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
https://www.a-trust.at

a.trust
Certification Practice Statement für fortgeschrittene Zertifikate a.sign SSL und a.sign SSL EV

Version: 1.3.5
Datum: 03.06.2015

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

1 Einführung

1.1 Überblick

Das Ziel der vorliegenden Zertifizierungsrichtlinie besteht darin, die Umsetzung der Ausgabe, Administration und Anwendung von a.sign SSL und a.sign SSL EV 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 Herausgabe von a.sign SSL 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 3647 - Internet X.509 Public Key Infrastructures, Certificate Policy and Certification Practices Framework) der Internet Society.

1.2 Identifikation

Name der Richtlinie:	a.trust Certification Practice Statement für fortgeschrittene Zertifikate a.sign SSL und a.sign SSL EV
Version:	1.3.5 / 03.06.2015
Object Identifier:	1.2.40.0.17 (a.trust) .2 (CPS) .22 (a.sign SSL EV) .1.3.5 (Version) vorliegende Version

1.3 Zertifizierungsinfrastruktur und Anwendungsbereich

1.3.1 Zertifizierungsstellen

Es existiert eine zentrale Zertifizierungsstelle, die die öffentlichen Schlüssel der Zertifikatsinhaber von Serverzertifikaten sowie die Widerrufsinformationen für diese Zertifikate signiert.

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.

Die Ausstellung von a.sign SSL EV Zertifikaten erfolgt nur durch A-Trust selbst.

1.3.3 Widerrufsdienst

Die Anwender können sich zum Zweck der Durchführung eines Widerrufs ihres Zertifikats telefonisch oder per Fax an den Widerrufsdienst wenden (Details siehe 2.5.2) und die Durchführung veranlassen.

1.3.4 Anwender

Unter 'Anwender' sind einerseits die Signatoren zu verstehen, welche a.sign SSL bzw. a.sign SSL EV Zertifikate von a.trust erhalten und andererseits jene, die diese Zertifikate nutzen bzw. den Zertifikatsangaben vertrauen.

Bei Anwendern von a.sign SSL EV Zertifikaten handelt es sich immer um juristische Personen; dies wird von A-Trust überprüft.

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 a.sign SSL (EV)) Policy gilt für fortgeschrittene a.sign SSL (EV)) Zertifikate entsprechend der Definition § 2 Abs. 8 [SigG], welche zur Durchführung von Signatur-, Geheimhaltungs- oder Authentifizierungsoperationen ausgestellt werden. Die geheimen Schlüssel der Zertifikatsinhaber befinden sich auf deren Rechner.

A.sign SSL EV Zertifikate unterliegen weiters den Vorgaben aus [EV-GL]. EV Zertifikate sind an der entsprechenden EV-Policy OID zu erkennen. Die Generierung der Schlüssel der Zertifikatswerber wird von diesen selbst in sicherer Weise vorgenommen. Die Schlüssel müssen nicht in spezieller Hardware erzeugt und aufbewahrt werden, jedoch muss die Erzeugung unter Verwendung von Verfahren geschehen die eine hinreichende Zufallsqualität gewährleisten.

A-Trust hält sich an die jeweils aktuelle Version der "CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Vertificates" sowie an die "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", die unter http://www.cabforum.org veröffentlicht werden. Sollte eine Inkonsistenz zwischen CPS bzw. CP von A-Trust und den Guidelines bestehen, so erhalten die Richtlinien aus den Guidelines des CA/Browser Forums den Vorrang.

1.3.6 a.trust Verzeichnisbaum

Eine schematische Darstellung des Verzeichnisbaums ist in Abbildung 1 zu finden. Das Zertifikat des Schlüssels A-Trust-nQual-nn ist das Stammzertifikat, wobei nn die Version der Root-CA bezeichnet, welche mit dem zugehörigen geheimen Schlüssel digitale Signaturen erstellt.

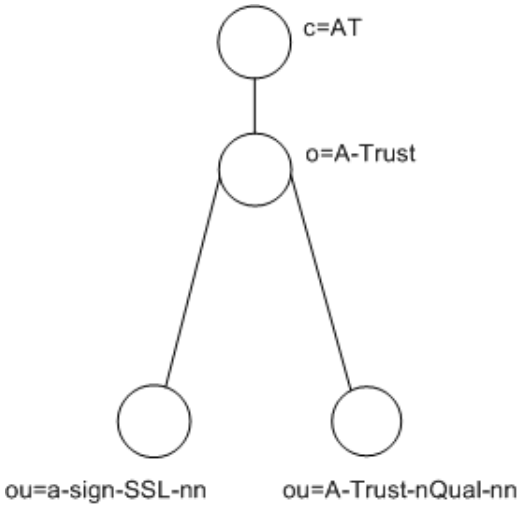

Abbildung 1: a.trust Verzeichnisbaum

Mit A-Trust-nQual-nn werden alle CA-Zertifikate und die zugehörigen CRLs signiert.

Die Zertifikate der Zertifikatsinhaber von a.sign SSL und a.sign SSL EV Zertifikaten und die zugehörigen CRLs werden mit den CA-Schlüsseln

- a-sign-SSL-nn
- a-sign-SSL-EV-nn

signiert, wobei -nn die Version des CA-Zertifikates bezeichnet, welche mit dem zugehörigen geheimen Schlüssel digitale Signaturen erstellt.

1.3.7 Zertifizierungshierarchie

Abbildung 2 zeigt eine schematische Darstellung der Zertifikatshierarchie.

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 SSL (EV)) Zertifikate erhält man auf folgenden Wegen:

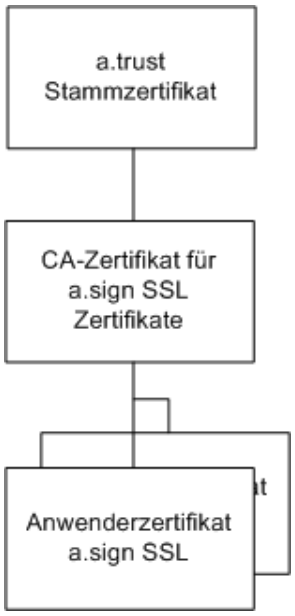

Abbildung 2: Zertifizierungshierarchie

- Auf der Homepage von a.trust:
  https://www.a-trust.at/
- bei der Informationshotline des Call Centers:
  die Telefonnummer und Erreichbarkeit ist auf der a.trust Homepage zu finden.
- in ausgewählten Registrierungsstelle von a.trust und
- auf schriftliche Anfrage

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 des Zertifizierungsdiensteanbieters

Der Zertifizierungsdiensteanbieter a.trust befolgt die Regelungen dieser Zertifizierungsrichtlinie, die sich insbesondere auf die folgenden Aspekte erstreckt:

- Die Zertifikate für Zertifikatsinhaber 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.
- Der Zertifizierungsdiensteanbietes beschäftigt Personal mit angemessener Qualifikation.
- Der Zertifizierungsdiensteanbieter kommt seiner Informationspflicht hinsichtlich Signatoren und Aufsichtsbehörden nach.
- Der Zertifizierungsdiensteanbieter sorgt durch geeignete Maßnahmen (technisch, organisatorisch, infrastrukturell und personell) für den Schutz des privaten Schlüssels der Zertifizierungsstelle.
- Der Einsatz des privaten Schlüssels des Zertifizierungsdienstes erfolgt ausschließlich zum Signieren der Zertifikate der Signatoren und zum Signieren der Widerrufsinformationen.

  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.
- Der Zertifizierungsdiensteanbieter veröffentlicht alle ausgestellten Zertifikate sowie Widerrufslisten.

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 Authentifikationsmechanismen sicher, die in dieser Zertifizierungsrichtlinie beschrieben sind.
- Die Registrierungsstellen beschäftigen Personal mit angemessener Qualifikation.
- Die Registrierungsstellen übermitteln die a.sign SSL (EV) Zertifikate in elektronischer Form an den Signator. a.trust stellt dem Signator insbesondere folgende Dokumente elektronisch zur Verfügung:
  - Vertragsbedingungen,
  - Entgeltbestimmungen sowie
  - Certificate Policy, Certification Practice Statement.

2.1.3 Verpflichtungen der Signatoren

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

- Die Signatoren verpflichten sich, die Allgemeinen Geschäftsbedingungen zusammen mit der Certificate Policy für a.sign SSL und a.sign SSL EV, der gegenständlichen Zertifizierungsrichtlinie und den Entgeltbestimmungen von a.trust als Grundlage für den abgeschlossenen Vertrag anzuerkennen.
- Der Signator ist für die Richtigkeit der Angaben verantwortlich, die er bei der Registrierung macht und wirkt gemäß den in dieser Zertifizierungsrichtlinie angegebenen Verfahren zur Identitätsfeststellung und Authentifizierung mit.
- Der Signator ist verpflichtet, seinen privaten Schlüssel angemessen zu schützen. Dies umfasst insbesondere eine verschlüsselte Speicherung die keinen Zugriff durch unautorisierte Personen auf den privaten Schlüssel zulässt und, wenn es Aktivierungsdaten (PIN) des privaten Schlüssels gibt, die Nichtweitergabe dieser.
- Falls nötig, initiiert der Signator unverzüglich den Widerruf seines Zertifikats.
- Der Signator setzt sein Zertifikat nur zu dem im Zertifikat angegebenen Zweck ein (siehe hiezu Kapitel 7.1.3). Maßgeblich hierfür sind stets die zum Zeitpunkt der Ausstellung des Zertifikats gültige Zertifizierungsrichtlinie und die zugehörige Policy.
- Der Signator ist verpflichtet, die jeweiligen nationalen Ausfuhrbestimmungen sowie etwaige nationale Nutzungsbeschränkungen bei einer Verwendung des privaten Schlüssels im Ausland zu beachten.

2.1.4 Verpflichtungen der Zertifikatsnutzer

Die Zertifikatsnutzer von a.sign SSL und a.sign SSL EV Zertifikaten verpflichten sich, vor der Akzeptanz folgende Prüfungen durchzuführen:

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

2.1.5 Verpflichtungen der Verzeichnisdienste

Der Verzeichnisdienst veröffentlicht in regelmäßigen Abständen

- ausgestellte Zertifikate und
- 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

- 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,
- sie 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.

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 Signator 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 Signator 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 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 Abrufen von Zertifikaten

Der Abruf von a.sign SSL und a.sign SSL EV Zertifikaten über den Verzeichnisdienst ist kostenfrei.

2.5.2 Widerruf von Zertifikaten

Der Widerruf eines Zertifikats ist kostenfrei.

2.5.3 Abrufen von Statusinformationen

Der Zugang zu Widerrufslisten und Statusinformationen ist gebührenfrei.

2.5.4 Richtlinien für Gebührenrückerstattung

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

2.6 Bekanntmachung und Verzeichnisdienste

2.6.1 a.trust Stammzertifikat

Das aktuelle a.trust Stammzertifikat ist unter

- https://www.a-trust.at/certs/A-Trust-nQual-nn.crt
- ldap://ldap.a-trust.at/ou=A-Trust-nQual-nn,o=A-Trust,c=AT

zu finden. Ältere Versionen des Stammzertifikats sind lediglich über das LDAP Verzeichnis abrufbar.

Erläuterung: -nn ist die Versionsnummer der Root-CA welche bei Generierung eines neuen Schlüssels und Veränderung des Distinguished Name erhöht wird.

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

2.6.2 a.trust CA-Zertifikat

Das benötigte CA-Zertifikat für a.sign SSL bzw. a.sign SSL EV Zertifikate ist unter

- https://www.a-trust.at/certs/a-sign-SSL-nn.crt
- https://www.a-trust.at/certs/a-sign-SSL-EV-nn.crt

zu finden (die Bedeutung von -nn ist in Abschnitt 2.6.1 beschrieben) und kann von hier heruntergeladen werden.

2.6.3 Widerrufsinformationen

Verteilungspunkte für die Zertifikatswiderrufslisten (CRLs) für a.sign SSL (EV) Zertifikate:

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

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

2.6.4 Veröffentlichung von Informationen der Zertifizierungsstelle

Der Zertifizierungsdiensteanbieter 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 https://www.a-trust.at/. Die Signatoren 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
- optional: in einem elektronischen Newsletter per E-Mail
- optional: Briefsendung
- optional: Printmedien oder TV

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

2.6.5 Frequenz der Aktualisierung

Eine Aktualisierung der Zertifizierungsrichtlinie erfolgt gemäß Kapitel 8.

2.6.6 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.

2.7 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.

A.sign SSL EV Zertifikate unterliegen einem monatlichen Audit. Hierbei werden 3% der seit dem letzten Audit ausgestellten Zertifikate auf die korrekte Durchführung aller Schritte im Zuge der Ausstellung überprüft. Diese Maßnahme wird protokolliert.

2.7.2 Identität bzw. Anforderungen an den Auditor

Interne Audits werden im Rahmen der Revision durchgeführt.

Audits gemäß [EV-GL] werden durch einen externen Auditor in den vorgeschriebenen Intervallen 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, das die folgenden Konsequenzen nach sich zieht:

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

2.7.6 Bekanntgabe der Ergebnisse

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 Signator bekannt gegebenen Daten vertraulich im Sinne des Datenschutzgesetzes zu behandeln. Die Daten, die bei der Anmeldung angegeben werden, werden ausschließlich für die Dienstleistungen der Zertifizierungsstelle benutzt.

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 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 vertraulichen Daten des Signators 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 und
- Öffentliche Schlüssel des Zertifizierungsdiensteanbieters.

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

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

3 Identifizierung und Authentifikation

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. Bei a.sign SSL EV Zertifikaten richtet sich das Zertifikatsprofil nach [EV-GL] Abschnitt 8.1. Es sind folgende Daten aufzunehmen:

- Name für das Zertifikat (Common Name):
  Der Domainname oder IP-Adresse (bei a.sign SSL EV nicht zulässig), für den das Serverzertifikat beantragt wird.
- Name der Organisation (vollständiger Name z. B. lt. Firmenbucheintrag oder Abkürzung), falls der Domaininhaber eine Organisation ist (bei a.sign SSL EV zwingend notwendig). Der DN (Distinguished Name) muss eindeutig und immer demselben Signator zugewiesen sein.
- Nationalität des Domaininhabers bzw. Land des Sitzes der Organisation
- Name der Organisationsuntereinheit (Abteilung etc.): optional
- E-Mailadresse: optional
  unabhängig davon muss für die Zustellung des Zertifikats jedenfalls eine E Mailadresse angegeben werden.
- im Falle von a.sign SSL EV: zusätzlich notwendige Felder laut [EV-GL] (Business Category, Jurisdiction of Incorporation or Registration, Firmenbuchnummer, physikalische Adresse des Antragssteller)

3.1.2 Regeln zur Interpretation unterschiedlicher Namensformen

Keine Bestimmungen.

3.1.3 Eindeutigkeit der Namen

Der Name (subject) für ein a.sign SSL bzw. a.sign SSL EV Zertifikat ist je nach Zertifikat durch die Kombination Namen wie Domain, Organisation, Abteilungsname, E Mailadresse, CIN eindeutig gestaltet.

3.1.4 Anspruch auf Namen und Beilegung von Streitigkeiten

Keine Bestimmungen.

3.1.5 Anerkennung, Bestätigung und Bedeutung von Warenzeichen

Der Zertifikatsnehmer haftet für etwaige Copyright - Verletzungen.

3.1.6 Methode zum Beweis des Besitzes des geheimen Schlüssels

Der Signator generiert das Schlüsselpaar mit einer geeigneten Software, einem Hardware Device wie Smartcard oder Hardware Security Modul in einem Arbeitsschritt zusammen mit der Erstellung des Zertifikatsrequests, welcher im Anschluss an a.trust gesandt wird. Somit ist gesichert, dass der zum zertifizierten öffentlichen Schlüssel gehörige private Schlüssel sich unter der alleinigen Kontrolle des Signators befindet.

3.1.7 Authentisierung von Organisationen

Für die Bestellung eines a.sign SSL (EV)) Zertifikats für eine Domain welche einer Organisation gehört, muss die zum Signator gehörige Organisation überprüft werden. Wenn die Organisation 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. Eine Ausstellung von a.sign SSL EV Zertifikaten ist derzeit nur für Organisationen möglich, deren Sitz sich im EU - Raum befindet. Die Firmenbuch- bzw. EBR-Nummer muss in diesem Fall bei der Antragstellung angegeben werden. Die phyikalische Adresse der Organisation wird ebenfalls mittels Firmenbuch überprüft. Wenn der Antragsteller kein registriertes Unternehmen ist, dann erfolgt die Überprüfung mittels Vorlage einer Kopie eines Dokumentes, aus welchem hervorgeht, dass die Organisation tatsächlich existiert. Dies 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.

Sämtliche Kommunikation mit den betroffenen Stellen (Antragsteller, zeichnungspberechtigte Person im betroffenen Unternehmen, vertrauenswürdige Dritte) wird über E-Mail, Fax und Telefon abgewickelt.

Die Überprüfung der hier erhobenen Daten erfolgt auf Basis der Vorgaben aus [EV-GL] Abschnitt 10.

Im Falle der Bestellung eines a.sign SSL EV Zertifikats sind weitere Informationen zu erbringen bzw. durch A-Trust einzuholen:

- eine von der Bank der Organisation ausgestellte Bestätigung über die Existenz des Kontos der Organisation
- ein von einem unabhängigen Wirtschaftsprüfer bestätigter Jahresabschluss
- Überprüfung, ob gegen den Antragsteller ein Embargo vorliegt (Anfrage durch A-Trust bei zuständiger Stelle im Land des Antragsstellers)
- Überprüfung der physikalischen Adresse der Organisation. Sofern die Adresse aus dem Firmenbuch bzw. EBR und die Adresse im Zertifikatsantrag übereinstimmen, so ist die Erwähnung der selben Adresse in einem Rechtsgutachten bzw. dem zertifizierten Jahresabschluß ausreichend. Sollten diese Bedingungen nicht zutreffen, so ist eine Überprüfung nur durch die persönliche Begutachtung durch den ausstellenden Registration Officer möglich. Genaue Gesichtspunkte der Begutachtung sind unter [EV-GL] Abschnitt 10.4.1 zu finden. Die Kosten der Vor-Ort Überprüfung sind vom Antragsteller zu tragen.

Ist eine vollständige Einholung aller für die Ausstellung notwendiger Informationen nicht in einer angemessenen Zeit möglich, so wird der Antrag auf Ausstellung eines a.sign SSL EV Zertifikates abgelehnt und der Antragssteller von diesem Umstand in Kenntnis gesetzt.

3.1.8 Überprüfung von Domain oder IP Adresse

Über die Rechtmäßigkeit der Verwendung einer Domain informiert sich die Registrierungsstelle durch Abfrage der Datenbank der zuständigen Registrierungsorganisation (z. B. www.nic.at, www.denic.de, etc.). Ist das nicht möglich, so muss der Besitzer der Domain eine schriftliche Bestätigung ausstellen, aus der hervor geht, dass der Zertifikatsantrag für die Domain rechtmäßig gestellt wird. Wird ein Serverzertifikat nicht für eine Domain, sondern eine IP-Adresse ausgestellt, so muss eine Bestätigung des Providers eingeholt werden, aus der hervorgeht, dass dem Antragsteller die entsprechende IP-Adresse zugewiesen wurde.

Im Falle von EV-Zertifikaten ist die Verwendung einer IP Adresse nicht zulässig.

Im Zuge der Ausstellung kann A-Trust eine Bestätigung über den administrativen Kontakt einholen, aus der hervorgeht, dass sich der Antragsteller der ausschließlichen Kontrolle über den Domain-Namen bewusst ist. Diese Bestätigung kann telefonisch oder per E-Mail eingeholt werden.

3.1.9 Authentisierung von Individuen

Die Personen, die für den Antrag auf ein a.sign SSL bzw. a.sign SSL EV Zertifikat überprüft werden, sind

- der Signator, das ist der Domaininhaber

und, falls der Domaininhaber im Auftrag einer Organisation handelt,

- ein organisatorisch Verantwortlicher, der über eine Zeichnungsberechtigung verfügt und die Rechtmäßigkeit des Zertifikatsantrags bestätigt.

Von den im Antrag genannten Personen muss eine Kopie eines gültigen, amtlichen Lichtbildausweises an a.trust übermittelt werden. Dabei sind die folgenden Ausweise zulässig:

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

Wenn der organisatorisch Verantwortliche nicht im Firmenbuch oder EBR aufscheint, dann muss zusätzlich einen Nachweis über die Zeichnungsberechtigung (z. B. eine Vollmacht) an a.trust übermittelt werden.

3.2 Erneute Registrierung/Rezertifizierung

Der Signator wird vor Ablauf der Gültigkeitsdauer eines a.sign SSL (EV) Zertifikats kontaktiert und gebeten, einen neuen PKCS#10-Request an die Registrierungsstelle zu senden. Ob ein neuer Schlüssel generiert wird, bleibt dem Signator selbst überlassen, allerdings empfiehlt a.trust, die Möglichkeit des Schlüsselwechsels zu nützen.

Die bei einer Erstausstellung durchgeführten Prüfungen auf Rechtmäßigkeit des Antrags werden erneut durchgeführt.

3.3 Erneute Registrierung nach Widerruf

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

3.4 Widerrufsantrag bzw. Sperre

Widerrufe werden entsprechend Abschnitt 4.3 gehandhabt.

4 Betriebliche Anforderungen

4.1 Antrag auf Ausstellung von Zertifikaten

Die Antragstellung erfolgt mittels eines elektronischen Formulars auf der a.trust Homepage.

Die Ausweiskopien und ggf. Bestätigungen sendet der Signator an die Registrierungsstelle.

Wenn in einem a.sign SSL (EV) Zertifikat die Zugehörigkeit zu einer Behörde abgebildet werden soll, so wird von einem autorisierten Behördenvertreter zusätzlich zum Antrag ein Schreiben an die a.trust Registrierungsstelle gesandt, das die Rechtmäßigkeit dieser Angabe bestätigt.

Die Vorgehensweise der Antragstellung auf Ausstellung von a.sign SSL EV Zertifikaten unterliegt den genauen Vorgaben aus [EV-GL] Abschnitt 9. Die Identifikation der im Antrag genannten natürlichen Person muss persönlich, anhand eines amtlichen Lichtbildausweises erfolgen. Kopien des verwendeten Ausweisdokuments werden hinterlegt. Alternativ kann die Identität auch über eine qualifzierte Signatur (basierend auf einem von A-Trust ausgestelltem Zertifikat) festgestellt werden.

Werden durch denselben Antragsteller mehrere a.sign SSL (EV) Zertifikate zur selben Zeit angefordert, so sind die Anträge einzeln einzubringen. Zu diesem Zwecke eingeholte Dokumente werden für alle eingegangenen Anträge des Antragstellers herangezogen, sofern die Bestellungen zur selben Zeit durchgeführt wurden.

4.2 Veröffentlichung und Akzeptanz von Zertifikaten

Das fertig gestellte Zertifikat kann dem Signator elektronisch auf zwei Arten zur Verfügung gestellt werden:

- Es wird per E-Mail zugesandt.
- Es gibt eine Suchfunktion auf der a.trust Website (der URL wird dem Signator per Mail zugesandt), bei welcher der Common Name einzugeben ist. Das Ergebnis der Suche ist der Link zum Download des entsprechenden Zertifikats.

4.3 Widerruf und Sperre von Zertifikaten

Für alle Arten von a.sign SSL Zertifikaten ist ein sofortiger und permanenter Widerruf oder eine temporäre Sperre des Zertifikats möglich.

Der Abruf der Widerrufsliste ist per Verzeichnisdienst (LDAP) sowie per OCSP jederzeit möglich; die Verfügbarkeit wird durch eine redundante Auslegung der Rechenzentren

sowie entsprechenden Verträgen mit deren Betreiber gewährleistet.

4.3.1 Gründe für einen Widerruf

Der Widerruf eines Zertifikats wird erforderlich, wenn

- wesentliche Angaben im Zertifikat nicht mehr korrekt sind,
- der private Schlüssel zu einem a.sign SSL bzw. a.sign SSL EV Zertifikat nicht mehr verwendet werden kann (z. B. das Speichermedium ist defekt und keine Sicherungskopie verfügbar),
- Verdacht auf eine Kompromittierung besteht (wenn z. B. ein Unbefugter Zugriff auf den Rechner, auf dem sich der private Schlüssel befindet, hatte) bzw. eine Kompromittierung vorliegt,
- der Zertifizierungsstelle ein wesentlicher Verstoß des Signators gegen diese Richtlinien oder die Allgemeinen Geschäftsbedingungen bekannt wird,
- das Vertragsverhältnis beendet wird,
- die Person des Signators sich ändert,
- die eingesetzten Algorithmen nicht mehr den Sicherheitserwartungen entsprechen.
- Einstellung der Tätigkeit durch den Zertifizierungsdiensteanbieter

Für a.sign SSL EV Zertifikate gelten die Vorgaben aus [EV-GL] 11.2.2.

4.3.2 Wer kann einen Widerruf anordnen

Ein Widerruf eines Zertifikates kann angeordnet werden durch:

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

4.3.3 Prozedur für einen Widerrufsantrag

Der Widerruf eines a.sign SSL (EV) Zertifikats erfolgt mit einem Telefonanruf oder per Fax beim für die a.sign SSL (EV) Zertifikate zuständigen Widerrufsdienst. Die aktuellen Telefonnummern des Widerrufsdienstes sind der Homepage (http://www.a-trust.at/widerruf) zu entnehmen. Der Widerrufsdienst ist 7 Tage die Woche rund um die Uhr erreichbar und steht bei dringenden Anfragen zu jeder Zeit in direktem Kontakt mit einer A-Trust Bereitschaft-Hotline.

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 Schlüssel, 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
- Domainname oder Zertifikatsnummer: obligatorisch

Wenn beim Widerruf eines a.sign SSL oder a.sign SSL EV Zertifikats das Passwort nicht genannt werden kann, so kann der Widerruf per Einschreiben (mit firmenmäßiger Zeichnung) erfolgen. Alternativ kann nach Identifikation des Signators eine Sperre des Zertifikats ausgelöst werden.

4.3.4 Sperre eines Zertifikates

Für eine Sperre eines Zertifikats gelten, wenn nicht explizit anders angegeben, die selben Bestimmungen wie für einen Widerruf.

Mit der Sperre eines Zertifikats verliert dieses die Gültigkeit und wird in die nächste Sperrliste aufgenommen. Wird eine Sperre nicht aufgehoben so geht diese automatisch in einen Widerruf über, wobei als Widerrufsdatum das Datum der Sperre gilt.

Wird eine Sperre durch Bekanntgabe eines zum Sperrzeitpunkt festgelegten Sperraufhebungspassworts aufgehoben, so behält das Zertifikat seine Gültigkeit. Es ist anzumerken, dass das Zertifikat nach Aufhebung der Sperre auch für den Zeitraum dieser gültig war und somit eine Sperre nur aufgehoben werden darf wenn eine Kompromittierung ausgeschlossen werden kann.

4.3.5 Prozedur für einen Sperrantrag

Eine Sperre eines Zertifikats kann beim Widerrufsdienst nach Bekanntgabe der Domain oder Zertifikatsnummer und erfolgreicher Identifikation des Signators (z.B. durch Nennung des Widerrufspasswortes) erfolgen. Gleichzeitig wird ein Sperraufhebungspasswort festgelegt, welches zur Aufhebung der Sperre berechtigt.

Der Signator wird nach auslösen der Sperre per Email oder Brief verständigt und es wird ihm der Zeitpunkt des endgültigen Widerrufs mitgeteilt. Die Sperre kann nun bis Ende dieser Frist, durch Bekanntgabe des Sperraufhebungspassworts oder andere Identifikation des Signators, beim Widerrufsdienst aufgehoben werden.

4.3.6 Frist bis zur Bekanntgabe des Widerrufs

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

Der Widerrufsdienst für a.sign SSL (EV) Zertifikate ist zu den auf der a.trust Homepage angegebenen Geschäftszeiten erreichbar (http://www.a-trust.at/widerruf).

4.3.7 Aktualisierungsfrequenz der Widerrufsliste

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

Wird ein Widerruf durchgeführt, so wird dieser Eintrag auch nach Ablauf des Zertifikates nicht aus der Widerrufsliste entfernt.

4.3.8 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 einem Schlüssel signiert wurde für den ein gültigen CA-Zertifikat existiert 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.

4.3.9 Möglichkeiten zur online Statusabfrage

Es wird ein OCSP-Dienst unter http://ocsp.a-trust.at/ocsp angeboten, über welchen der Status eines Zertifikates in Echtzeit abgefragt werden kann.

4.3.10 Anforderungen an die Statusabfrage

Ein Zertifikatsnutzer sollte die Authentizität der Auskunft des Verzeichnisdiensts durch die Prüfung der in der Antwort enthaltenen Signatur verifizieren. Des weiteren ist der in der Auskunft enthaltene Zeitpunkt, auf den sich der Status bezieht, mit dem fraglichen Prüfzeitpunkt zu vergleichen.

Sofern keine erfolgreiche Gültigkeitsprüfung vorgenommen werden kann (beispielsweise aus technischen Gründen), sollte das Zertifikat nicht akzeptiert werden. Das Risiko für die Akzeptanz eines solchen Zertifikats trägt jedenfalls der Zertifikatsnutzer.

4.3.11 Weitere Verfahren zur Bekanntgabe von Widerrufen

Keine Bestimmungen.

4.3.12 Anforderungen an die Überprüfung weiterer Verfahren zur Bekanntgabe von Widerrufen

Keine Bestimmungen.

4.3.13 Spezielle Verfahren bei Kompromittierung von privaten Schlüsseln

Wenn bei einem a.sign SSL bzw. a.sign SSL EV Zertifikat der Verdacht auf Kompromittierung besteht, muss der Signator 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 Signator oder auch
- Änderungen an den Daten des Signators.

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:

- Daten des Signators, die zur Zertifizierung verwendet wurden,
- Zertifizierungsanträge,
- Alle von der Zertifizierungsstelle ausgestellten Zertifikate (Zertifikate der Zertifizierungsstelle und Dienste, Cross-Zertifikate 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),
- Datum und Uhrzeit von Schlüsselwechseln der Zertifizierungsstelle und
- Daten zu Verfahrensrichtlinien (CP, CPS).

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.

Für a.sign SSL EV Zertifikate gelten die Vorgaben aus [EV-GL] 13.2.

4.5.3 Schutzvorkehrungen

Das Archiv befindet sich in gesicherten Räumlichkeiten. Der Zugriff ist nur autorisierten Personen gestattet, eine genaue Regelung erfolgt über ein Rollenkonzept.

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 a.trust System zu archivierenden Daten verantwortlich.

4.5.6 Prozeduren zum Abrufen und Überprüfen von Daten

Bei Archivierung von elektronischen Daten über lange Zeiträume ist damit zu rechnen, dass dann veraltete Datenformate nicht mehr von neuen Systemen unterstützt werden. Die Zertifizierungsstelle hält deshalb auch die Systeme verfügbar, mit denen sich diese Daten auch über den Archivierungszeitraum verarbeiten lassen.

Es werden Regelungen getroffen, dass das Archiv auch bei Unterbrechungen oder Einstellung der Tätigkeit der Zertifizierungsstelle über den festgelegten Archivierungszeitraum bestehen bleibt.

4.6 Schlüsselwechsel von CA-Schlüsseln

Ein Schlüsselwechsel von CA- und Root-Schlüsseln kann im Zusammenhang mit dem Ausfall eines Hardware Security Moduls erfolgen bzw. ist auf jeden Fall notwendig, 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 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 könnte, so werden die entsprechenden Komponenten umgehend aus dem Betrieb

genommen.

Bei Zertifikaten sind die betroffenen Signatoren 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, um eine Veröffentlichung unkorrekter Daten zu verhindern. Die Wiederaufnahme des Dienstes ist mit der Veröffentlichung der neuen Widerrufsliste verbunden. In Abhängigkeit der Fehler und der Ausfallzeit der Verzeichnisdienste werden die Anwender informiert.

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

4.7.2 Widerruf von Zertifikaten zu Zertifizierungsstellenschlüsseln

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 4.3.9 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 Signatoren 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 6.2.8 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 widerrufen, so müssen dadurch alle unter diesem Zertifikat ausgestellten Zertifikate widerrufen werden. Der Dienst der Statusauskunft wird bei Anfragen zu allen unter der Zertifizierungsstelle bzw. unter deren Untereinheiten ausgestellten Zertifikaten generell mit einem ungültigen Status antworten.

Signatoren, deren Zertifikate von dem Widerruf betroffen sind, erhalten nach den festgelegten Verfahren (siehe Kapitel 3.2) ein neues Zertifikat. Die Zertifizierung erfolgt dabei mit einem neuen Schlüssel der Zertifizierungsstelle.

4.7.2.3 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 Signatoren über den Schlüsselwechsel ist bei einem unmittelbaren Widerruf nicht möglich. Sie 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.

4.8.1 Versicherungsdeckung

A-Trust GmbH verfügt über eine Versicherungsdeckung gemäß Signaturgesetz:

Zertifizierungsdiensteanbieter müssen über ausreichende Finanzmittel verfügen, um den Anforderungen der Richtlinie entsprechend arbeiten zu können. Sie müssen insbesondere in der Lage sein, das Haftungsrisiko für Schäden zu tragen, zum Beispiel durch Abschluß einer entsprechenden Versicherung.

Die abgeschlossene Versicherung erfüllt mit einem Rating von A weiters die Vorgaben aus [EV-GL].

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 finden Sie auf der Web-Seite der a.trust https://www.a-trust.at/ veröffentlicht.

Tabelle 1: Standorte

5.1.2 Zugangskontrollen

Der Zugang zu allen technischen Komponenten im Rechenzentrum ist nur durch einen von der a.trust eingerichteten Berechtigungsmechanismus möglich.

Die Zugangskontrollen sind dem angestrebten Sicherheitsniveau für einzelne Bereiche, in denen sich sicherheitskritische Komponenten befinden, angepasst.

Der Zutritt in den Hochsicherheitsbereich des Rechenzentrums ist an die Anwesenheit von zwei Personen mit Berechtigungskarten und PIN-Eingabe gebunden. Diese Zutritte werden protokolliert und sind dadurch jederzeit nachvollziehbar. Zusätzlich sind Videoüberwachungssysteme und Einbruchmeldesysteme installiert.

5.1.3 Stromversorgung und Klimaanlage

Die Stromversorgung in den Örtlichkeiten entspricht internationalen Standards und ist - bis auf die Registrierungsstellen überall redundant ausgelegt. Zusätzlich existiert für das Rechenzentrum eine Notstromversorgung.

Die Örtlichkeiten, in denen technische Komponenten der a.trust untergebracht sind, verfügen alle über eine angemessene Klimaanlage.

5.1.4 Wasserschäden

Die Örtlichkeiten, in denen technische Komponenten der a.trust untergebracht sind, verfügen alle über einen angemessenen Schutz vor Wasserschäden.

5.1.5 Feuer

Alle Räumlichkeiten, die technische Komponenten beherbergen, verfügen über eine EDV-geeignete Feuermeldeanlage.

Im Hochsicherheitsbereich des Rechenzentrums richtet sich der Brandschutz nach den dort geltenden Richtlinien für den Hochsicherheitsbetrieb eines Rechenzentrums.

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, soweit technisch möglich, 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 2: Funktionen der a.trust

5.2.2 Sicherheitskritische Funktionen

Rolle	Funktion
Sicherheitsbeauftragter	siehe Tabelle 2
Revision	siehe Tabelle 2
Datenschutz	siehe Tabelle 2
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
Sicherheits-systemadministrator	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 und Sperre
Registration Officer (RO), Mitarbeiter der Registrierungsstelle	Entgegennahme von Zertifikatsanträgen Identifikation von Zertifikatswerbern im Rahmen der Registrierung Belehrung der Zertifikatsinhaber

Tabelle 3: 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 2

Tabelle 4: Sonstige Funktionen

5.2.4 Anzahl erforderlicher Personen für sicherheitsrelevante Tätigkeiten

Tabelle 5 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 für a.sign SSL	RO	Nein	Nein
Registrierung und Identifizierung von Zertifikatswerbern für a.sign SSL EV	RO	Ja (tech-nisch umge-setzt)	Nein
Überprüfung der eingeholten Informationen vor der Ausstellung eines a.sign SSL EV Zertifikates	RO (nicht in Informations-beschaffung involviert)	Nein	Nein
Kontrolle Registrierung und Identifizierung von Zertifikatswerbern bei der Ausstellung von a.sign SSL EV zertifikaten	SO	Nein	Nein
Widerrufen von Anwenderzertifikaten	RCA, RO	Nein	Nein
Erzeugung der Schlüssel für Root-CA und Zertifizierungsstellen sowie Schlüsselwechsel	SO, SO	Ja	Ja
Aktivierung der Schlüssel für Root-CA und Zertifizierungsstellen	SO, SO	Ja	Ja
Löschen der Schlüssel für Root-CA und Zertifizierungsstellen	SO, SO	Ja	Ja
Zertifizierung für die Root-CA und die Zertifizierungsstellen	SO, SO	Ja	Ja
Widerruf von Zertifikaten der CA	SO, SO	Ja	Ja
Vergabe der Berechtigungen für RO und RCA	SO, SO	Ja	Ja
Inbetriebnahme eines kryptographischen Moduls (Signaturerstellungseinheit der CA)	SO, SO	Ja	Ja

Tätigkeit	Personen	Vier-augen-prinzip	Hoch-sicher-heit
Ab- und Anschalten von Komponenten, insbesondere Verzeichnisdiensten	Sicherheits-systemadministrator	Nein	Nein
Austausch von Hardware-Komponenten	Sicherheits-systemadministrator (2x)	Ja	Ja
Austausch von Software-Komponenten	Sicherheits-systemadministrator (2x)	Ja	Ja
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	Sicherheits-systemadministrator (2x)	Ja	Ja
Qualitätsprüfung der verwendeten Schlüssellängen und Parameter zur Schlüsselerzeugung	SO	Nein	Nein
Wartung oder Austausch eines kryptographischen Moduls	SO, SO	Ja	Ja

Tabelle 5: 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.

5.2.6 Risikoanalyse

Im Zuge der Einführung von Prozessen zur Zertifikatsausstellung werden Risikoanalysen der einzelnen Teilbereiche durchgeführt.

A-Trust führt ein jährliches Review der Risikoanalysen durch und prüft hierbei, ob Risiken und mögliche Folgen sowie die Gegenmaßnahmen einer Veränderung unterlegen 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 zur Signatur von a.sign SSL und a.sign SSL EV Zertifikaten werden in einem Hardware Security Modul der Zertifizierungsstelle generiert. Für die geheimen Schlüssel der Zertifizierungsstelle erfolgt ein Export bzw. Backup nur auf ein anderes Security Modul, das aus Gründen der Ausfallsicherheit bereit steht.

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 werden von den Zertifikatsinhabern in Software oder einem Hardware Security Modul, unter Verwendung von Verfahren die eine hinreichende Zufallsqualität gewährleisten, erzeugt.

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

6.1.2 Auslieferung privater Schlüssel an Zertifikatsinhaber

Eine Auslieferung privater Schlüssel wird nicht durchgeführt, da nur der Signator die Kontrolle über den privaten Schlüssel hat 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 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 a.sign SSL (EV) Zertifikats

Das Schlüsselpaar wird vom Signator selbst generiert und er ist daher im Besitz des öffentlichen Schlüssels.

6.1.4 Schlüssellängen

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

Der von a.trust zur Erstellung der Signatur über die Zertifikate verwendete Hash-Algorithmus ist SHA-1 oder ein kryptographisch sichereres Verfahren.

Die Signatoren müssen für a.sign SSL als Schlüssellänge mindestens 1024 Bit (RSA-Schlüssel) wählen. Für a.sign SSL EV Zertifikate ist laut [EV-GL] eine Schlüssellänge von mindestens 2048 Bit (RSA) notwendig.

Nähere Informationen zur Mindestanforderung an die zu verwendenden kryptographischen Verfahren bei a.sign SSL EV Zertifikaten siehe [EV-GL] Appendix A.

Bei a.sign SSL (EV) Zertifikaten ist als Hash-Algorithmus SHA-1 oder ein kryptographisch sichereres Verfahren zu verwenden.

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

6.1.5 Parameter zur Schlüsselerzeugung

Die Erzeugung des Schlüssels der Zertifizierungsstelle erfolgt unter Einsatz eines physikalischen Zufallszahlengenerators, der auf einer physikalischen Rauschquelle basiert und das Primärrauschen kryptographisch nachbehandelt.

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 für a.sign SSL und a.sign SSL EV Zertifikate werden in einer speziellen Hardware erzeugt und dort auch eingesetzt.

Die Schlüssel der a.sign SSL (EV) Zertifikate werden vom Signator mittels Software oder geeigneter Hardware-Einheiten erzeugt (Vorgangsweise siehe in Kapitel 6.1.1). Weder die Zertifizierungs- noch die Registrierungsstelle erhalten Kenntnis vom privaten Schlüssel des Signators.

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).

6.1.8.1 Verwendung der Schlüssel der Root-CA

Die Root-CA besitzt ein selbst signiertes Zertifikat, in welchem im Attribut 'keyUsage' die Bits

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

gesetzt sind.

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

Bei dem zu einem Zertifikat für SSL-Authentifizierung gehörigen Schlüssel eines a.sign SSL und a.sign SSL EV Zertifikats dient zur Verschlüsselung, weshalb in diesem Fall im Zertifikat die folgenden Bits gesetzt sind:

- digitalSignature
- keyEncipherment.

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 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 für a.sign SSL bzw. a.sign SSL EV Zertifikate 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 befinden sich entweder in einem Hardware Security Modul oder auf der Festplatte des Servers des Zertifikatsinhabers und werden gegen unberechtigte Nutzung abgesichert.

6.2.3 Hinterlegung privater Schlüssel

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

6.2.4 Backup privater Schlüssel

Private Schlüssel der Root-CA und der Zertifizierungsstellen für a.sign SSL und a.sign SSL EV werden aus Gründen der Ausfallsicherheit in ein weiteres Hardware Security Modul eingebracht.

6.2.5 Archivierung privater Schlüssel

Für private Schlüssel der Zertifizierungsstelle gibt es keine Archivierung.

6.2.6 Einbringung privater Schlüssel in das kryptographische Modul

Die eingesetzte kryptografische Hardware ist so beschaffen, dass die privaten Schlüssel nur innerhalb dieses Mediums generiert werden. Eine Einbringung von bereits generierten Schlüsseln ist nur mittels Import von einem anderen Hardware Security Modul möglich, um die Ausfallsicherheit zu gewährleisten. Die Anwendung der privaten Schlüssel erfolgt ebenfalls direkt im Hardware Security Modul.

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

6.2.7 Methode zur Deaktivierung privater Schlüssel

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

6.2.8 Methode zur Vernichtung privater Schlüssel

Private Schlüssel der Zertifizierungsstelle werden, sofern notwendig, durch eine Funktion des Hardware Security Moduls sicher gelöscht.

Für die Löschung der geheimen Schlüssel zu a.sign SSL (EV) Zertifikaten sind die Signatoren 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 Gültigkeitsdauern (Jahre):

Zertifikatstyp	Gültigkeitsdauer
Root-CA	10
Zertifizierungsstellen	10
a.sign SSL	3,25
a.sign SSL EV	2,25

Tabelle 6: Gültigkeitsdauer von Zertifikaten

6.4 Aktivierungsdaten

6.4.1 Erzeugung und Installation der Aktivierungsdaten (PINs) für Schlüssel der Zertifizierungsstelle

Die Schlüssel der Root-CA und der Zertifizierungsstellen für a.sign SSL und a.sign SSL EV Zertifikate können ausschließlich im Vieraugen-Prinzip durch zwei Security Officer 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.

6.4.2 Schutz der Aktivierungsdaten

6.4.2.1 Aktivierungsdaten für Schlüssel der Zertifizierungsstelle

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

6.4.2.2 Aktivierungsdaten für Schlüssel der Signatoren

Die Signatoren sind verpflichtet, sofern sie über Aktivierungsdaten für den geheimen Schlüssel (PIN) verfügen, diese nicht weiterzugeben und nicht an für unberechtigte 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-Zertifikate

Attribut	**Inhalt**	**Erläuterung**
Version	v3(2)	Die Versionsnummer wird auf '2' gesetzt, um ein X.509 Zertifikat der Version 3 anzuzeigen
Seriennummer	Seriennummer des Zertifikats	Eindeutig innerhalb der a.trust Zertifizierungsinfrastruktur
Algorithmus	≥ SHA-1	Für die Signatur über das Zertifikat verwendeter Algorithmus
Aussteller des Zertifikats	CN = CommonName OU = OrganizationalUnit O = Organization C = AT	CommonName, OrganizationalUnit: A-Trust-nQual-nn Organization: A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH
Gültig von Gültig bis	Beginn und Ende der Gültigkeit des Zertifikats	Der Gültigkeitszeitraum beträgt höchstens zehn Jahre
Zertifikatsinhaber	CN = CommonName OU = OrganizationalUnit O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH C = AT	CommonName, OrganizationalUnit: a-sign-SSL-nn bzw. a-sign-SSl-EV-nn -nn bezeichnet die Generation der CA
Öffentlicher Schlüssel	≥ RSA 2048 Bit	Öffentlicher Schlüssel des Zertifikatsinhabers (der CA)

Tabelle 7: Profil für CA-Zertifikat

7.1.2 Zertifikate der Signatoren

Attribut	Inhalt	Erläuterung
Version	v3(2)	Die Versionsnummer wird auf '2' gesetzt, um ein X.509 Zertifikat der Version 3 anzuzeigen
Seriennummer	Seriennummer des Zertifikats	Eindeutig innerhalb der a.trust Zertifizierungsinfrastruktur
Algorithmus	≥ SHA-1	Für die Signatur über das Zertifikat verwendeter Algorithmus
Aussteller des Zertifikats	CN = CommonName OU = OrganizationalUnit O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH C = AT	CommonName, OrganizationalUnit: a-sign-SSL-nn -nn bezeichnet die Generation der CA.
Gültig von Gültig bis	Beginn und Ende der Gültigkeit des Zertifikats	Der Gültigkeitszeitraum beträgt höchstens 39 Monate
Zertifikatsinhaber (subject)	C = CountryName CN = CommonName O = Organization OU = OrganizationalUnit E = E-Mailadresse Seriennummer = SerialNumber	CountryName: AT, DE etc. CommonName: Name der Domain oder IP-Adresse Organization: Name der Organisation (lt. Eintragung im Firmenbuch oder Abkürzung) OrganizationalUnit: Abteilung etc., optional E-Mailadresse: optional SerialNumber: eindeutige Identifikationsnummer des Signators (CIN)
Öffentlicher Schlüssel	≥ RSA 1024 Bit	Öffentlicher Schlüssel des Signators

Tabelle 8: Profil für a.sign SSL

7.1.3 Erweiterungen (certificate extensions)

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

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

Auf die Erweiterung keyusage wird in Abschnitt 6.1.8 näher eingegangen.

Optional können a.sign SSL Zertifikate eine Zertifikatserweiterung enthalten, welche den Signator als Mitarbeiter einer Behörde ausweist (Behördenkennzeichen - OID 1.2.40.0.10.1.1.1). In dieser Erweiterung kann weiters optional auch ein Verwaltungsbezeichner enthalten

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 = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH C = AT	CommonName, OrganizationalUnit: a-sign-SSL-EV-nn -nn bezeichnet die Generation der CA.
Gültig von Gültig bis	Beginn und Ende der Gültigkeit des Zertifikats	Der Gültigkeitszeitraum beträgt höchstens 27 Monate
Zertifikatsinhaber (subject)	C = CountryName CN = CommonName O = Organization OU = OrganizationalUnit E = E-Mailadresse Seriennummer = SerialNumber	CountryName: AT, DE etc. CommonName: Name der Domain oder IP-Adresse Organization: Name der Organisation (lt. Eintragung im Firmenbuch oder Abkürzung) OrganizationalUnit: Abteilung etc., optional E-Mailadresse: optional SerialNumber: eindeutige Identifikationsnummer des Signators (CIN)
Öffentlicher Schlüssel	≥ RSA 1024 Bit	Öffentlicher Schlüssel des Signators
BusinessCategory	OID	gemäß [EV-GL] Abschnitt 8
Jurisdiction of Incorporation Locality	OID	Gerichtsstand der Organisation (vgl. [EV-GL] Abschnitt 8)
Registration Number	OID	zB. Firmenbuchnummer [EV-GL] Abschnitt 8
physikalische Adresse der Organisation	OID	[EV-GL] Abschnitt 8

Tabelle 9: Profil für a.sign SSL EV

sein, der die Zugehörigkeit zu einer Organisationseinheit der öffentlichen Verwaltung angibt.

Erweiterung	Zertifikatstyp		Klassifikation	
	Root	CA	kritisch	nicht kritisch
Standarderweiterungen				
authorityKeyIdentifier	Nein	Ja		X
subjectKeyIdentifier	Ja	Ja		X
keyUsage	Ja	Ja	X	
subjectAltName	Optional	Optional		X
basicConstraints	Ja	Ja	X	
CRLDistributionPoints	Nein	Ja		X
Private Extensions				
authorityInfoAccess	Nein	Ja		X

Tabelle 10: Erweiterungen (CA-Zertifikate)

Erweiterung	Im Zertifikat vorhanden	Klassifikation	
		kritisch	nicht kritisch
Standarderweiterungen			
authorityKeyIdentifier	Ja		X
subjectKeyIdentifier	Ja		X
keyUsage	Ja	X	
certificatePolicies	Ja		X
basicConstraints	Ja		X
cRLDistributionPoints	Ja		X
subjectAltName	optional		X
Private Extensions			
authorityInfoAccess	Ja		X
1.2.40.0.10.1.1.1	optional		X
1.2.40.0.10.1.1.2	optional		X
1.3.36.8.3.4	optional		X

Tabelle 11: Erweiterungen (a.sign SSL bzw. a.sign SSL EV Zertifikat)

Weiters können a.sign SSL Zertifikate optional eine Zertifikatserweiterung enthalten, welche ein Zertifikat als einer Organisation zugehörig ausweist, die im Auftrag einer öffentlichen Verwaltungsorganisation tätig ist (Dienstleistereigenschaft - OID 1.2.40.0.10.1.1.2).

Die in Abschnitt 2.2.1 beschriebene Haftungsobergrenze ist optional in a.sign SSL Zertifikaten enthalten und unter der OID 1.3.36.8.3.4 im Zertifikat ausgewiesen.

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 Signatoren. Dies sind insbesondere Änderungen, die

- Verpflichtungen, Haftung, finanzielle Verantwortung,
- Registrierung,
- Personalisierung,
- Internetadressen und Kontaktinformationen,
- Schlüssel- und Zertifikatsmanagement,
- Verzeichnis- und Widerrufsdienst 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 die aktuelle Zertifizierungsrichtlinie und Certificate Policy sowie auch weiterhin alte Versionen abgerufen werden.

8.3 Genehmigung und Eignung einer Zertifizierungsrichtlinie

Diese Zertifizierungsrichtlinie gilt für die Produkte a.sign SSL. a.trust stellt sicher, dass diese Zertifizierungsrichtlinie für die betroffenen Certificate Policies geeignet ist.

A Anhang

A.1 Begriffe und Abkürzungen

Aktivierungsdaten	Daten, die zur Aktivierung der Schlüssel benötigt werden (siehe auch PIN).
Anwender	Person, die die Dienstleistungen der Zertifizierungsstelle der a.trust nutzt. Anwender sind sowohl Signatoren als auch Zertifikatsnutzer.
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 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 Zertifizierungshierachie 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	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 generiert die Schlüssel der Anwender und stellt in Zertifikaten die Zuordnung von Anwendern zu Schlüsseln sicher. Zusätzlich übernimmt sie noch weitere Dienstleistungen, wie z. B. das Veröffentlichen von Zertifikaten oder Widerrufslisten.

A.2 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

EV-GL Guidelines For The Issuance And Management Of Extended Validation Certificates (aktuelle Version: http://www.cabforum.org)

A.3 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 und BGBl. II Nr. 527/2004 vom 30.12.2004

[SigRL] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, 13. 12. 1999

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

[EV-GL] Guidelines For The Issuance And Management of Extended Validation Certificates 1.2, 2009