf der Festplatte des Rechners gespeichert und weder in ein Hardware Security Modul eingebracht noch in einem solchen aufbewahrt.

6.2.7.3 Methode zur Freischaltung / Aktivierung privater Schlüssel

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

Den Inhabern der a.sign government Zertifikate wird empfohlen, zur Aktivierung des privaten Schlüssels für die Signaturerstellung eine PIN zu wählen.

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.

6.2.9 Methode zur Vernichtung privater Schlüssel

Für die Löschung ihrer geheimen Schlüssel sind die Zertifikatsinhaber selbst verantwortlich.

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 dabei die übergeordnete Instanz herangezogen. Dabei muss das übergeordnete Zertifikat nur zum Zeitpunkt der Ausstellung des zu überprüfenden Zertifikats gültig gewesen sein. Ein übergeordnetes Zertifikat kann widerrufen werden, ohne dass die ihm untergeordneten Zertifikate dadurch ihre Gültigkeit verlieren. Solange der Zertifizierungsschüssel noch als sicher gilt, kann eine Rezertifizierung vorgenommen werden.

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

Zertifikatstyp	Gültigkeits-dauer
Root-CA	3
Zertifizierungsstellen	3
a.sign government server	3
a.sign government user	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 Root-CA und der Zertifizierungsstellen können ausschließlich im Vieraugen-Prinzip durch zwei Beauftragte mittels Chipkarte und PIN aktiviert werden. Die Aktivierungsdaten werden direkt in einem Hardware Security Modul 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 Signatorenzertifikate

Die Zertifikatsinhaber sind angehalten, eine entsprechende Sicherheitsstufe zu wählen, sodass das Auslösen der Signaturfunktion durch eine PIN abgesichert wird.

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 Zertifikatsinhaber

Die Zertifikatsinhaber sind verpflichtet, ihre PIN (wenn eine vergeben wurde) nicht weiterzugeben und nicht an für andere Personen sichtbarer Stelle aufzubewahren.

6.5 Computer Sicherheitsbestimmungen

6.5.1 Spezifische Sicherheitsanforderungen an die Computer

Keine Bestimmungen.

6.5.2 Bewertung der Computersicherheit

Keine Bestimmungen.

6.6 Lebenszyklus der Sicherheitsvorkehrungen

6.6.1 Systementwicklung

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

6.6.2 Sicherheitsmanagement

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

6.6.3 Bewertung

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

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 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

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-nQual-nn OU = A-Trust-nQual-nn O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH C = AT	-nn bezeichnet die Generation des Schlüssels, der für die Signatur des Zertifikats verwendet wurde. Bei jeder Ausstellung eines neuen Root-Keys wird diese Generationsnummer um eins erhöht.
Gültig von Gültig bis	Beginn und Ende der Gültigkeit des Zertifikats	Der Gültigkeitszeitraum beträgt höchstens drei Jahre
Zertifikatsinhaber	CN = a-sign-corporate-light-nn oder CN = a-sign-light-nn OU = a-sign-corporate-light-nn oder OU = a-sign-light-nn O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH C = AT	-nn bezeichnet die Generation des zertifizierten Schlüssels

Öffentlicher Schlüssel	RSA 2048 Bit	Öffentlicher Schlüssel des Zertifikats-inhabers

Tabelle 8 Profil für CA-Zertifikat

7.1.2 Zertifikate für Zertifikatsinhaber

7.1.2.1 a.sign government user

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-sign-light-nn OU = a-sign-light-nn O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH C = AT	-nn bezeichnet die Generation des Schlüssels, der von a.trust für die Signatur des Zertifikats verwendet wurde. Bei jeder Ausstellung eines neuen CA-Schlüssels wird diese Generationsnummer um eins erhöht.
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 E = E-Mailadresse	CountryName: AT etc. Title: Titel (Dr. etc.) SurName: Zuname GivenName: Vorname CommonName: Vorname + Zuname SerialNumber: eindeutige Identifikationsnummer des Zertifikatsinhabers: siehe auch Abschnitt 3.1.4 E-Mailadresse: xxx@organisation.gv.at

Öffentlicher Schlüssel	RSA 1024 Bit	Öffentlicher Schlüssel des Zertifikats-inhabers

Tabelle 9 Profil für a.sign government user Zertifikat

7.1.2.2 a.sign government server

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-sign-corporate-light-nn OU = a-sign-corporate-light-nn O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH C = AT	-nn bezeichnet die Generation des Schlüssels, der von a.trust für die Signatur des Zertifikats verwendet wurde. Bei jeder Ausstellung eines neuen CA-Schlüssels wird diese Generationsnummer um eins erhöht.
Gültig von Gültig bis	Beginn und Ende der Gültigkeit des Zertifikats	Der Gültigkeitszeitraum beträgt höchstens drei Jahre
Zertifikatsinhaber	C = CountryName CN = CommonName O = Organisation OU = Organisationsunter-einheit Seriennummer = SerialNumber	CountryName: AT etc. CommonName: Bezeichnung des Signaturdienstes oder Name des Mitarbeiters der Dienststelle Organisation: Name der Behörde (vollständig oder Abkürzung) Organisationsuntereinheit:: Untereinheit der Behörde, Dienststelle, Abteilung etc., optional SerialNumber: Identifikationsnummer: siehe auch Abschnitt 3.1.4
Öffentlicher Schlüssel	RSA 1024 Bit	Öffentlicher Schlüssel des Zertifikats-inhabers

Tabelle 10 Profil für a.sign government server Zertifikat

7.1.3 Erweiterungen (certificate extensions)

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

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

Tabelle 11 Erweiterungen (CA-Zertifikate)

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

Erweiterung	Im Zertifikat vorhanden	Klassifikation	
		kritisch	Nicht kritisch
Standarderweiterungen			
AuthorityKeyIdentifier	Ja		X
SubjectKeyIdentifier	Ja		X
KeyUsage	Ja	X	
ExtKeyUsage	optional		X
CertificatePolicies	Ja		X
SubjectAltName	optional		X

		Klassifikation	
BasicConstraints	Ja		X
CRLDistributionPoints	Ja		X
Private Extensions			
1.2.40.0.10.1.1.1	Ja		X

Tabelle 12 Erweiterungen (Anwenderzertifikate)

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

Die Erweiterung subjectAltName kann bei a.sign government server Zertifkaten eine nähere Bezeichnung des Signaturdienstes in Form eines URL enthalten.

Alle a.sign government Zertifikate enthalten eine Zertifikatserweiterung, welche die Behördeneigenschaft ausdrückt (Behördenkennzeichen – OID 1.2.40.0.10.1.1.1). Diese Erweiterung muss vorhanden sein und kann optional auch einen Verwaltungsbezeichner (eindeutiges Kennzeichen für Organisationseinheiten der öffentlichen Verwaltung) enthalten.

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

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

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

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 government. a.trust stellt sicher, dass diese Zertifizierungsrichtlinie für die betroffenen Certificate Policies geeignet ist.

9 Anhang

A Glossar

a.sign government server	Produktname für Serverzertifikate, welche für Signaturdienste von Behörden ausgestellt werden.
a.sign government user	Produktname für Softwarezertifikate, die an Mitarbeiter der öffentlichen Verwaltung ausgestellt werden.
Aktivierungsdaten	Daten, die zur Aktivierung des privaten Schlüssels benötigt werden (siehe auch PIN).
Anwender	Person, die die Dienstleistungen der Zertifizierungsstelle der a.trust nutzt. Anwender sind sowohl Zertifikatsinhaber als auch Zertifikatsnutzer.
Audit	Sicherheitsüberprüfung, Revision
CA (Certification Authority)	Zertifizierungsinstanz; gleichbedeutend mit Zertifizierungsstelle (siehe dort).
CA-Schlüssel	Schlüssel, die zur Ausstellung von Zertifikaten und zum Signieren 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.
Chipkarte	Smart Card auf der die Schlüssel des jeweiligen Anwenders sicher gespeichert sind und auf denen die Signatur berechnet wird.
Dienste (CA-Dienste)	Überbegriff für angebotene Dienstleistungen wie Verzeichnisdienst, Statusauskunft und Zeitstempeldienst
Dienste-Schlüssel	Schlüssel eines Dienstes (bspw. Signaturschlüssel zur Signatur von Statusauskünften)
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 Anwender registriert und identifiziert, bevor sie die Zertifikate erhalten. Die Registrierungsstelle kann auch zusätzliche Aufgaben übernehmen, wie z. B. die Annahme und Weiterleitung von Änderungsanträgen.
Root-CA	Die Root-CA ist die oberste CA in der Zertifizierungshierarchie der a.trust. Sie stellt die Zertifikate für die nachgeordneten CAs aus.
Signaturerstellungs-daten	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	Dienst, bei dem die Anwender Auskunft über den aktuellen Status (gültig oder widerrufen) eines Zertifikates abrufen können. Der Zugriff wird über OCSP realisiert, bzw. dienen hiezu auch 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 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.
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 Herausgabe von Zertifikaten.
Zertifizierungsstelle	Die Zertifizierungsstelle stellt in Zertifikaten die Zuordnung von Anwendern (Personen) oder Diensten zu Schlüsseln sicher. Zusätzlich übernimmt sie noch weitere Dienstleistungen, wie z. B. das Veröffentlichen von Zertifikaten oder Widerrufen.

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