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 cyberDOC

Version: 1.0.1

Datum: 21.06.2004

Inhaltsverzeichnis

1 Einleitung 12
1.1 Überblick 12
1.2 Dokumentidentifikation 12
1.3 Zertifizierungsinfrastruktur und Anwendbarkeit 12
1.3.1 Zertifizierungsstellen 12
1.3.2 Registrierungsstellen 13
1.3.3 Widerrufsdienst 13
1.3.4 Anwender 13
1.3.5 Anwendbarkeit 13
1.3.6 Zertifizierungshierarchie 14
1.3.7 a.trust Verzeichnisbaum 15
1.4 Ansprechpartner und Kontaktstellen 15
1.4.1 Organisation zur Verwaltung dieses Dokuments 15
1.4.2 Kontaktinformation 16
1.4.3 Verantwortlicher für die Anerkennung anderer Policies 16
2 Generelle Bestimmungen 17
2.1 Verpflichtungen 17
2.1.1 Verpflichtungen der Zertifizierungsstellen 17
2.1.2 Verpflichtungen der Registrierungsstellen 17
2.1.3 Verpflichtungen der Zertifikatsinhaber 18
2.1.4 Verpflichtungen der Zertifikatsnutzer 19
2.1.5 Verpflichtungen der Verzeichnisdienste 19
2.2 Haftung 19

2.2.1 Haftung der Zertifizierungsstelle 20
2.2.2 Haftung der Registrierungsstelle 20
2.3 Finanzielle Verantwortung 20
2.3.1 Schadensersatz der beteiligten Parteien 20
2.3.2 Treuhänderische Beziehungen 21
2.3.3 Administrative Prozesse 21
2.4 Auslegung und (gerichtliche) Durchsetzung 21
2.4.1 Zugrunde liegende Gesetzesbestimmungen 21
2.4.2 Trennbarkeit der Bestimmungen, Fortbestehen von Ansprüchen, Fusion, Kündigung 21
2.4.3 Schlichtungsverfahren 21
2.5 Gebühren 22
2.5.1 Ausgabe und Erneuerung von Zertifikaten 22
2.5.2 Abrufen von Zertifikaten 22
2.5.3 Sperre oder Widerruf von Zertifikaten 22
2.5.4 Abrufen von Statusinformationen 22
2.5.5 Richtlinien für Gebührenrückerstattung 22
2.6 Bekanntmachung und Verzeichnisdienste 23
2.6.1 Web-Seiten und Verzeichnisse 23
2.6.2 a.trust Stammzertifikat 23
2.6.3 a.trust CA-Zertifikat 23
2.6.4 Widerrufsinformationen 24
2.6.5 Suche nach einem Zertifikat 24
2.6.6 Veröffentlichung von Informationen der Zertifizierungsstelle 24
2.6.7 Frequenz der Aktualisierung 25

2.6.8 Zugriffskontrollen 25
2.6.9 Verzeichnisse 26
2.7 Interne Prüfung (Audit) 26
2.7.1 Häufigkeit des Audits 26
2.7.2 Identität bzw. Anforderungen an den Auditor 26
2.7.3 Beziehungen zwischen Auditor und zu untersuchender Partei 26
2.7.4 Aspekte des Audits 27
2.7.5 Handlungen nach unzureichendem Ergebnis 27
2.7.6 Bekanntgabe der Ergebnisse 27
2.8 Vertraulichkeit 27
2.8.1 Vertraulich eingestufte Informationen 27
2.8.2 Nicht vertraulich eingestufte Informationen 28
2.8.3 Offenlegung von Informationen zu Zertifikatssperren bzw. -widerruf 28
2.8.4 Offenbarung an Behörden im Rahmen gesetzlicher Pflichten 28
2.8.5 Offenbarung im Rahmen zivilrechtlicher Auskunftspflichten 28
2.8.6 Weitere Gründe zur Freigabe von vertraulichen Informationen 28
2.9 Urheberrechte und Eigentumsrechte 28
3 Identifizierung und Authentisierung 30
3.1 Erstregistrierung 30
3.1.1 Namenstypen 30
3.1.2 Anforderungen an die Namen 30
3.1.3 Regeln zur Interpretation unterschiedlicher Namensformen 31
3.1.4 Eindeutigkeit der Namen 31
3.1.5 Anspruch auf Namen und Beilegung von Streitigkeiten 31
3.1.6 Anerkennung, Bestätigung und Bedeutung von Warenzeichen 31

3.1.7 Methode zum Beweis des Besitzes des geheimen Schlüssels 31
3.1.8 Authentisierung von Individuen 31
3.2 Erneute Registrierung/Rezertifizierung 32
3.3 Erneute Registrierung nach Widerruf 32
3.4 Sperr- und Widerrufsantrag 32
4 Betriebliche Anforderungen 34
4.1 Antrag auf Ausstellung von Zertifikaten 34
4.2 Herausgabe und Akzeptanz von Zertifikaten 34
4.3 Sperre und Widerruf von Zertifikaten 35
4.3.1 Gründe für einen Widerruf 35
4.3.2 Wer kann einen Widerruf anordnen 35
4.3.3 Prozedur für einen Widerrufsantrag 36
4.3.4 Frist bis zur Bekanntgabe des Widerrufs 36
4.3.5 Gründe für eine Sperre 37
4.3.6 Wer kann eine Sperre anordnen 37
4.3.7 Prozedur für einen Sperrantrag 37
4.3.8 Sperraufhebung 38
4.3.9 Grenzen einer Sperrperiode 38
4.3.10 Aktualisierungsfrequenz der Widerrufsliste 38
4.3.11 Anforderungen an die Überprüfung durch Widerrufslisten 38
4.3.12 Möglichkeiten zur online Statusabfrage 39
4.3.13 Anforderungen an die Statusabfrage 39
4.3.14 Weitere Verfahren zur Bekanntgabe von Widerrufen 39
4.3.15 Anforderungen an die Überprüfung weiterer Verfahren zur Bekanntgabe von Widerrufen 39

4.3.16 Spezielle Verfahren bei Kompromittierung von privaten Schlüsseln 40
4.4 Protokollierung sicherheitsrelevanter Ereignisse 40
4.4.1 Protokollierte Ereignisse 40
4.4.2 Frequenz der Überprüfung der Protokolldateien 41
4.4.3 Aufbewahrungszeitraum der Protokolldateien 41
4.4.4 Schutz der Protokolldateien 41
4.4.5 Protokollierungssystem (intern/extern) 41
4.4.6 Benachrichtigung beim Auftreten sicherheitskritischer Ereignisse 42
4.4.7 Bewertungen zur Angreifbarkeit 42
4.5 Archivierung 42
4.5.1 Archivierte Daten 42
4.5.2 Aufbewahrungszeiten 43
4.5.3 Schutzvorkehrungen 43
4.5.4 Anforderungen, die Daten mit Zeitstempeln zu versehen 43
4.5.5 System zur Erfassung der Archivierungsdaten (intern / extern) 44
4.5.6 Prozeduren zum Abrufen und Überprüfen von Daten 44
4.6 Schlüsselwechsel von a.trust-Schlüsseln 44
4.7 Kompromittierung und Notfallplan 45
4.7.1 Rechner, Software und/oder Daten sind korrumpiert 45
4.7.2 Widerruf von Zertifikaten zu Zertifizierungsstellen- und Dienste-Schlüsseln 45
4.7.3 Schlüsselkompromittierung bzw. Verdacht auf Schlüsselkompromittierung 47
4.7.4 Sicherheitsvorkehrungen nach Katastrophen 48
4.8 Einstellung der Tätigkeit der Zertifizierungsstelle 48
5 Physische, verfahrensorientierte und personelle Sicherheitsvorkehrungen . 50
5.1 Physische Sicherheitsvorkehrungen 50

5.1.1 Standort und örtliche Gegebenheiten 50
5.1.2 Zugangskontrollen 50
5.1.3 Stromversorgung und Klimaanlage 51
5.1.4 Wasserschäden 51
5.1.5 Feuer 51
5.1.6 Datenträger 51
5.1.7 Müllentsorgung 52
5.1.8 Redundante Auslegung 52
5.2 Verfahrensorientierte Sicherheitsvorkehrungen 52
5.2.1 Funktionen der a.trust 53
5.2.2 Sicherheitskritische Funktionen 53
5.2.3 Sonstige (nicht sicherheitskritische) Funktionen 54
5.2.4 Anzahl erforderlicher Personen für sicherheitsrelevante Tätigkeiten 55
5.2.5 Identifikation und Authentikation der Rollen 57
5.3 Personelle Sicherheitsvorkehrungen 57
5.3.1 Anforderungen an das Personal 57
5.3.2 Überprüfung des Personals 57
5.3.3 Anforderungen an die Schulung 57
5.3.4 Anforderungen und Häufigkeit von Schulungswiederholungen 58
5.3.5 Ablauf und Frequenz der Job Rotation 58
5.3.6 Sanktionen für unautorisierte Handlungen 58
5.3.7 Anforderungen an Vertragsvereinbarungen mit dem Personal 58
5.3.8 An das Personal auszuhändigende Dokumente 58
6 Technische Sicherheitsvorkehrungen 59
6.1 Schlüsselgenerierung und Installation 59

6.1.1 Schlüsselgenerierung 59
6.1.2 Auslieferung privater Schlüssel an Zertifikatsinhaber 59
6.1.3 Auslieferung öffentlicher Schlüssel an die Zertifikatsinhaber 60
6.1.4 Schlüssellängen 60
6.1.5 Parameter zur Schlüsselerzeugung 61
6.1.6 Qualitätsprüfung der Parameter 61
6.1.7 Hardware/Software Schlüsselerzeugung 61
6.1.8 Verwendungszweck der Schlüssel (nach X.509 v3 key usage Feld) 61
6.2 Schutz der privaten Schlüssel 63
6.2.1 Schutz des Schlüssels der Zertifizierungsstelle 63
6.2.2 Schutz der Schlüssel der Zertifikatsinhaber 63
6.2.3 Aufteilung privater Schlüssel auf mehrere Personen 63
6.2.4 Hinterlegung privater Schlüssel 63
6.2.5 Backup privater Schlüssel 64
6.2.6 Archivierung privater Schlüssel 64
6.2.7 Einbringung privater Schlüssel in das kryptographische Modul 64
6.2.8 Methode zur Deaktivierung privater Schlüssel 65
6.2.9 Methode zur Vernichtung privater Schlüssel 65
6.3 Weitere Aspekte zum Schlüsselmanagement 66
6.3.1 Archivierung öffentlicher Schlüssel 66
6.3.2 Verwendungszeitraum öffentlicher und privater Schlüssel 66
6.4 Aktivierungsdaten 67
6.4.1 Erzeugung und Installation der Aktivierungsdaten (PINs) 67
6.4.2 Schutz der Aktivierungsdaten 68
6.5 Computer Sicherheitsbestimmungen 68

6.5.1 Spezifische Sicherheitsanforderungen an die Computer 68
6.5.2 Bewertung der Computersicherheit..... 68
6.6 Lebenszyklus der Sicherheitsvorkehrungen 68
6.6.1 Systementwicklung 68
6.6.2 Sicherheitsmanagement 69
6.6.3 Bewertung..... 69
6.7 Vorkehrungen zur Netzwerksicherheit 69
6.8 Vorkehrungen zur Wartung (Analyse) des kryptographischen Moduls 69
7 Profile von Zertifikaten und Widerrufslisten..... 70
7.1 Zertifikatsprofile..... 70
7.1.1 CA-Zertifikate 70
7.1.2 Zertifikate für Zertifikatsinhaber..... 71
7.1.3 Erweiterungen (certificate extensions)..... 72
7.2 Profil der Widerrufsliste..... 73
7.2.1 Versionsnummern..... 73
7.2.2 CRL und CRL Entry Extensions..... 73
8 Administration dieser Spezifikation 75
8.1 Prozeduren zur Änderung dieses Dokuments 75
8.2 Verfahren zur Publizierung und Bekanntgabe 75
8.3 Genehmigung und Eignung einer Zertifizierungsrichtlinie..... 76
9 Anhang 77

Tabellenverzeichnis

Tabelle 1 a.trust Homepage und Verzeichnisdienste 23

Tabelle 2 Standorte 50

Tabelle 3 Funktionen der a.trust 53

Tabelle 4 Sicherheitskritische Funktionen 54

Tabelle 5 Sonstige Funktionen 55

Tabelle 6 Anzahl erforderlicher Personen 56

Tabelle 7 Gültigkeitsdauer von Zertifikaten 66

Tabelle 8 Profil für CA-Zertifikat 71

Tabelle 9 Profil für a.sign cyberDOC Zertifikat 72

Tabelle 10 Erweiterungen (CA-Zertifikate) 72

Tabelle 11 Erweiterungen (a.sign cyberDOC Zertifikate) 73

Abbildungsverzeichnis

Abbildung 1 Zertifizierungshierarchie 14

Abbildung 2 a.trust Verzeichnisbaum 15

1 Einleitung

1.1 Überblick

Das Ziel der vorliegenden a.trust Zertifizierungsrichtlinie besteht darin, die Umsetzung der Ausgabe, Administration und Anwendung von a.sign cyberDOC 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 Ausgabe von a.sign cyberDOC 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 Zertifizierungsrichtlinie:	a.trust Certification Practice Statement für einfache Zertifikate a.sign cyberDOC
Version:	1.0.1/21.06.2004
Object Identifier:	**1.2.040.0.17** (a.trust) **.2** (CPS) **.16** (a.sign cyberDOC) **.1.0.1** (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 a.sign cyberDOC Zertifikate aus, die auf einer Smartcard als Signaturerstellungseinheit basieren.

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. Die Aushändigung der Karte erfolgt ebenfalls in der Registrierungsstelle.

1.3.3 Widerrufsdienst

Die Anwender können sich zum Zweck der Durchführung einer Sperre, einer Sperraufhebung oder eines Widerrufs ihres Zertifikats telefonisch an den Widerrufsdienst wenden und die Durchführung veranlassen.

1.3.4 Anwender

Unter „Anwender“ sind einerseits die Personen zu verstehen, welche a.sign cyberDOC Zertifikate von a.trust erhalten (Zertifikatsinhaber, Signatoren) und andererseits jene, die diese Zertifikate nutzen bzw. den Zertifikatsangaben vertrauen. Letztere sind Empfänger von digital signierten Daten eines Zertifikatsinhabers oder Absender von verschlüsselten Daten an einen Zertifikatsinhaber.

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.

Der Produktname a.sign cyberDOC bezieht sich auf alle auf Karten basierenden nicht qualifizierten Zertifikate, welche in dieser Zertifizierungsrichtlinie beschrieben werden. In technischer Hinsicht (ausstellende CA) wird unterschieden zwischen den Zertifikaten der a.sign cyberDOC Karte für Signatur (a-sign-Token-Sig) und Geheimhaltung (a-sign-Token-Enc).

Die folgenden Anwenderzertifikate unterliegen dieser Zertifizierungsrichtlinie:

- Zertifikate von Signaturschlüsseln, welche in der a.sign cyberDOC Karte erzeugt und aufbewahrt werden und nur zur Erstellung einfacher Signaturen dienen,

- Zertifikate von Geheimhaltungsschlüsseln, welche in der a.sign cyberDOC Karte erzeugt und aufbewahrt werden und zur Authentifizierung, Geheimhaltung und zur Erstellung einfacher Signaturen verwendet werden können.

1.3.6 Zertifizierungshierarchie

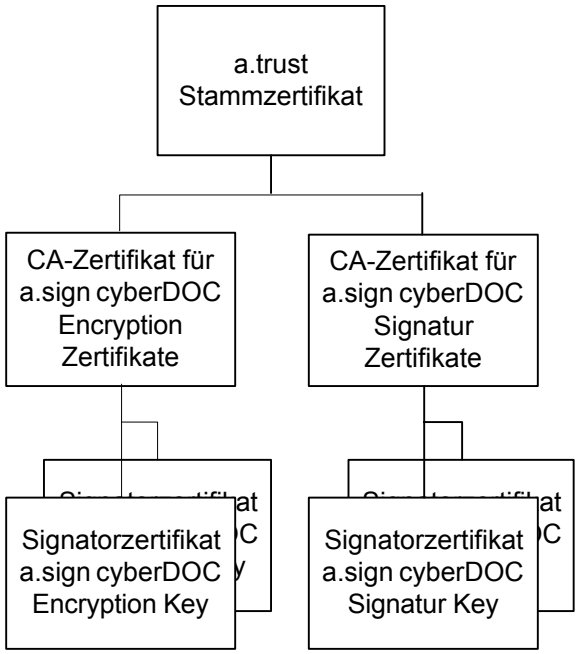

Abbildung 1 Zertifizierungshierarchie

1.3.7 a.trust Verzeichnisbaum

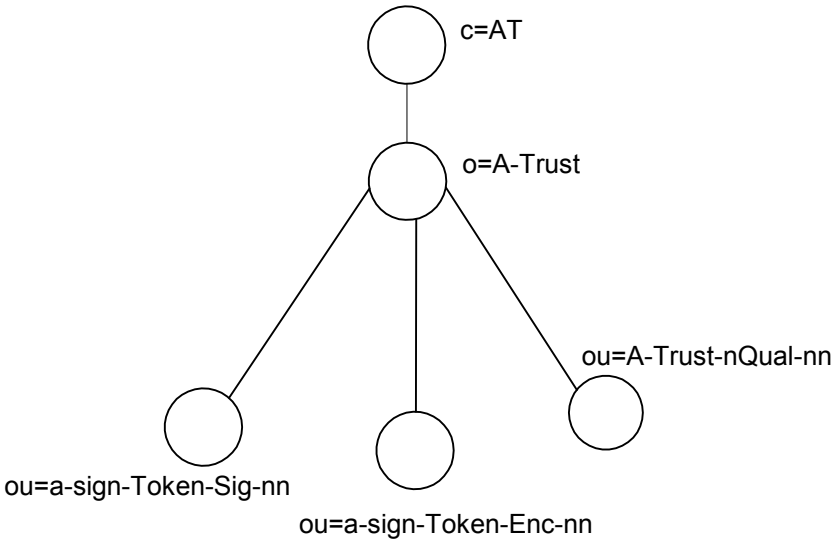

Abbildung 2 a.trust Verzeichnisbaum

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 Zertifikate der Zertifikatsinhaber und die zugehörigen CRLs werden je nach Art des Zertifikats mit den CA-Schlüsseln

- a-sign-Token-Sig-nn oder
- a-sign-Token-Enc-nn

signiert, wobei -nn die Version der Zertifizierungsstelle bezeichnet.

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 cyberDOC Zertifikate von a.trust erhält man auf folgenden Wegen:

- Auf der Homepage von a.trust:
  http://www.a-trust.at/
- bei der Informationshotline des Call Centers:
  die Telefonnummer ist der Homepage zu entnehmen
- in jeder Registrierungsstelle von a.trust und
- auf schriftliche Anfrage an:
  A-Trust
  Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH.
  Landstraßer Hauptstraße 5
  A-1030 Wien

1.4.3 Verantwortlicher für die Anerkennung anderer Policies

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

2 Generelle Bestimmungen

2.1 Verpflichtungen

2.1.1 Verpflichtungen der Zertifizierungsstellen

Die Zertifizierungsstelle von 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 gesperrt, widerrufen oder erneuert werden.
- Die Zertifizierungsstelle arbeitet im Einklang mit dem der Aufsichtsbehörde vorgelegten Sicherheits- und Zertifizierungskonzept.
- Die Zertifizierungsstelle beschäftigt Personal mit angemessener Qualifikation.
- Die Zertifizierungsstelle kommt ihrer Informationspflicht hinsichtlich Zertifikatsinhaber und Aufsichtsbehörden nach.
- Die Zertifizierungsstelle sorgt durch geeignete Maßnahmen (technisch, organisatorisch, infrastrukturell und personell) für den Schutz des privaten Schlüssels der Zertifizierungsstelle.
- Der Einsatz des privaten Schlüssels der Zertifizierungsstelle erfolgt ausschließlich zum Signieren der Zertifikate der Zertifikatsinhaber und zum Signieren der zugehörigen Widerrufslisten.
- Die Zertifizierungsstelle veröffentlicht alle ausgestellten a.sign cyberDOC Zertifikate sowie alle widerrufenen und alle gesperrten 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 Registrierungsstellen übermitteln die Zertifikate durch persönliche Übergabe der Karte an den im Zertifikat benannten Signator. Eine Ausnahme bildet die Kanzleikarte, die nicht auf einen Signator persönlich, sondern auf den Namen des Notariats ausgestellt wird. a.trust stellt dem Zertifikatsinhaber insbesondere folgende Dokumente elektronisch zur Verfügung:
  - Vertragsbedingungen,
  - Entgeltbestimmungen sowie
  - Certificate Policy, Certification Practice Statement.

2.1.3 Verpflichtungen der Zertifikatsinhaber

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

- Die Zertifikatsinhaber verpflichten sich, die Allgemeinen Geschäftsbedingungen zusammen mit der a.sign cyberDOC Certificate Policy, 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 Authentikation mit.
- Der Zertifikatsinhaber ist verpflichtet, seinen privaten Schlüssel angemessen zu schützen. Dies umfasst insbesondere keinen Zugriff durch unautorisierte Personen auf den auf der a.sign cyberDOC Karte gespeicherten privaten Schlüssel zuzulassen und Aktivierungsdaten (PIN) des privaten Schlüssels nicht weiterzugeben.
- Falls nötig initiiert der Signator unverzüglich die Sperre seines Zertifikats. Wird die Sperre nicht nach einem vorgegebenen Zeitraum aufgehoben, so erfolgt automatisch ein Widerruf des Zertifikats. Ebenso kann er einen sofortigen Widerruf veranlassen.

- Der Zertifikatsinhaber setzt sein Zertifikat nur zu dem im Zertifikat angegebenen Zweck ein (siehe hiezu Kapitel 7.1.3). Maßgeblich hierfür sind 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 im Ausland zu beachten.

2.1.4 Verpflichtungen der Zertifikatsnutzer

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

- Im Falle eines Signaturzertifikats prüft der Zertifikatsnutzer die digitale Signatur.
- 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 Listen mit

- ausgestellten Zertifikaten,
- gesperrten Zertifikaten und
- widerrufenen Zertifikaten.

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

2.2 Haftung

Die Allgemeinen Geschäftsbedingungen bilden zusammen mit der Zertifizierungsrichtlinie, der Certificate Policy und den Entgeltbestimmungen der a.trust in der jeweils gültigen Form die Grundlage für den abgeschlossenen Vertrag.

2.2.1 Haftung der Zertifizierungsstelle

a.trust haftet gegenüber Dritten, die auf die Richtigkeit des Zertifikats vertraut haben, dass

- 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.

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 von a.sign cyberDOC Zertifikaten über den Verzeichnisdienst ist kostenfrei.

2.5.3 Sperre oder Widerruf von Zertifikaten

Die Sperre und der Widerruf eines Zertifikats sind 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 a.trust CA-Zertifikat

Das jeweils benötigte CA-Zertifikat ist unter

- http://www.a-trust.at/certs/a-sign-token-Enc-nnx.crt
  für das Geheimhaltungs-Zertifikat der a.sign cyberDOC Karte
- http://www.a-trust.at/certs/a-sign-token-Sig-nnx.crt
  für das Signatur-Zertifikat der a.sign cyberDOC Karte

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

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

2.6.4 Widerrufsinformationen

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

- ldap://ldap.a-trust.at/ou=a-sign-token-Enc-nn,o=A-Trust,c=AT?certificaterevocationlist? für das Geheimhaltungs-Zertifikat der a.sign cyberDOC Karte
- ldap://ldap.a-trust.at/ou=a-sign-token-Sig-nn,o=A-Trust,c=AT?certificaterevocationlist? für das Signatur-Zertifikat der a.sign cyberDOC Karte

(-nn bezeichnet die Versionsnummer der a.trust Zertifizierungsstelle,
z. B. ou=a-sign-token-Sig-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 Zertifikat (Suchkriterien: Nachname, Vorname) und den Download eines gefundenen Zertifikats steht auf der a.trust Homepage ein Formular 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 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, das 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. Bei der Verwendung von Pseudonymen durch den Zertifikatsinhaber muss a.trust den ihr bekannten korrekten und vollständigen Namen des Zertifikatsinhabers an berechtigte Dritte weitergeben.

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

2.8.2 Nicht vertraulich eingestufte Informationen

Als nicht vertrauliche Daten werden die Informationen in den öffentlich verfügbaren Zertifikaten und Widerrufslisten angesehen.

2.8.3 Offenlegung von Informationen zu Zertifikatssperren bzw. -widerruf

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

2.8.4 Offenbarung an Behörden im Rahmen gesetzlicher Pflichten

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.

Es sind folgende Daten aufzunehmen:

- Name für das Zertifikat:
  Zertifikat eines Karteninhabers, der in seiner von der ÖNK zugewiesenen Rolle (z. B. Notar, Substitut etc.) arbeitet : Nachname und Vorname des Signators sind erforderlich.
  Kanzleizertifikat: Genaue Bezeichnung des Notariats, für welches das Zertifkat ausgestellt wird.
  Zusätzlich wird auch die von der ÖNK zugewiesene Rolle in das Zertifikat aufgenommen.

- Die Angabe der postalischen Adresse des Zertifikatsinhabers ist erforderlich.

- Die Angabe der Meldeadresse ist optional.

- Auf der Kartenoberfläche stehen zwei Zeilen für Namensinformationen zur Verfügung. Die Angabe der ersten Zeile ist erforderlich, die zweite Zeile ist optional.

- Die Angabe einer E-Mailadresse ist optional und wird, wenn vorhanden, in die Zertifikatserweiterungen aufgenommen.

3.1.2 Anforderungen an die Namen

Der vollständige Name wird laut vorgelegtem Dokument erfasst.

3.1.3 Regeln zur Interpretation unterschiedlicher Namensformen

Keine Bestimmungen.

3.1.4 Eindeutigkeit der Namen

Jeder Inhaber eines a.sign cyberDOC Zertifikats erhält eine zwölf-stellige Identifikationsnummer (Cardholder Identification Number = CIN). Diese Nummer ist ein Teil des eindeutigen Namens des Zertifikatsinhabers und ermöglicht die eindeutige und unveränderliche Zuordnung zu einem Zertifikatsinhaber.

3.1.5 Anspruch auf Namen und Beilegung von Streitigkeiten

Keine Bestimmungen.

3.1.6 Anerkennung, Bestätigung und Bedeutung von Warenzeichen

Keine Bestimmungen.

3.1.7 Methode zum Beweis des Besitzes des geheimen Schlüssels

Die a.sign cyberDOC Karte wird mit je einem generierten Schlüsselpaar für Signatur und Geheimhaltung an den Zertifikatsinhaber übergeben. Somit ist kein Beweis des Besitzes eines zum öffentlichen Schlüssel gehörenden privaten Schlüssels erforderlich.

3.1.8 Authentisierung von Individuen

Die Angaben des Antragstellers werden bei der Abholung der Karte in der Registrierungsstelle vom Registration Officer überprüft. Der Antragsteller beweist seine Identität durch das Vorlegen eines gültigen, amtlichen Lichtbildausweises (Dienstausweis

des Karteninhabers, der in seiner von der ÖNK zugewiesenen Rolle, z. B. Notar, Substitut etc., arbeitet). Der Abholer einer Kanzleikarte wird mit dem Dienstausweis oder mittels Informationen, die die zuständige Kammer beherbergt, identifiziert.

3.2 Erneute Registrierung/Rezertifizierung

Der registrierte Zertifikatsinhaber kann neue bzw. zusätzliche Zertifikate (Ersatz- und Zusatzkarten) beantragen. Der Vorgang verläuft analog zur Erstregistrierung (siehe Abschnitt 3.1). Dabei sind allfällige Änderungen in den personenbezogenen Daten anzugeben. Die Identifikationsnummer des Zertifikatsinhabers wird dabei nicht verändert.

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 Sperr- und Widerrufsantrag

Sperren, Sperraufhebungen und Widerrufe werden entsprechend Abschnitt 4.3 gehandhabt.

Der Zertifikatsinhaber kann sein Zertifikat per Telefon sowohl sperren als auch widerrufen oder die Sperre aufheben lassen. Darüberhinaus kann er sein Zertifikat mittels eines Faxantrags widerrufen lassen.

Der Karteninhaber muss zumindest seinen Vor- und Zunamen und das Passwort für Sperre und Widerruf angeben.

Sollte er dazu nicht in der Lage sein, werden für eine Sperre die Angaben

- Geburtsdatum und
- Geburtsort

benötigt. Weitere Angaben können bei mangelnder Eindeutigkeit herangezogen werden.

Wenn im Falle eines Widerrufs das Passwort vergessen wurde, kann der Karteninhaber sein Sperr- und Widerrufspasswort mit Ausweisleistung in der Registrierungsstelle erfragen. Anstelle eines Widerrufs kann er eine Sperre beantragen, die auch

ohne Passwortangabe möglich ist. Eine Sperraufhebung ist nur mit dem Sperraufhebungspasswort möglich.

4 Betriebliche Anforderungen

4.1 Antrag auf Ausstellung von Zertifikaten

Die Antragstellung erfolgt mittels eines Formulars, das von a.trust zur Verfügung gestellt wird. Das Formular wird vom Antragsteller ausgefüllt und an die Registrierungsstelle übermittelt.

Der Antragsteller erhält

- die PIN- und PUK-Daten sowie
- den Antrag auf Ausstellung eines Zertifikats mit den Vertragsbedingungen.

4.2 Herausgabe und Akzeptanz von Zertifikaten

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

Für die Ausgabe der Karte an den Signator muss dieser persönlich in der von ihm angegebenen Registrierungsstelle vorstellig werden (Ausnahme: Kanzleikarte, die nicht an eine Person, sondern an ein Notariat ausgestellt wird). Der Registration Officer darf die Karte erst herausgeben, wenn

- er die Identität des Antragstellers anhand eines gültigen, amtlichen Lichtbildausweises (Dienstausweis desKarteninhabers, der in seiner von der ÖNK zugewiesenen Rolle, z. B. Notar, Substitut etc., arbeitet) überprüft hat,
- der Antragsteller den Erhalt der Vertragsbedingungen (elektronisch oder vor Ort in der Registrierungsstelle) und die Korrektheit der Antragsdaten bestätigt hat,
- der Antragsteller den Erhalt des Briefes mit PIN, PUK und Passwort bestätigt hat, sowie
- die Allgemeinen Geschäftsbedingungen akzeptiert hat.

4.3 Sperre und Widerruf von Zertifikaten

a.sign cyberDOC Zertifikate können vorübergehend gesperrt werden. Diese Sperre kann auch, wenn sie nicht aufgehoben wird, in einen endgültigen Widerruf umgewandelt werden.

Ebenso ist ein sofortiger und permanenter Widerruf des Zertifikats möglich.

4.3.1 Gründe für einen Widerruf

Der Widerruf eines Zertifikats wird erforderlich, wenn

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

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) oder
- die Zertifizierungsstelle selbst.

4.3.3 Prozedur für einen Widerrufsantrag

Ein Widerruf kann durch den Zertifikatsinhaber vorgenommen werden. Dies kann wie folgt geschehen: Der Zertifikatsinhaber wendet sich per Telefon oder auch Fax an den Widerrufsdienst. Die aktuellen Telefonnummern der Widerrufsdienste sind der a.trust Homepage zu entnehmen.

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

- Telefonat: Der Zertifikatsinhaber kann rund um die Uhr einen Widerruf per Telefon vornehmen.
  Für den Widerruf ist die Angabe des Passworts für Sperre und Widerruf verpflichtend.
  Der Grund für den Widerruf (Kompromittierung des privaten Schlüssel, Änderung von Zertifikatsdaten, Auflösung des Vertrages etc.) muss dem Mitarbeiter des Widerrufsdienstes mitgeteilt werden.

- Faxnachricht: Ist ein telefonischer Anruf nicht möglich, dann kann der Widerruf per Fax vorgenommen werden. Die Daten, die auf dem Faxantrag anzugeben sind, sind die selben wie beim Telefonat.

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

- Passwort für Sperre und Widerruf: obligatorisch

- Vor- und Nachname bzw. Bezeichnung des Notariats: obligatorisch

- Wenn die Karte sich durch oben genannte Angaben nicht eindeutig identifizieren lässt: Verwendung von weiteren Daten wie Geburtsdatum und –ort, Kartennummer, Identifikationsnummer, Adresse, etc.

Hat der Inhaber eines a.sign cyberDOC Zertifikats sein Sperr- und Widerrufspasswort vergessen, ist ein Widerruf nicht möglich. Er kann statt dessen eine Sperre beantragen oder sein Passwort mit Ausweisleistung in einer Registrierungsstelle erfragen.

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.

Der Widerrufsdienst ist täglich 24 Stunden erreichbar.

Die aktuelle Update-Frequenz für die Widerrufsliste und die Erreichbarkeit des Widerrufsdienstes sind der a.trust Homepage zu entnehmen.

4.3.5 Gründe für eine Sperre

Die Sperre ist ein temporäres Aussetzen der Gültigkeit des Zertifikats. Sie kann bei Verdacht auf einen Defekt, eine Manipulation oder den Verlust der Karte eingesetzt werden. Im Gegensatz zu einem Widerruf kann eine Sperre innerhalb einer festgelegten Frist auch wieder aufgehoben werden. Nach dem Ende der Sperrperiode (siehe Kapitel 4.3.9) wird eine nicht aufgehobene Sperre durch a.trust automatisch in einen Widerruf umgewandelt.

4.3.6 Wer kann eine Sperre anordnen

Die bevollmächtigten Personen für eine Sperre sind:

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

4.3.7 Prozedur für einen Sperrantrag

Eine Sperre kann durch den Zertifikatsinhaber wie folgt veranlasst werden: Der Zertifikatsinhaber wendet sich per Telefon an den Widerrufsdienst.

Für die Sperre ist die Angabe des Sperr- und Widerrufspassworts oder die Angabe von Geburtsdatum und –ort verpflichtend.

Die für eine Sperre benötigten Informationen lassen sich wie folgt zusammenfassen:

- Passwort für die Authentikation oder Geburtsdatum und Geburtsort: obligatorisch
- Vor- und Nachname bzw. Bezeichnung des Notariats: obligatorisch
- Wenn die Karte sich durch oben genannte Angaben nicht eindeutig identifizieren lässt: Verwendung von weiteren Daten wie Geburtsdatum und Geburtsort, Kartennummer, Identifikationsnummer, Adresse, etc.

Bei Bekanntgabe der Sperre muss der Signator dem Mitarbeiter des Widerrufsdienstes ein vier- bis zehn-stelliges Sperraufhebungspasswort nennen, mit dem er

die Sperre bis 22:00 Uhr des zweiten darauffolgenden Werktages aufheben lassen kann. Wird die Sperre nicht aufgehoben, so geht sie automatisch in einen Widerruf über.

4.3.8 Sperraufhebung

Innerhalb der Sperrperiode (siehe Kapitel 4.3.9) kann der Inhaber eines a.sign cyberDOC Zertifikats die Sperre des Zertifikats wieder aufheben lassen. Dazu muss er die Sperraufhebung beim Widerrufsdienst telefonisch beantragen. Weiß der Zertifikatsinhaber sein Sperraufhebungspasswort nicht, so ist eine Sperraufhebung nicht möglich.

Die Archivierung der Anträge erfolgt in gleicher Weise wie bei Sperre und Widerruf.

4.3.9 Grenzen einer Sperrperiode

Die Sperre kann bis 22:00 Uhr des zweiten auf den Tag der Sperre folgenden Werktags wieder aufgehoben werden, sonst wird sie durch a.trust automatisch in einen Widerruf umgewandelt.

4.3.10 Aktualisierungsfrequenz der Widerrufsliste

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

4.3.11 Anforderungen an die Überprüfung durch Widerrufslisten

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

Für eine positive Gültigkeitsüberprüfung ist erforderlich, dass

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

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), ist es empfehlenswert keine Zertifikate zu akzeptieren. Das Risiko für die Akzeptanz eines solchen Zertifikats trägt jedenfalls der Zertifikatsnutzer.

4.3.12 Möglichkeiten zur online Statusabfrage

Es wird ein OCSP-Dienst über das Internet angeboten.

4.3.13 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.

4.3.14 Weitere Verfahren zur Bekanntgabe von Widerrufen

Keine Bestimmungen.

4.3.15 Anforderungen an die Überprüfung weiterer Verfahren zur Bekanntgabe von Widerrufen

Keine Bestimmungen.

4.3.16 Spezielle Verfahren bei Kompromittierung von privaten Schlüsseln

Bei einem Verlust der Karte lässt der Zertifikatsinhaber diese sperren. Sollte zugleich auch die zugehörige PIN nicht mehr verfügbar oder sicher sein, führt der Zertifikatsinhaber einen Widerruf durch.

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,
- Sperr- und Widerrufsanträge,
- ausgeführte Sperren und Widerrufe sowie

- Schlüsselwechsel.

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

- Bestätigung des Kartenerhalts und des Erhalts von PIN- und PUK-Kuvert durch den Signator,
- Akzeptanzerklärung der Allgemeinen Geschäftsbedingungen und der Entgeltbestimmungen durch den Zertifikatswerber oder auch
- Änderungen an den personenbezogenen Daten des Zertifikatsinhabers.

4.4.2 Frequenz der Überprüfung der Protokolldateien

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

4.4.3 Aufbewahrungszeitraum der Protokolldateien

Sicherheitsrelevante Protokolldateien werden über die gesetzliche Frist hinaus aufbewahrt. Protokolldateien, die benötigt werden, um nachträglich Aussagen über die Gültigkeit von Zertifikaten zu treffen, werden archiviert. Dies gilt besonders für Daten zur Veröffentlichung von Zertifikaten und Widerrufslisten sowie Eingang und Bearbeitung von Sperranträgen. 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, ggf. Cross-Zertifikate und Zertifikate der Signatoren),
- Sperr- und Widerrufanträge mit Datum und Uhrzeit des Eintreffens (inklusive entsprechender Protokolldateien),
- alle ausgestellten Widerrufslisten,
- Datum und Uhrzeit der Veröffentlichung der Zertifikate und Widerrufslisten (inkl. 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 Sperr- und 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

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 a.trust-Schlüsseln

Ein Schlüsselwechsel von CA- und Root-Schlüsseln erfolgt im Zusammenhang mit dem Ausfall eines Hardware Security Moduls oder 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 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 Veröffentlichung unkorrekter Daten zu verhindern. Die Wiederaufnahme des Dienstes ist mit der Veröffentlichung der neuen Widerrufsliste verbunden. Abhängig von Fehlern und Ausfallszeit 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 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.

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 auch der dazugehörige private Schlüssel nicht weiter eingesetzt. Um aber die Zertifizierungsdienstleistungen und Dienste weiter aufrecht zu erhalten, muss die Zertifizierungsstelle einen neuen Schlüssel einsetzen. Verfügt die Zertifizierungsstelle aufgrund eines durchgeführten Schlüsselwechsels bereits über einen solchen neuen Schlüssel, so kann dieser eingesetzt werden. Dies ist aber nur unter der Bedingung möglich, dass der Schlüssel auch weiterhin gültig ist. Sollte dies nicht mehr der Fall sein, so wird ein Schlüsselwechsel nach den Richtlinien aus Abschnitt 4.6 durchgeführt, die sich aber in folgenden Punkten von dem regulären Wechsel unterscheiden:

- Eine rechtzeitige Information der Zertifikatsinhaber über den Schlüsselwechsel ist bei einem unmittelbaren Widerruf nicht möglich. Die Zertifikatsinhaber werden im Zusammenhang mit der Widerrufsinformation auch 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 Maßnahmen. 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 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 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 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	Externer Beauftragter zur Durchführung der betriebsinternen Audits Darf keine andere Funktion aus dem sicherheitskritischen Bereich durchführen, außer wenn es für die Revision erforderlich ist.
Datenschutz	Überwachung 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
Sicherheitssystemad-ministrator	Zutritt in die Hochsicherheitszone Beaufsichtigung von Systemadministrator und System-operator
Kartenproduzent-Initialisierer	Initialisieren der Karten auf der Initialisierungsanlage
Kartenproduzent-Personalisierer	Personalisieren der Karten auf der Personalisierungsan-lage
Revocation Center Agent (RCA), Mit-arbeiter im Widerrufs-dienst	Ansprechpartner für die Zertifikatsinhaber hinsichtlich der Annahme von Anträgen für Sperre, Widerruf und Auf-hebung von Sperren Durchführung der Umwandlung einer Sperre in einen Widerruf
Registration Officer (RO), Mitarbeiter der Registrierungsstelle	Entgegennahme von Zertifikatsanträgen, Änderungsan-trägen und Nachdruckaufträgen für PIN-Kuverts. Identifikation von Zertifikatswerbern im Rahmen der Regis-trierung und der Bekanntgabe des Sperr- und Widerrufs-passworts 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 Sicherheits-systemadministrator beaufsichtigt.

Rolle	Funktion
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
Initialisierung der Karten	Kartenproduzent-Initialisierer	Nein	Nein
Personalisierung der Karten	Kartenproduzent-Personalisierer	Nein	Nein
Sperren von Anwenderzertifikaten	RCA	Nein	Nein
Widerrufen von Anwenderzertifikaten	RCA	Nein	Nein
Aufheben einer Sperre von Anwender-zertifikaten	RCA	Nein	Nein
Erzeugung der a.trust 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

Tätigkeit	Personen	Vier-augen-prinzip	Hoch-sicher-heit
Vergabe der Berechtigungen für RO und RCA	SO	Nein	Nein
Inbetriebnahme eines krypto-graphischen Moduls (Signaturer-stellungseinheit der a.trust 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
Überprüfung von Protokolldateien auf verdächtige Vorkommnisse	Systemadministrator	Nein	Nein
Überprüfung der Protokolldateien auf Manipulation	Systemadministrator	Nein	Nein
Anfertigung eines Backups der Proto-kolldateien und Lagerung desselben	Sicherheitssystemad-ministrator, Sicher-heitssystemad-ministrator	Ja	Ja
Qualitätsprüfung der verwendeten Schlüssellängen und Parameter zur Schlüsselerzeugung	SO	Nein	Nein
Wartung oder Austausch eines krypto-graphischen 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 zur Signatur von a.sign cyberDOC Zertifikaten 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 Geheimhaltungsschlüssel, welche sich im Chip der a.sign cyberDOC Karte befinden, werden von a.trust generiert und in verschlüsselter Form an den Kartenhersteller übermittelt, wo sie auf die Karte aufgebracht werden.

Die Generierung des Signaturschlüssels der a.sign cyberDOC Karte erfolgt im Hochsicherheitsbereich des Kartenherstellers. Die Schlüssel werden in den Karten erzeugt, auf welche anschließend die persönlichen Daten des Karteninhabers, der in seiner von der ÖNK zugewiesenen Rolle (z. B. Notar, Substitut etc.) arbeitet bzw. die Daten für das Notariat im Falle einer Kanzleikarte aufgebracht werden. In beiden Fällen wird noch kein Zertifikat erstellt. Dies geschieht erst auf Veranlassung der Registrierungsstelle, nachdem der Zertifikatsinhaber zuverlässig identifiziert und authentifiziert wurde.

6.1.2 Auslieferung privater Schlüssel an Zertifikatsinhaber

Die privaten Schlüssel werden in der a.sign cyberDOC Karte an den Zertifikatsinhaber ausgeliefert.

Ein Auslesen der privaten Schlüssel aus der Chipkarte ist nicht möglich. Der private Signatur- und der Geheimhaltungsschlüssel können nur durch die korrekte Eingabe der jeweiligen Identifikationsdaten (PIN) benutzt werden. Das Wissen über die PINs besitzt nur der Zertifikatsinhaber.

6.1.3 Auslieferung öffentlicher Schlüssel an die Zertifikatsinhaber

6.1.3.1 Öffentliche Schlüssel der Zertifizierungsstelle

Der öffentliche Schüssel der Root-CA wird jedem Zertifikatsinhaber, der über eine Chipkarte verfügt, mit dieser sicher ausgeliefert.

Zusätzlich werden die Zertifikate des Schlüssels der Root-CA sowie aller a.trust Zertifizierungsstellen 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 cyberDOC Zertifikats

Die öffentlichen Schlüssel werden analog zu den privaten Schlüsseln in der Chipkarte an den Zertifikatsinhaber ausgeliefert.

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

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

Die genannten Mindestlängen können sich aufgrund von Anpassung an geänderte gesetzliche Vorgaben oder, weil die Algorithmen nicht mehr den Sicherheitserwartungen entsprechen, 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 entspricht der 4. Fermatzahl.

6.1.6 Qualitätsprüfung der Parameter

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

6.1.7 Hardware/Software Schlüsselerzeugung

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

Die Schlüssel der Zertifikatsinhaber werden entweder in der a.sign cyberDOC Karte selbst oder in einem Hardware Security Modul von a.trust erzeugt.

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

Im den Zertifikaten für die öffentlichen Signaturschlüssel von a.sign cyberDOC Karten werden die folgenden Bits gesetzt:

- nonRepudiation
- digitalSignature.

In den Zertifikaten für die Geheimhaltungsschlüssel von a.sign cyberDOC Karten werden die folgenden Bits gesetzt:

- digitalSignature
- keyEncipherment
- dataEncipherment.

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 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 einer gesetzeskonformen Smartcard, die von A-SIT nach §18(5) [SigG] bescheinigt wurde, gespeichert. Die Verwendung des privaten Schlüssels ist durch eine PIN abgesichert.

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 einer Chipkarte (Schlüssel der Zertifikatsinhaber).

Es gilt, dass für die Aktivierung des Schlüssels der Root-CA oder einer Zertifizierungsstelle 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 Zertifikatsinhabern.

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

Private Schlüssel der Zertifizierungsstelle werden nicht archiviert.

Eine Speicherung von Schlüsseln der Zertifikatsinhaber findet durch a.trust in verschlüsselter Form im Falle der auf einer a.sign cyberDOC Karte befindlichen Geheimhaltungsschlüssel statt, damit diese Schlüssel auf einer Ersatz- oder Zusatzkarte ebenfalls verwendet werden können.

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 Signaturschlüssel des Zertifikatsinhabers, der sich auf der a.sign cyberDOC Karte befindet, wird direkt in der Karte generiert und ist vor dem Auslesen geschützt.

Der private Geheimhaltungsschlüssel des Zertifikatsinhabers, der sich auf einer a.sign cyberDOC Karte befindet, wird in einem Hardware Security Modul erzeugt und zur Wiederverwendung auf der nächsten Karte außerhalb des Security Moduls in verschlüsselter Form gespeichert.

6.2.7.3 Methode zur Freischaltung / Aktivierung privater Schlüssel

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

Die Schlüssel der Zertifikatsinhaber werden durch die korrekte Eingabe einer PIN aktiviert. Die PIN ist vor der Signaturerstellung oder Entschlüsselung einzugeben.Die Signatur-PIN ist vor jeder Aktivierung des privaten Schlüssel erneut einzugeben, die Geheimhaltungs-PIN schaltet den geheimen Schlüssel für mehrere aufeinander folgende Operationen frei.

Nach jeweils drei aufeinanderfolgenden Fehlversuchen ist die PIN gesperrt. Die PIN kann durch die korrekte Eingabe des PUK-Codes für drei weitere Versuche freigegeben werden. Dieser Vorgang kann maximal zehnmal durchgeführt werden, daraufhin ist der PUK gesperrt.Wenn die Anzahl von zehn PUK-Fehleingaben überschritten ist, ohne dazwischen eine korrekte PIN eingegeben zu haben, ist der PUK ebenfalls gesperrt.

6.2.8 Methode zur Deaktivierung privater Schlüssel

Wird ein Hardware Security Modul deaktiviert, so führt dies automatisch zur Deaktivierung aller in ihm enthaltenen privaten Schlüssel. Private Schlüssel, die nicht mehr genutzt werden, werden mit einer geeigneten Funktion im Hardware Security Modul deaktiviert.

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

6.2.9 Methode zur Vernichtung privater Schlüssel

Die auf dem Chip befindlichen Schlüssel der Zertifikatsinhaber werden durch die Zerstörung der Karte vernichtet.

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

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 Gültigkeitsdauern (Jahre):

Zertifikatstyp	Gültigkeits-dauer
Root-CA	3
Zertifizierungsstelle	3
a.sign cyberDOC	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 a.sign cyberDOC Zertifikate

Die Zertifikatsinhaber aktivieren ihren privaten Schlüssel über eine PIN.

Die Initial (bzw. Transport)-PIN für den Signaturschlüssel der a.sign cyberDOC Karte wird in einem Hardware Security Modul erzeugt. Die Zertifikatsinhaber erhalten diese mit der Benachrichtigung, dass ihre a.sign cyberDOC Karte zur Abholung bereit liegt. Mit dieser PIN kann noch keine Signatur durchgeführt werden. Die Eingabe der Initial-PIN fordert den Zertifikatsinhaber zur Änderung in eine selbstgewählte PIN auf. Erst unter Authentikation mit dieser Signatur-PIN ist eine Signaturerstellung möglich. Vor ihrer Änderung und innerhalb von drei Monaten ab Kartenerstellung kann der Zertifikatsinhaber die Initial-PIN nachdrucken lassen.

Die PIN für den Geheimhaltungsschlüssel der a.sign cyberDOC Karte wird ebenfalls in einem Hardware Security Modul erzeugt und unter den selben Bedingungen wie die oben beschriebene Signatur-PIN an den Zertifikatsinhaber versandt. Die PIN für den Entschlüsselungsvorgang kann vom Zertifikatsinhaber nicht verändert werden. Ein Nachdruck kann jederzeit erfolgen.

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 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-Zertifikate

Attribut	Inhalt	Erläuterung
Version	v3(2)	Die Versionsnummer wird auf „2“ gesetzt, um ein X.509 Zertifikat der Version 3 anzuzeigen
Seriennummer	Seriennummer des Zertifikats	Eindeutig innerhalb der a.trust Zertifizierungsinfrastruktur
Algorithmus	SHA-1	Für die Signatur über das Zertifikat verwendeter Algorithmus
Aussteller des Zertifikats	CN = A-Trust-nQual-nn OU = A-Trust-nQual-nn O = A-Trust 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-Token-Sig-nn oder CN = a-sign-Token-Enc-nn OU = a-sign-Token-Sig-nn oder OU = a-sign-Token-Enc-nn O = A-Trust 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

Attribut	Inhalt	Erläuterung
Version	v3(2)	Die Versionsnummer wird auf „2“ ge-setzt, 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-Token-Sig-nn oder CN = a-sign-Token-Enc-nn OU = a-sign-Token-Sig-nn oder OU = a-sign-Token-Enc-nn O = A-Trust C = AT	-nn bezeichnet die Generation des zertifizierten Schlüssels
Gültig von Gültig bis	Beginn und Ende der Gültigkeit des Zertifikats	Der Gültigkeitszeitraum beträgt höchstens drei Jahre
Zertifikatsin-haber	C = CountryName T = Title SN = SurName G = GivenName CN = CommonName OU = OrganizationalUnit Seriennummer = SerialNumber	CountryName: AT etc., enthält das Land, in dem das zur Registrierung vorgelegte Identifikationsdokument ausgestellt wurde. Title: Titel (Dr. etc.) SurName: Zuname GivenName: Vorname CommonName: Vorname + Zuname des Signators bei einem persönlichen Zertifikat oder Name des Notariats bei einem Kanzleizertifikat. OrganizationalUnit: Bezeichnung der

		von der ÖNK zugewiesenen Rolle SerialNumber: eindeutige Identifikationsnummer des Zertifikatsinhabers: siehe auch Abschnitt 3.1.4
Öffentlicher Schlüssel	RSA 1024 Bit	Öffentlicher Schlüssel des Zertifikatsinhabers

Tabelle 9 Profil für a.sign cyberDOC Zertifikat

7.1.3 Erweiterungen (certificate extensions)

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

Erweiterung	Zertifikatstyp		Klassifikation	
	Root	CA	kritisch	Nicht kritisch
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 10 Erweiterungen (CA-Zertifikate)

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

Erweiterung	Zertifikatstyp		Klassifikation	
	Signatur	Verschl.	kritisch	Nicht kritisch
Standarderweiterungen				
authorityKeyIdentifier	Ja	Ja		X
subjectKeyIdentifier	Ja	Ja		X
keyUsage	Ja	Ja	X	
certificatePolicies	Ja	Ja		X
subjectAltName	Optional	Optional		X
basicConstraints	Ja	Ja		X
cRLDistributionPoints	Ja	Ja		X
subjectDirectoryAttributes	Optional	Optional		X
Private Extensions				
authorityInfoAccess	Ja	Ja		X

Tabelle 11 Erweiterungen (a.sign cyberDOC Zertifikate)

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

Die Erweiterung subjectDirectoryAttributes kann optional das Geburtsdatum des Zertifikatsinhabers 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
- Sperren 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 cyberDOC. a.trust stellt sicher, dass diese Zertifizierungsrichtlinie für die betroffenen Certificate Policies geeignet ist.

9 Anhang

A Glossar

a.sign cyberDOC	Produktname für nicht qualifizierte Kartenzertifikate, die an Notariate und alle Karteninhaber, die in ihrer von der ÖNK zugewiesenen Rolle arbeiten (z. B. Notar, Substitut etc.) ausgestellt werden.
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 Zertifikatsinhaber 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 oder Klasse von Applikationen gleicher Sicherheitsanforderungen anzeigt.
Chipkarte	Smart Card auf der die Schlüssel des Anwenders sicher gespeichert sind und mit der die Signatur berechnet wird.
Dienste (CA-Dienste)	Überbegriff für angebotene Dienstleistungen wie Verzeichnisdienst, Statusauskunft und Zeitstempeldienst
Dienste-Schlüssel	Schlüssel eines Dienstes (z. B. 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.
ÖNK	Österreichische Notariatskammer
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. 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 gesperrt) 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 gesperrten und 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	Signator; Anwender, dessen Schlüssel und Daten im Zertifikat festgehalten sind.
Zertifikatsnutzer	Anwender, der Zertifikate der a.trust über die Schlüssel und Daten anderer nutzt, um Signaturen zu prüfen bzw. Daten zu verschlüsseln.
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 Sperren.

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