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

A-Trust

Certification Practice Statement für einfache Zertifikate trust|mark

Version: 1.3

Datum: 09.09.2002

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

1 Einleitung

1.1 Überblick

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

Eine Zertifizierungsrichtlinie gibt Auskunft über die Praktiken der Zertifizierungsstelle zur Herausgabe von trust|mark 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:	trust|mark Certification Practice Statement für einfache Zertifikate
Version:	1.3/09.09.2002
Object Identifier:	**1.2.040.0.17** (A-Trust) **.2** (CPS) **.2** (trust|mark) **.1.3** (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 Softwarezertifikate (trust|mark|vsc) und Serverzertifikate (trust|mark|server) aus sowie Zertifikate, die auf einer Smartcard als Signaturerstellungseinheit basieren (trust|mark|token Zertifikate).

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. Wenn ein trust|mark|token Zertifikat auszugeben ist, erfolgt die Aushändigung der Karte 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 trust|mark Zertifikate von A-Trust erhalten (Zertifikatsinhaber) und andererseits jene, die trust|mark 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.

Die folgenden Anwenderzertifikate unterliegen dieser Zertifizierungsrichtlinie:

- trust|mark|token Zertifikate von Verschlüsselungsschlüsseln, welche in der trust|sign Karte erzeugt und aufbewahrt werden,
- trust|mark|token Zertifikate von Signaturschlüsseln, welche in der trust|mark Karte erzeugt und aufbewahrt werden,
- trust|mark|token Zertifikate von Verschlüsselungsschlüsseln, welche in der trust|mark Karte erzeugt und aufbewahrt werden,
- trust|mark|vsc Zertifikate: Zertifikate von Schlüsseln, die sich nicht in einer Smartcard befinden und

- entweder nur für Angehörige von Behörden ausgestellt werden und der Signatur von E-Mails dienen oder
- für jedermann ausgestellt werden können und sowohl für Signatur als auch für Verschlüsselung Verwendung finden,

- trust|mark|server Zertifikate: Zertifikate von Schlüsseln, die sich auf einem Rechner befinden und
  - für SSL-Authentifizierung von Webservern,
  - für Signaturanwendungen von Signaturservern oder
  - für Geheimhaltungsanwendungen von Signaturservern Verwendung finden.

1.3.6 Zertifizierungshierarchie

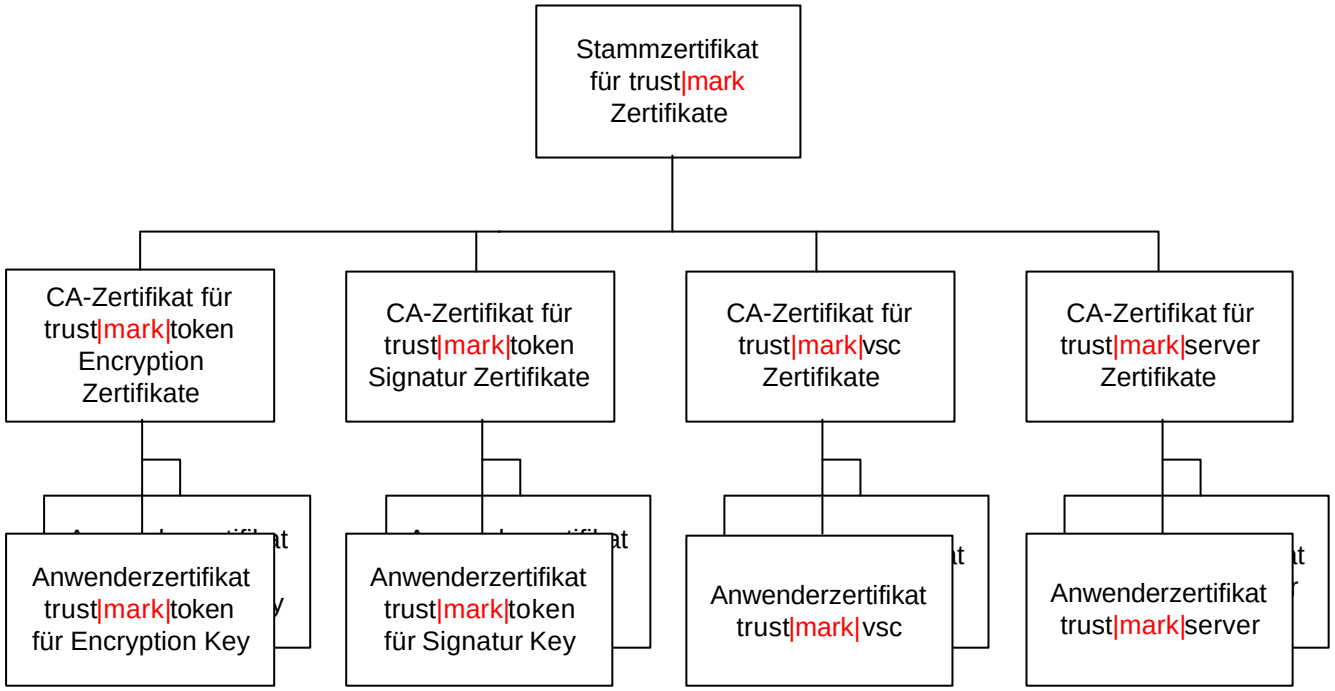

Abbildung 1 Zertifizierungshierarchie

1.3.7 A-Trust Verzeichnisbaum

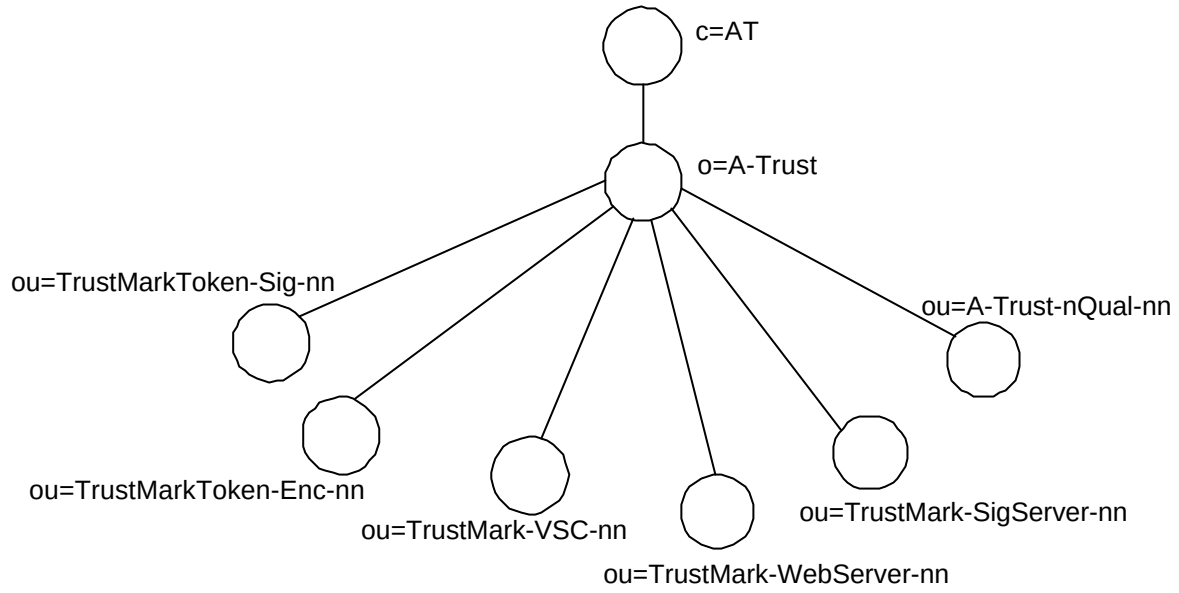

Abbildung 2 A-Trust Verzeichnisbaum

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

Mit A-Trust-nQual-nn werden die CA-Zertifikate für trust|mark und die zugehörigen CRLs signiert.

Die Zertifikate der Zertifikatsinhaber von trust|mark Zertifikaten und die zugehörigen CRLs werden je nach Art des Zertifikats mit den CA-Schlüsseln

- TrustMarkToken-Sig-nn,
- TrustMarkToken-Enc-nn,
- TrustMark-VSC-nn,
- TrustMark-WebServer-nn oder
- TrustMark-SigServer-nn.

signiert, wobei -nn die Version der A-Trust Zertifizierungsstelle bezeichnet, welche mit dem zugehörigen geheimen Schlüssel digitale Signaturen erstellt.

1.4 Ansprechpartner und Kontaktstellen

1.4.1 Organisation zur Verwaltung dieses Dokuments

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

1.4.2 Kontaktinformation

Kontaktinformationen für trust|mark 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:
  Telefonnummer: 0900 833 201
- 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 Widerrufslisten.
  Anmerkung: Es gibt auch private A-Trust-Schlüssel für andere Zwecke. In dieser Richtlinie werden nur die privaten Schlüssel für die Ausstellung von Zertifikaten und Widerrufslisten behandelt.
- Die Zertifizierungsstelle veröffentlicht alle ausgestellten Zertifikate (sofern nicht die Veröffentlichung eines Kartenzertifikats auf Wunsch des Inhabers unterdrückt wird) sowie alle widerrufenen Zertifikate und alle gesperrten Zertifikate. Dem Zertifikatsinhaber eines trust|mark|token Zertifikats steht bei der Antragstellung die Option frei, die Veröffentlichung seines Zertifikats zu verhindern. Es ist dann nicht öffentlich abfragbar, wird aber bei einer Sperre oder einem Widerruf in die Widerrufsliste aufgenommen.

2.1.2 Verpflichtungen der Registrierungsstellen

Die Registrierungsstellen der A-Trust befolgen die Regelungen 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 trust|mark Zertifikate (trust|mark|token Zertifikate durch persönliche Übergabe der Karte, trust|mark|vsc und trust|mark|server Zertifikate in elektronischer Form) an den Zertifikatsinhaber. A-Trust stellt dem Zertifikatsinhaber insbesondere folgende Dokumente elektronisch zur Verfügung:
  - Vertragsbedingungen,
  - Entgeltbestimmungen sowie
  - Certificate Policy, Certification Practice Statement.

2.1.3 Verpflichtungen der Zertifikatsinhaber

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

- Die Zertifikatsinhaber verpflichten sich, die Allgemeinen Geschäftsbedingungen zusammen mit der Certificate Policy für trust|mark|token bzw. trust|mark|vsc oder trust|mark|server, der gegenständlichen trust|mark Zertifizierungsrichtlinie und den Entgeltbestimmungen von A-Trust als Grundlage für den abgeschlossenen Vertrag anzuerkennen.
- Der Zertifikatsinhaber ist für die Richtigkeit der Angaben verantwortlich, die er bei der Registrierung macht und wirkt gemäß den in dieser Zertifizierungsrichtlinie angegebenen Verfahren zur Identitätsfeststellung und Authentikation mit.

- Der Zertifikatsinhaber ist verpflichtet, seinen privaten Schlüssel angemessen zu schützen. Dies umfasst insbesondere keinen Zugriff durch unautorisierte Personen auf den privaten Schlüssel, sei er auf der trust|mark Karte oder auf einem anderen digitalen Medium (wie z. B. Festplatte eines Rechners) gespeichert, zuzulassen und, wenn es Aktivierungsdaten (PIN) des privaten Schlüssels gibt, diese nicht weiterzugeben.

- Falls nötig initiiert der Zertifikatsinhaber eines trust|mark|token Zertifikats unverzüglich die Sperre seines Zertifikats. Wird die Sperre nicht nach einem vorgegebenen Zeitraum aufgehoben, so erfolgt automatisch ein Widerruf des Zertifikats. Für alle Arten von trust|mark Zertifikaten kann der Zertifikatsinhaber einen 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 Zertifikatsinhaber ist verpflichtet, die jeweiligen nationalen Ausfuhrbestimmungen sowie etwaige nationale Nutzungsbeschränkungen bei einer Verwendung im Ausland zu beachten.

2.1.4 Verpflichtungen der Zertifikatsnutzer

Die Zertifikatsnutzer von trust|mark 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, die zur Veröffentlichung freigegeben sind,

- 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 im Falle von trust|mark|token und trust|mark|vsc Zertifikaten einander bei der Verwendung der von A-Trust bereitgestellten oder als geeignet bezeichneten Produkte und Verfahren in komplementärer Weise entsprechen,
- das Zertifikat bei Vorliegen der Voraussetzungen (siehe Kapitel 4.3.1) unverzüglich widerrufen wird und ein Widerrufsdienst verfügbar ist,
- sie die Anforderungen des Signaturgesetzes an Anbieter von Zertifizierungsdiensten erfüllt,
- sie die X.509-Standards einhält,
- die Abläufe, die in der gegenständlichen Zertifizierungsrichtlinie beschrieben sind, einhält.

A-Trust kann in den Zertifikaten eine Haftungsobergrenze festlegen. Ist ein solches Transaktionslimit im Zertifikat enthalten, haftet A-Trust nur bis zu diesem Betrag. Wenn kein Betrag angegeben ist, liegt keine Haftungsbeschränkung vor.

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

Die Zertifizierungsstelle haftet für die Registrierungsstellen.

2.2.2 Haftung der Registrierungsstelle

Die Zertifizierungsstelle haftet für die Registrierungsstellen.

2.3 Finanzielle Verantwortung

2.3.1 Schadensersatz der beteiligten Parteien

Keine Bestimmungen.

2.3.2 Treuhänderische Beziehungen

Keine Bestimmungen.

2.3.3 Administrative Prozesse

Keine Bestimmungen.

2.4 Auslegung und (gerichtliche) Durchsetzung

2.4.1 Zugrunde liegende Gesetzesbestimmungen

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

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

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

Änderungen der Allgemeinen Geschäftsbedingungen wie der Zertifizierungsrichtlinie werden dem Signator vor der Zertifikatserneuerung schriftlich mitgeteilt. Ändert A-Trust die Allgemeinen Geschäftsbedingungen, so hat der Signator jederzeit die Möglichkeit zu kündigen. Widerspricht der Signator den geänderten Allgemeinen Geschäftsbedingungen nicht binnen eines Monats, so gelten diese als akzeptiert.

2.4.3 Schlichtungsverfahren

Keine Bestimmungen.

2.5 Gebühren

Die aktuell gültige Gebührenregelung findet sich in der Entgeltregelung. Alle Entgelte, die nicht im Grundentgelt enthalten sind, werden mit der Nutzung der jeweiligen Leistung fällig.

2.5.1 Ausgabe und Erneuerung von Zertifikaten

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

2.5.2 Abrufen von Zertifikaten

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

2.5.3 Sperre oder Widerruf von Zertifikaten

Die Sperre oder der Widerruf eines Zertifikats ist kostenfrei.

2.5.4 Abrufen von Statusinformationen

Der Zugang zu 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:	www.a-trust.at/
Verzeichnisdienst:	ldap.a-trust.at/
Widerrufliste:	ldap.a-trust.at/
OCSP:	ocsp.a-trust.at/

Tabelle 1 A-Trust Homepage und Verzeichnisdienste

2.6.2 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 A-Trust 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 A-Trust CA-Zertifikat ist unter

- http://www.a-trust.at/certs/TrustMark-VSC-nnx.crt
  für trust|mark|vsc Zertifikate

- http://www.a-trust.at/certs/TrustMarkToken-Enc-nnx.crt
  für an trust|sign oder trust|mark Karten gebundene trust|mark Encryption Key-Zertifikate

- http://www.a-trust.at/certs/TrustMarkToken-Sig-nnx.crt
  für an trust|mark Karten gebundene trust|mark Signature Key-Zertifikate

- http://www.a-trust.at/certs/TrustMark-WebServer-nnx.crt
  für trust|mark|server Zertifikate für Webserver

- http://www.a-trust.at/certs/TrustMark-SigServer-nnx.crt
  für trust|mark|server Zertifikate für Signaturserver

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

Über die A-Trust 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=TrustMark-VSC-nn,o=A-Trust,c=AT?certificaterevocationlist?
  für trust|mark|vsc Zertifikate

- ldap://ldap.a-trust.at/ou=TrustMarkToken-Enc-nn,o=A-Trust,c=AT?certificaterevocationlist?
  für an trust|sign oder trust|mark Karten gebundene trust|mark Encryption Key-Zertifikate

- ldap://ldap.a-trust.at/ou=TrustMarkToken-Sig-nn,o=A-Trust,c=AT?certificaterevocationlist?
  für an trust|mark Karten gebundene trust|mark Signature Key-Zertifikate

- ldap://ldap.a-trust.at/ou=TrustMark-WebServer-nn,o=A-Trust,c=AT?certificaterevocationlist?
  für trust|mark|server Zertifikate für Webserver

- ldap://ldap.a-trust.at/ou=TrustMark-SigServer-nn,o=A-Trust,c=AT?certificaterevocationlist?
  für trust|mark|server Zertifikate für Signaturserver

(-nn bezeichnet die Versionsnummer der A-Trust Zertifizierungsstelle, z. B. ou=TrustMarkToken-Sig-01).

Darüberhinaus kann die aktuelle CRL von der A-Trust 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 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 des A-Trust-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 (im Falle von trust|mark|token Zertifikaten) 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 ausgestellten und veröffentlichten Zertifikaten sowie die 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.

3.1.1.1 trust|mark|token Zertifikat

Es sind folgende Daten aufzunehmen:

- Name für das Zertifikat: Nachname und Vorname sind erforderlich.
  Alternativ kann auch ein Pseudonym gewählt werden (Details zum Namen des Zertifikatsinhabers siehe Abschnitt 7.1.2.1). Der korrekte und vollständige Name muss der Registrierungsstelle und der Zertifizierungsstelle auch bei Verwendung eines Pseudonyms bekannt sein.
- 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-Mail-Adresse ist optional und wird, wenn vorhanden, in die Zertifikatserweiterungen aufgenommen.

3.1.1.2 trust|mark|vsc Zertifikat

Es sind folgende Daten aufzunehmen:

- Name für das Zertifikat: Nachname und Vorname sind erforderlich.
  Die Verwendung eines Pseudonyms ist nicht vorgesehen, sondern es muss sich der vollständige Name im Zertifikat befinden (Details zum Namen des Zertifikatsinhabers siehe Abschnitt 7.1.2.2).
- Die Angabe der postalischen Adresse des Zertifikatsinhabers ist erforderlich.

- Die Angabe einer E-Mail-Adresse ist aus Gründen der Bestellabwicklung und Authentikation erforderlich. Sie bildet einen obligatorischen Teil des Namens des Zertifikatsinhabers (siehe Abschnitt 7.1.2.2). Eine weitere optionale E-Mailadresse kann ebenfalls angegeben werden und wird in die Zertifikatserweiterungen aufgenommen.

- Aus Abwicklungsgründen muss zusätzlich die Telefonnummer des Antragstellers mitgeteilt werden.

3.1.1.3 trust|mark|server Zertifikat

Es sind folgende Daten aufzunehmen:

- Name für das Zertifikat:
  bei Webserverzertifikat: der Name des Servers (vollständiger Domainname des Servers, für den das Serverzertifikat beantragt wird)
  bei Signaturserverzertifikat: der Name des zertifizierten Schlüssels, wird aus der Organisation bzw. deren Kurzform, einer Kennung des Schlüssels (Sig, Enc) und einem für die Organisation eindeutigen Ordnungsbegriff gebildet.

- Der Name der Organisation (vollständiger Name z. B. lt. Firmenbucheintrag oder Abkürzung) ist erforderlich.

- Das Land des Sitzes der Organisation wird ebenfalls in den eindeutigen Namen (Distinguished Name) des Zertifikats aufgenommen.

- Name der Organisationsuntereinheit (Abteilung etc.)
  nur bei Signaturserverzertifikat

- E-Mailadresse
  optional, nur bei Signaturserverzertifikat,
  unabhängig davon muss für die Zustellung des Signaturserverzertifikats jedenfalls eine E-Mailadresse angegeben werden.

3.1.2 Anforderungen an die Namen

Der vollständige Name wird bei trust|mark|token Zertifikaten laut vorgelegtem Dokument erfasst.

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

Das verwendete Pseudonym darf weder anstößig noch offensichtlich zur Verwechslung mit Namen oder Kennzeichen geeignet sein.

3.1.3 Regeln zur Interpretation unterschiedlicher Namensformen

Keine Bestimmungen.

3.1.4 Eindeutigkeit der Namen

Jeder Inhaber eines trust|mark|token 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.

Die Eindeutigkeit des Namens eines Inhabers eines trust|mark|vsc Zertifikats ergibt sich aus der Kombination von E-Mailadresse, Vorname und Zuname.

Der Name eines Inhabers eines trust|mark|server Zertifikats ist je nach Zertifikat (Webserver oder Signaturserver) durch die Kombination aus Organisationsname und anderen Namen (wie z. B Domain, Abteilungsname, eindeutiger Schlüsselkennung, E-Mailadresse) eindeutig gestaltet.

3.1.5 Anspruch auf Namen und Beilegung von Streitigkeiten

Keine Bestimmungen.

3.1.6 Anerkennung, Bestätigung und Bedeutung von Warenzeichen

Keine Bestimmungen.

3.1.7 Methode zum Beweis des Besitzes des geheimen Schlüssels

3.1.7.1 trust|mark|token Zertifikat

Die trust|mark Karte wird mit je einem generierten Schlüsselpaar für die Signatur und die Verschlüsselung an den Zertifikatsinhaber übergeben. Somit ist kein Beweis des Besitzes eines zum öffentlichen Schlüssel gehörenden privaten Schlüssels er-

forderlich. Für das auf der trust|sign Karte befindliche Geheimhaltungsschlüsselpaar gilt dasselbe.

3.1.7.2 trust|mark|vsc Zertifikat

Das von der Registrierungsstelle generierte Schlüsselpaar wird zusammen mit dem Zertifikat in verschlüsselter Form per E-Mail an den Zertifikatsinhaber gesandt. Damit ist gewährleistet, dass der Zertifikatsinhaber im Besitz des zum öffentlichen Schlüssel gehörigen privaten Schlüssels ist.

Die Registrierungsstelle löscht das erstellte Schlüsselpaar nach dem Absenden an den Zertifikatsinhaber und gewährleistet damit die Rechte des Zertifikatsinhabers auf die Einzigartigkeit der Schlüsselverwaltung.

3.1.7.3 trust|mark|server Zertifikat

Der Antragsteller generiert das Schlüsselpaar mit der Serversoftware oder einem an den Server angeschlossenen Hardware Security Modul in ein und demselben Arbeitsschritt zusammen mit der Erstellung des Zertifikatsrequests, welcher im Anschluss an A-Trust gesandt wird. Somit ist gesichert, dass der zum zertifizierten öffentlichen Schlüssel gehörige private Schlüssel sich im Besitz des Antragstellers befindet.

3.1.8 Authentisierung von Organisationen

Für die Bestellung eines trust|mark|server Zertifikats muss die bestellende Organisation überprüft werden. Wenn die Antrag stellende Organisation eine ins österreichische Firmenbuch bzw. ins European Business Register (EBR) eingetragene Firma ist, so erfolgt die Überprüfung durch A-Trust mittels Online-Abfrage des Firmenbuchs bzw. des EBR. Die Firmenbuch- bzw. EBR-Nummer muss in diesem Fall bei der Antragstellung angegeben werden. Wenn die Antrag stellende Organisation kein registriertes Unternehmen ist, dann erfolgt die Überprüfung mittels Vorlage einer Kopie eines Dokumentes, aus welchem hervorgeht, dass die Organisation tatsächlich existiert. Das kann ein aktueller (nicht älter als drei Monate) Auszug aus einem zuständigen amtlichen Register bzw. vergleichbare Dokumente sein. Darüber hinaus kann die Überprüfung auch anhand von Datenbanken vertrauenswürdiger Dritter erfolgen.

Über die Rechtmäßigkeit der Verwendung der Domain informiert sich A-Trust durch Abfrage der Datenbank der zuständigen Registrierungsorganisation (z. B. www.nic.at, www.denic.de, etc.).

3.1.9 Authentisierung von Individuen

3.1.9.1 Zertifikate der trust|mark Karte und Verschlüsselungszertifikat der trust|sign -Karte

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. Dabei sind Personalausweis, Reisepass, Identitätskarte oder Führerschein zulässig. Für Ausländer werden nur gültige Reisepässe in deutscher oder englischer Sprache oder beglaubigte Abschriften zugelassen.

3.1.9.2 trust|mark|vsc Zertifikat

Zum Beweis seiner Identität gibt der Antragsteller mit der Bestellung seine E-Mailadresse und Telefonnummer an. Nach Aufforderung per E-Mail ruft er bei der Registrierungsstelle an, worauf er von dieser zurückgerufen wird. Damit ist die Identität mit dem Antragsteller geprüft und die Angaben für das Zertifikat können telefonisch abgeglichen werden.

3.1.9.3 trust|mark|server Zertifikat

Die Personen, die überprüft werden, sind der Antragsteller (z. B. Serveradministrator) und eine zeichnungsberechtigte Person. Von beiden muss eine Ausweiskopie eines gültigen, amtlichen Lichtbildausweises an A-Trust übermittelt werden. Dabei sind Personalausweis, Reisepass, Identitätskarte oder Führerschein zulässig. Für Ausländer werden nur gültige Reisepässe in deutscher oder englischer Sprache oder beglaubigte Abschriften zugelassen.

Wenn die zeichnungsberechtigte Person nicht im Firmenbuch oder EBR genannt ist, dann muss die Organisation zusätzlich einen Nachweis über die Zeichnungsberechtigung an A-Trust übermitteln.

3.2 Erneute Registrierung/Rezertifizierung

3.2.1 trust|mark|token Zertifikat

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 Inhabers eines Kartenzertifikats wird dabei nicht verändert.

3.2.2 trust|mark|vsc Zertifikat

Im Falle von trust|mark|vsc Zertifikaten muss vor der Bestellung eines neuen Zertifikats das ursprüngliche Zertifikat widerrufen werden.

3.2.3 trust|mark|server Zertifikat

Mit der Bestellung eines trust|mark|server Zertifikats wird ein unbefristeter Vertrag mit A-Trust abgeschlossen. Daher wird von A-Trust automatisch vor Ablauf der Gültigkeitsdauer eines trust|mark|server Zertifikats ein neues Zertifikat wiederum mit der Laufzeit gem. Kapitel 6.3.2 ausgestellt. Berücksichtigt werden dabei nur aktive Zertifikate, d. h. solche, die nicht widerrufen sind. Wenn ein Zertifikatsinhaber keine automatische Verlängerung wünscht, so muss das bis spätestens einen Monat vor Ablauf der Gültigkeitsdauer schriftlich an A-Trust mitgeteilt werden. Die Tatsache wird in einer A-Trust Datenbank vermerkt, sodass das Zertifikat ohne Verlängerung abläuft.

Zum Zweck der Verlängerung wird der gespeicherte PKCS#10-Request herangezogen und daraus das neue Zertifikat erstellt. Es enthält mit Ausnahme der Gültigkeitsdauer und der Zertifikatsseriennummer dieselben Daten wie das ursprüngliche Zertifikat und basiert auf demselben Schlüsselpaar.

Wenn die Organisation ihren Schlüssel zu ändern wünscht, dann muss zeitgerecht ein PKCS#10-Request mit neuem Public Key an A-Trust übermittelt werden. Dieser Request wird wiederum von A-Trust für die Verlängerung der Gültigkeitsdauer aufbewahrt, bis der Antragsteller wieder einen neuen Request übermittelt.

Die Existenz der Domain und ihre unveränderte Zugehörigkeit zur Organisation, die den Antrag gestellt hat, wird von A-Trust anlässlich der Verlängerung erneut überprüft.

A-Trust empfiehlt den Zertifikatsinhabern die Möglichkeit des Schlüsselwechsels regelmäßig in Anspruch zu nehmen.

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 Inhaber eines trust|mark|token Zertifikats 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 Inhaber eines trust|mark|server Zertifikats kann sein Zertifikat per Telefon oder in Ausnahmefällen per Einschreiben widerrufen lassen.

Der Inhaber eines trust|mark|vsc Zertifikats kann sein Zertifikat mittels eines Telefonanrufs widerrufen lassen.

3.4.1 trust|mark|token Zertifikat

Der Karteninhaber muss zumindest seinen Vor- und Zunamen und das Passwort für Sperre, Sperraufhebung 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 oder einer Sperraufhebung das Passwort vergessen wurde, kann der Karteninhaber sein Passwort mit Ausweisleistung in der Registrierungsstelle erfragen. Anstelle eines Widerrufs kann er eine Sperre beantragen, die ohne Passwortangabe möglich ist. Eine Sperraufhebung ist nur mit dem Passwort möglich.

3.4.2 trust|mark|vsc Zertifikat

Sperren sind bei trust|mark|vsc Zertifikaten nicht möglich, somit auch keine Sperraufhebungen.

Zur Durchführung eines Widerrufs muss der Zertifikatsinhaber bei trust|mark|vsc Zertifikaten seinen Vor- und Zunamen und, wenn nötig, die E-Mailadresse oder die Seriennummer seines Zertifikats angeben.

3.4.3 trust|mark|server Zertifikat

Sperren und Sperraufhebungen sind bei trust|mark|server Zertifikaten nicht möglich.

Der Widerruf eines trust|mark|server Zertifikats erfolgt mit einem Telefonanruf beim für die trust|mark|server Zertifikate zuständigen Widerrufsdienst von A-Trust. Beim Widerruf muss das bei der Antragstellung selbst gewählte Passwort für den Widerruf angegeben werden. Die für die Identifikation des Zertifikats anzugebenden Daten sind der DN (Organisationsname und Servername) oder auch die Zertifikatsnummer.

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

4 Betriebliche Anforderungen

4.1 Antrag auf Ausstellung von Zertifikaten

4.1.1 trust|mark|token Zertifikat

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.

4.1.2 trust|mark|vsc Zertifikat

Die Antragstellung erfolgt mittels eines elektronischen Formulars, wobei der Antragsteller die dazu notwendige Software installieren muss. Der Antrag wird an die Registrierungsstelle weitergeleitet.

Bei den für Behörden ausgestellten Zertifikaten kann der Antrag auch in Papierform an die Registrierungsstelle übermittelt werden.

Die PIN, welche zum Installieren des Zertifikats dient, wird dem Zertifikatsinhaber vom Registration Officer telefonisch mitgeteilt. Der Zertifikatsinhaber muss die PIN nach der Installation in einen selbst gewählten Wert ändern.

4.1.3 trust|mark|server Zertifikat

Die Antragstellung erfolgt mittels eines elektronischen Formulars auf der A-Trust Homepage.

Die Ausweiskopien und ggf. Bestätigungen sendet der Antragsteller per Fax an A-Trust.

4.2 Herausgabe und Akzeptanz von Zertifikaten

4.2.1 trust|mark|token Zertifikat

Die mit den Schlüsseln versehene trust|mark Karte (ebenso wie die trust|sign 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 Kunden muss dieser persönlich in der von ihm angegebenen Registrierungsstelle vorstellig werden. Der Registration Officer darf die Karte erst herausgeben, wenn

- er die Identität des Antragstellers anhand eines gültigen, amtlichen Lichtbildausweises (Personalausweis, Reisepass, Identitätskarte oder Führerschein) überprüft hat,
- der Antragsteller den 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.

4.2.2 trust|mark|vsc Zertifikat

Das fertig gestellte Zertifikat wird zusammen mit dem generierten Schlüsselpaar in einer von der Registrierungsstelle gem. PKCS#12 erstellten und verschlüsselten Datei per E-Mail an den Zertifikatsinhaber verschickt. Dieser installiert das Zertifikat und den Schlüssel unter Anwendung seiner PIN am PC.

Mit derselben E-Mail erhält der Zertifikatsinhaber einen Verweis zur A-Trust Homepage, wo er sich mit dem ebenfalls erhaltenen Passwort anmelden kann, um die erforderliche Software, den A-Trust Client, herunter zu laden. Diese Software wird zur Änderung der PIN und zur PIN-gesicherten Signaturerstellung und Entschlüsselung benötigt.

Die Vertragsbedingungen werden dem Zertifikatsinhaber auf elektronischem Weg bekannt gemacht.

4.2.3 trust|mark|server Zertifikat

Das fertig gestellte Zertifikat wird dem Zertifikatsinhaber auf elektronischem Weg zur Verfügung gestellt.

Bei Webserverzertifikaten gibt es dazu eine Suchfunktion auf der A-Trust Website, bei welcher der Domainname einzugeben ist. Das Ergebnis der Suche ist der Link zum Download des entsprechenden Zertifikats.

Zertifikate für Signaturserver werden dem Zertifikatsinhaber per E-Mail zugesandt.

4.3 Sperre und Widerruf von Zertifikaten

trust|mark|token Zertifikate können vorübergehend gesperrt werden. Diese Sperre kann auch, wenn sie nicht aufgehoben wird, in einen endgültigen Widerruf umgewandelt werden.

Ebenso ist für alle Arten von Zertifikaten 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 trust|mark Karte diese verloren hat bzw. sie wegen Funktionsuntüchtigkeit nicht mehr einsetzen kann,
- der private Schlüssel zu einem trust|mark|vsc oder trust|mark|server Zertifikat nicht mehr verwendet werden kann (z. B. Speichermedium defekt und keine Sicherung verfügbar),
- Verdacht auf eine Kompromittierung besteht (z. B. ein Unbefugter Zugriff auf den Rechner, auf dem sich der private Schlüssel befindet, hatte) bzw. eine Kompromittierung vorliegt,
- der Zertifizierungsstelle ein wesentlicher Verstoß des Zertifikatsinhabers gegen diese Richtlinien oder die Allgemeinen Geschäftsbedingungen bekannt wird,
- die Frist für die Aufhebung einer Sperre abläuft (nur bei trust|mark|token),
- das Vertragsverhältnis beendet wird,

- die eingesetzten Algorithmen nicht mehr den Sicherheitserwartungen entsprechen,
- es bei trust|mark|vsc Zertifikaten, die an Angehörige von Behörden ausgestellt wurden, Gründe gibt, die im Ermessen der zuständigen Behörde liegen,
- immer, bevor ein Inhaber eines trust|mark|vsc Zertifikats die Ausstellung eines neuen Zertifikats beantragt.

4.3.2 Wer kann einen Widerruf anordnen

Ein Widerruf eines Zertifikates kann angeordnet werden durch:

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

4.3.3 Prozedur für einen Widerrufsantrag

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

- trust|mark|token: Der Zertifikatsinhaber wendet sich per Telefon oder auch Fax an den Widerrufsdienst.
- trust|mark|vsc Zertifikat: Der Zertifikatsinhaber bzw. der Widerrufsberechtigte der Organisation, wenn es ein Zertifikat für den Angehörigen einer Behörde ist, wendet sich per Telefon oder auch Fax an den Widerrufsdienst.
- trust|mark|server Zertifikat: Der Zertifikatsinhaber ruft beim Widerrufsdienst an.

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 eines trust|mark|token oder eines trust|mark|server Zertifikats ist die Angabe des Passworts für den Widerruf verpflichtend. Beim Widerruf eines trust|mark|vsc Zertifikat ist die Angabe des Namens des Zertifikatsinhabers nötig.

Der Grund für den Widerruf (Kompromittierung des privaten Schlüssel, Defekt der Karte, 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 eines trust|mark|token oder eines trust|mark|vsc Zertifikats 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:

- trust|mark|token Zertifikat
  - Passwort für Sperre, Aufhebung und Widerruf: obligatorisch
  - Vor- und Nachname: 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.
- trust|mark|vsc Zertifikat
  - Vor- und Nachname: obligatorisch
  - E-Mailadresse
- trust|mark|server Zertifikat
  - Passwort für den Widerruf: obligatorisch
  - Organisationsname und Servername oder Zertifikatsnummer: obligatorisch

Hat der Inhaber eines trust|mark|token Zertifikats sein Passwort vergessen, ist ein Widerruf nicht möglich. Er kann statt dessen eine Sperre beantragen oder sein Passwort mit Ausweisleistung in einer Registrierungsstelle erfragen.

Wenn beim Widerruf eines trust|mark|server Zertifikats das Passwort nicht genannt werden kann, so kann der Widerruf per Einschreiben mit firmenmäßiger Zeichnung erfolgen.

4.3.4 Frist bis zur Bekanntgabe des Widerrufs

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

Der Widerrufsdienst für trust|mark|server Zertifikate ist zu den auf der A-Trust Homepage angegebenen Geschäftszeiten erreichbar.

Der Widerrufsdienst für trust|mark|vsc und trust|mark|token 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 in einen Widerruf umgewandelt.

4.3.6 Wer kann eine Sperre anordnen und aufheben

Eine Sperre und deren Aufhebung können nur bei trust|mark|token Zertifikaten beantragt werden.

Die bevollmächtigten Personen für eine Sperre oder Sperraufhebung 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 eines trust|mark|token Zertifikats wie folgt veranlasst werden: Der Zertifikatsinhaber wendet sich per Telefon an den Widerrufsdienst.

Für die Sperre eines trust|mark|token Zertifikats ist die Angabe des Passworts 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: 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.

4.3.8 Sperraufhebung

Innerhalb der Sperrperiode (siehe Kapitel 4.3.9) kann der Inhaber eines trust|mark|token Zertifikats die Sperre des Zertifikats wieder aufheben. Dazu muss er die Sperraufhebung beim Widerrufsdienst telefonisch beantragen.

Für die Identifikation und die erforderlichen Daten des Zertifikatsinhabers und des Zertifikats gelten dieselben Regeln wie beim Widerruf.

Hat der Zertifikatsinhaber sein Passwort vergessen, ist eine Sperraufhebung nicht möglich. Er muss in diesem Fall sein Passwort mit Ausweisleistung in einer Registrierungsstelle erfragen und dann den Widerrufsdienst kontaktieren.

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

4.3.9 Grenzen einer Sperrperiode

Die Sperre eines trust|mark|token Zertifikates kann bis 22:00 Uhr des zweiten auf den Tag der Sperre folgenden Werktags wieder aufgehoben werden, sonst wird sie durch A-Trust 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), sollten keine Zertifikate akzeptiert werden. 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 trust|mark Karte lässt der Zertifikatsinhaber diese sperren. Sollte zugleich auch die zugehörige PIN nicht mehr verfügbar oder sicher sein, führt der Zertifikatsinhaber einen Widerruf durch.

Bei einem trust|mark|vsc Zertifikat beantragt der Zertifikatsinhaber einen Widerruf, wenn er Grund zur Annahme hat, dass sein auf dem PC befindlicher privater Schlüssel kompromittiert wurde oder der PC von einem Unbefugten in Betrieb genommen und gleichzeitig seine PIN unberechtigten Personen bekannt wurde.

Wenn bei einem trust|mark|server Zertifikat der Verdacht auf Kompromittierung besteht, muss der Zertifikatsinhaber einen Widerruf beantragen.

4.4 Protokollierung sicherheitsrelevanter Ereignisse

4.4.1 Protokollierte Ereignisse

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

- Ab- und Anschalten von Systemen,
- Änderungen der Hardwarekonfiguration,
- Einrichtung oder Schließung von Berechtigungen,
- Änderungen bei der Rollenaufteilung (siehe Abschnitt 5.2),
- Änderung der Softwarekonfiguration (Installation oder Update von Software),

Weiterhin werden alle mit den Systemen durchgeführten Transaktionen zusammen mit Transaktionstyp, Zeitpunkt und Informationen darüber, ob die Transaktion abge-

schlossen 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 Kunden,
- Akzeptanzerklärung der Allgemeinen Geschäftsbedingungen und der Entgeltbestimmungen durch den Kunden 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, Cross-Zertifikate und Zertifikate der Zertifikatsinhaber),
- Sperr- und Widerrufanträge mit Datum und Uhrzeit des Eintreffens (inklusive entsprechender Protokolldateien),

- Alle ausgestellten Widerrufslisten,
- Datum und Uhrzeit der Veröffentlichung der Zertifikate und Widerrufslisten (inklusive entsprechender Protokolldateien) und
- Datum und Uhrzeit von Schlüsselwechseln der Zertifizierungsstelle.

4.5.2 Aufbewahrungszeiten

Die Aufbewahrungszeit beträgt mindestens sieben Jahre. Es sind folgende Aspekte zu berücksichtigen:

- Die Daten müssen mindestens so lange aufbewahrt werden, wie sie für die Wiederherstellung bei Ausfall von Systemkomponenten im Anwendungszeitraum benötigt werden.
- Insbesondere bei Anwendung digitaler Signaturen sind die Daten mindestens so lange aufzubewahren, wie die digital signierten Dokumente nachprüfbar gehalten werden.
- 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 sollte oder aber im Falle einer Kompromittierung von Schlüsseln. In letzterem Fall ist unbedingt ein Widerruf der betroffenen Zertifikate erforderlich.

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

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

lauf der im Zertifikat festgelegten Gültigkeitsdauer zum Nachprüfen von Zertifikaten eingesetzt werden.

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

4.7 Kompromittierung und Notfallplan

4.7.1 Rechner, Software und/oder Daten sind korrumpiert

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

Bei Zertifikaten sind die betroffenen Zertifikatsinhaber zu informieren. Es erfolgt eine unmittelbare Sperre der betroffenen Zertifikate, falls sich im Zertifikat fehlerhafte Angaben befinden.

Bei Fehlern in einer Widerrufsliste wird umgehend eine korrekte Widerrufsliste ausgestellt. Falls eine sichere, unmittelbare Ausstellung der Widerrufsliste nicht möglich ist und die Fehler sicherheitskritisch sind, werden die Verzeichnisdienste abgeschaltet, die die Widerrufsliste veröffentlichen, um eine weitere Verbreitung zu verhindern. Die Wiederaufnahme des Dienstes ist mit der Veröffentlichung der neuen Widerrufsliste verbunden. In Abhängigkeit der Fehler und der Ausfallzeit der Verzeichnisdienste werden die Anwender informiert.

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

4.7.2 Widerruf von Zertifikaten zu Zertifizierungsstellen- und Dienste-Schlüsseln

Zertifikate der Zertifizierungsstelle werden widerrufen:

- bei Kompromittierung oder Verdacht auf Kompromittierung der entsprechenden Schlüssel,

- wenn die eingesetzten Algorithmen nicht mehr den Sicherheitserwartungen entsprechen und dadurch eine sichere Anwendung nicht mehr gegeben wäre,

- bei Einstellung der Tätigkeit der Zertifizierungsstelle, wobei die Widerrufsliste oder Dienste zur Statusauskunft nicht weiter gepflegt werden.

Ist der Grund für den Widerruf des Zertifikats Kompromittierung oder der Verdacht auf Kompromittierung des zugehörigen privaten Schlüssels, dann ist insbesondere Abschnitt 4.7.3 zu berücksichtigen. Bei Widerruf des Zertifikats wegen Einstellung der Tätigkeit der Zertifizierungsstelle ist Abschnitt 4.8 zu beachten.

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

Private Schlüssel der Zertifizierungsstelle, deren zugehörige Zertifikate widerrufen wurden, werden nicht weiter durch die Zertifizierungsstelle eingesetzt. Diese privaten Schlüssel werden entsprechend Abschnitt 6.2.9 vernichtet.

4.7.2.1 Widerruf von Zertifikaten der Dienste

Werden Zertifikate der Dienste der Zertifizierungsstelle widerrufen, so werden die Dienste ohne gültigen Schlüssel umgehend aus dem Betrieb genommen. Dadurch wird verhindert, dass die Anwender Dienste nutzen, deren Signaturen ungültig sind. Die widerrufenen Schlüssel werden durch neue Schlüssel ersetzt. Die Dienste werden erst wieder in Betrieb genommen, wenn die neuen, gültigen Schlüssel installiert wurden.

4.7.2.2 Widerruf des Zertifikats der Zertifizierungsstelle

Wird ein Zertifikat der Zertifizierungsstelle 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 Aktionen. Wenn bedingt durch die Auswirkungen der Katastrophe übliche Verfahren, wie Widerruf oder das Anbieten von Informationen über E-Mail oder Web-Seite nicht möglich sind, dann werden verstärkt alternative Verfahren wie der Postweg zur Verbreitung der notwendigen Informationen eingesetzt.

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

4.8 Einstellung der Tätigkeit der Zertifizierungsstelle

Einstellung der Tätigkeit bedeutet, dass die kompletten Dienstleistungen (Ausnahme: Zugriff auf archivierte Daten) der Zertifizierungsstelle nicht weiter angeboten werden. Organisatorische Umstellungen oder Wechsel der Schlüssel der Zertifizierungsstelle sind hiervon nicht betroffen.

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

Rechtzeitig vor der endgültigen Einstellung der Zertifizierungsstelle werden alle noch gültigen und von der Zertifizierungsstelle ausgestellten Zertifikate widerrufen. Alle von den Widerrufen betroffenen Zertifikatsinhaber werden vom Widerruf ihres Zertifikates informiert.

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

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

5 Physische, verfahrensorientierte und personelle Sicherheitsvorkehrungen

5.1 Physische Sicherheitsvorkehrungen

5.1.1 Standort und örtliche Gegebenheiten

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

Dienstleistung	Adresse
Firmensitz	A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH. Landstraßer Hauptstraße 5 A-1030 Wien
Registrierung Widerrufsdienst	Die Registrierungsstellen und den Widerrufsdienst von A-Trust finden Sie auf der Web-Seite der A-Trust 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
- CD-ROMs
- Magnetbänder
- Festplatten

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

5.1.7 Müllentsorgung

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

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

5.1.8 Redundante Auslegung

Der gesamte Betrieb im Rechenzentrum ist redundant ausgelegt, so dass eine Hochverfügbarkeit (7 x 24 Stunden) des Rechenzentrumsbetriebs erreicht werden kann.

5.2 Verfahrensorientierte Sicherheitsvorkehrungen

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

5.2.1 Funktionen der A-Trust

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

Tabelle 3 Funktionen der A-Trust

5.2.2 Sicherheitskritische Funktionen

Rolle	Funktion
Sicherheitsbeauftragter	siehe Tabelle 3
Revision	siehe Tabelle 3
Datenschutz	siehe Tabelle 3
Security Officer (SO)	Zutritt in die Hochsicherheitszone Verantwortlichkeit für die Generierung und Zertifizierung der Schlüssel von A-Trust und Widerruf dieser Zertifikate Verwaltung der Hardware Security Module Vergabe der RO- und RCA-Berechtigung Ansprechpartner für sicherheitsrelevante Fragen Beaufsichtigung der Einhaltung der im CPS festgelegten Vorgehensweisen
Sicherheitssystemadministrator	Zutritt in die Hochsicherheitszone Beaufsichtigung von Systemadministrator und Systemoperator
Kartenproduzent-Initialisierer	Initialisieren der Karten auf der Initialisierungsanlage
Kartenproduzent-Personalisierer	Personalisieren der Karten auf der Personalisierungsanlage
Revocation Center Agent (RCA), Mitarbeiter im Widerrufsdienst	Ansprechpartner für die Zertifikatsinhaber hinsichtlich der Annahme von Anträgen für Sperre, Widerruf und Aufhebung von Sperren Durchführung der Umwandlung einer Sperre in einen Widerruf
Registration Officer (RO), Mitarbeiter der Registrierungsstelle	Entgegennahme von Zertifikatsanträgen, Änderungsanträgen und Nachdruckaufträgen. Identifikation von Zertifikatswerbern im Rahmen der Registrierung und der Bekanntgabe des Widerrufspasswortes 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.
Systemoperator	Laufende Systembetreuung, Datensicherung und –wieder-herstellung 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 Vier-augenprinzip 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, RO	Nein	Nein
Widerrufen von Anwenderzertifikaten	RCA, RO	Nein	Nein
Aufheben einer Sperre von Anwender-zertifikaten	RCA, RO	Nein	Nein
Umwandeln einer Sperre in einen Widerruf	RCA	Nein	Nein

Tätigkeit	Personen	Vier-augen-prinzip	Hoch-sicher-heit
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
Löschen der A-Trust Schlüssel für A-Trust Root-CA und Zertifizierungsstellen	SO, SO	Ja	Ja
Zertifizierung für die A-Trust Root-CA und die Zertifizierungsstellen	SO, SO	Ja	Ja
Widerruf von Zertifikaten der CA	SO, SO	Ja	Ja
Vergabe der Berechtigungen für RO und RCA	SO, SO	Ja	Ja
Inbetriebnahme eines kryptographischen Moduls (Signaturerstellungseinheit der A-Trust CA)	SO, SO	Ja	Ja
Ab- und Anschalten von Komponenten, insbesondere Verzeichnisdiensten	Sicherheitssystemadministrator	Nein	Nein
Austausch von Hardware-Komponenten	Sicherheitssystemadministrator, Sicherheitssystemadministrator	Ja	Ja
Austausch von Software-Komponenten	Sicherheitssystemadministrator, Sicherheitssystemadministrator	Ja	Ja
Überprüfung von Protokolldateien auf verdächtige Vorkommnisse	Systemadministrator	Nein	Nein
Überprüfung der Protokolldateien auf Manipulation	Systemadministrator	Nein	Nein
Anfertigung eines Backups der Protokolldateien und Lagerung desselben	Sicherheitssystemadministrator, Sicherheitssystemadministrator	Ja	Ja
Qualitätsprüfung der verwendeten Schlüssellängen und Parameter zur Schlüsselerzeugung	SO	Nein	Nein

Tätigkeit	Personen	Vier-augen-prinzip	Hoch-sicher-heit
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 trust|mark|vsc, trust|mark|token und Signaturserver 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 Schlüssel der Zertifizierungsstelle zur Signatur von Webserver Zertifikaten werden auf Softwarebasis generiert. Von diesen geheimen Schlüsseln können Backups erzeugt werden.

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 Entschlüsselungsschlüssel, welche sich im Chip der 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 trust|mark Karte erfolgt im Hochsicherheitsbereich des Kartenherstellers. Die Schlüssel werden in trust|mark Karten erzeugt, auf welche anschließend die persönlichen Daten des zukünftigen Zertifikatsinhabers 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.

Die Schlüssel der Inhaber von trust|mark|vsc Zertifikaten werden in der Software der Registrierungsstelle mit einem Algorithmus gem. ANSI X9.17 generiert. Die dazu erforderlichen Zufallsdaten werden per Mausbewegung erzeugt. Der öffentliche Schlüssel wird in einem Zertifikatsantrag an A-Trust übermittelt. A-Trust sendet das fertig gestellte Zertifikat an die Registrierungsstelle, die dann das Schlüsselpaar und das Zertifikat in einem PKCS#12-File an den Zertifikatsinhaber schickt.

Die Schlüssel der Inhaber von trust|mark|server Zertifikaten werden von diesen selbst mit Hilfe ihrer Serversoftware erzeugt. A-Trust erhält keine Kenntnis der

privaten Schlüssel. Die Zertifikate werden von der A-Trust Zertifizierungsstelle aufgrund des vom Antragsteller erzeugten PKCS#10-Requests erstellt.

6.1.2 Auslieferung privater Schlüssel an Zertifikatsinhaber

6.1.2.1 trust|mark|token Zertifikat

Die privaten Schlüssel werden in der trust|mark bzw. trust|sign Karte an den Zertifikatsinhaber ausgeliefert. Der Zertifikatsinhaber versichert sich bei der Übernahme der Karte in der RA, dass die Karte nicht offensichtlich beschädigt ist.

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

6.1.2.2 trust|mark|vsc Zertifikat

Der Zertifikatsinhaber erhält seinen privaten Schlüssel in verschlüsselter Form an seine bestätigte E-Mail-Adresse zugesandt. Der Zugriff auf diesen Schlüssel zum Zweck der Installation im Browser des Anwender-PCs ist nur mit einer telefonisch an den Zertifikatsinhaber mitgeteilten PIN möglich.

Die Benutzung des privaten Schlüssels kann aufgrund der Verwendung des A-Trust Client ebenfalls nur durch die korrekte Eingabe der PIN erfolgen.

6.1.2.3 trust|mark|server Zertifikat

Eine Auslieferung privater Schlüssel wird nicht durchgeführt, da die Schlüssel im Server, für den die Zertifikate ausgestellt werden, generiert werden und A-Trust keinen Zugriff auf die privaten Schlüssel erhält.

6.1.3 Auslieferung öffentlicher Schlüssel an die Zertifikatsinhaber

6.1.3.1 Öffentliche Schlüssel der Zertifizierungsstelle

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

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

6.1.3.2 Öffentlicher Schlüssel des trust|mark|token Zertifikats

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

6.1.3.3 Öffentlicher Schlüssel des trust|mark|vsc Zertifikats

Der Zertifikatsinhaber erhält seinen öffentlichen Schlüssel zusammen mit dem privaten Schlüssel in verschlüsselter Form an seine bestätigte E-Mail-Adresse zugesandt.

6.1.3.4 Öffentlicher Schlüssel des trust|mark|server Zertifikats

Der Zertifikatsinhaber generiert sein Schlüsselpaar selbst und ist daher im Besitz des öffentlichen Schlüssels.

6.1.4 Schlüssellängen

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

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

Die Schlüssel der Zertifikatsinhaber von trust|mark|token und trust|mark|vsc Zertifikaten entsprechen einer Länge von zur Zeit 1024 Bit (RSA-Schlüssel).

Den Zertifikatswerbern für Webserver Zertifikate wird empfohlen als Schlüssellänge 1024 Bit (RSA-Schlüssel) zu wählen. Mindestens aber muss die Schlüssellänge 512 Bit (RSA) betragen.

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

Als Hash-Algorithmus wird den Zertifikatsinhabern von trust|mark|token und trust|mark|vsc Zertifikaten die Verwendung von SHA-1 empfohlen.

Bei trust|mark|server Zertifikaten sind als Hash-Algorithmen SHA-1 bzw. MD5 möglich. Die Verwendung von SHA-1 wird den Zertifikatswerbern empfohlen.

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

6.1.5 Parameter zur Schlüsselerzeugung

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

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

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

und

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

gilt.

Der öffentliche Exponent e wird zufällig gewählt.

6.1.6 Qualitätsprüfung der Parameter

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

6.1.7 Hardware/Software Schlüsselerzeugung

Die Schlüssel der A-Trust Root und der A-Trust Zertifizierungsstellen für trust|mark|token, trust|mark|vsc und Signaturserver Zertifikate werden in einer speziellen Hardware erzeugt und dort auch eingesetzt. Die Schlüssel der A-Trust

Zertifizierungsstellen für Webserver Zertifikate werden in einer speziellen Software erzeugt.

Die Schlüssel der Zertifikatsinhaber, die sich auf Karten befinden, werden entweder in der trust|mark Karte selbst oder in einem Hardware Security Modul von A-Trust erzeugt.

Die Schlüssel der trust|mark|vsc Zertifikate werden durch die Software der Registrierungsstelle mit dem in Kapitel 6.1.1.2 beschriebenen Verfahren erzeugt.

Die Schlüssel der trust|mark|server Zertifikate werden durch den Antragsteller mittels der Server-Software oder einem dem Server angeschlossenen Hardware Security Modul erzeugt. Weder die Zertifizierungs- noch die Registrierungsstelle erhalten Kenntnis vom privaten Schlüssel des Zertifikatsinhabers.

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

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

6.1.8.1 Verwendung der Schlüssel der A-Trust Root

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

6.1.8.2 Verwendung der Schlüssel der A-Trust Zertifizierungsstellen

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

Deshalb werden die Bits

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

gesetzt.

6.1.8.3 Verwendung des Schlüssels des Zertifikatsinhabers

Im den Zertifikaten für die öffentlichen Signaturschlüssel von trust|mark Karten werden die folgenden Bits gesetzt:

- nonRepudiation
- digitalSignature

In den Zertifikaten für die Entschlüsselungsschlüssel von trust|mark und von trust|sign Karten werden die folgenden Bits gesetzt:

- digitalSignature
- keyEncipherment
- dataEncipherment.

Der zum trust|mark|vsc Zertifikat für Behörden gehörige Schlüssel dient nur zur Signatur von E-Mails weshalb das folgende Bits gesetzt ist:

- nonRepudiation.

Der Schlüssel für die anderen trust|mark|vsc Zertifikate dient zur Signaturerstellung und Geheimhaltung, weshalb die folgenden Bits gesetzt sind:

- digitalSignature
- keyEncipherment
- dataEncipherment.

Der zu einem Webserverzertifikat gehörige Schlüssel dient zur SSL-Verschlüsselung, weshalb in diesem Fall im trust|mark|server Zertifikat die folgenden Bits gesetzt sind:

- digitalSignature
- keyEncipherment.

Der zu einem Signaturserverzertifikat gehörige Signaturschlüssel dient zur Erstellung digitaler Signaturen, weshalb in diesem Fall im trust|mark|server Zertifikat das folgende Bit gesetzt ist:

- digitalSignature.

Der in einem Signaturserverzertifikat zertifizierte Verschlüsselungsschlüssel dient zum Zweck der Geheimhaltung, weshalb in diesem Fall im trust|mark|server Zertifikat die folgenden Bits gesetzt sind:

- keyEncipherment

- dataEncipherment.

6.2 Schutz der privaten Schlüssel

6.2.1 Schutz des Schlüssels der Zertifizierungsstelle

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

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

Für die Speicherung und Anwendung des privaten Schlüssels der A-Trust Root und der A-Trust Zertifizierungsstellen für trust|mark|token, trust|mark|vsc und Signaturserver Zertifikate werden nur Hardware Security Module eingesetzt, die einen angemessenen physikalischen Zugriffsschutz auf diese Schlüssel bieten.

Für die Speicherung und Anwendung des privaten Schlüssels der A-Trust Zertifizierungsstelle für Webserver Zertifikate wird der angemessene Zugriffsschutz mittels einer PIN gewährleistet.

6.2.2 Schutz der Schlüssel der Zertifikatsinhaber

Die Schlüssel der Zertifikatsinhaber werden entweder auf einer gesetzeskonformen Smartcard, die von A-SIT nach §18(5) [SigG] bescheinigt wurde, oder auf dem PC des Anwenders gespeichert. In beiden Fällen ist die Verwendung des privaten Schlüssels 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 A-Trust Root und der Zertifizierungsstelle für trust|mark|token, trust|mark|vsc und Signaturserver Zertifikate), in einem geschützten Bereich des Rechenzentrums (Schlüssel der Zertifizierungsstelle für Webserver Zertifikate), auf einer Chipkarte (Schlüssel der Zertifikatsinhaber mit trust|mark Karte) oder auf dem

Rechner des Zertifikatsinhabers unter dessen Kontrolle (Schlüssel der Zertifikatsinhaber von trust|mark|vsc oder trust|mark|server Zertifikaten).

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

6.2.4 Hinterlegung privater Schlüssel

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

6.2.5 Backup privater Schlüssel

Für private Schlüssel der A-Trust Root und der Zertifizierungsstelle für trust|mark|token, trust|mark|vsc und Signaturserver Zertifikate gibt es kein Backup. Bei privaten Schlüsseln der A-Trust Zertifizierungsstelle für Webserver Zertifikate ist ein Backup möglich.

6.2.6 Archivierung privater Schlüssel

Für private Schlüssel der Zertifizierungsstelle gibt es keine Archivierung. Eine Archivierung von Schlüsseln der Zertifikatsinhaber in verschlüsselter Form findet durch A-Trust im Falle der auf einer trust|mark oder trust|sign Karte befindlichen Verschlüsselungsschlüssel 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 trust|mark|token, trust|mark|vsc und Signaturserver Zertifikaten und Widerrufslisten werden in einem

Hardware Security Modul erzeugt und dort gespeichert. Die Anwendung erfolgt ebenfalls direkt im Hardware Security Modul.

Die privaten Schlüssel der Zertifizierungsstelle zum Signieren von Webserver Zertifikaten und Widerrufslisten sind in Software vorhanden und befinden sich nicht in einem Hardware Security Modul.

6.2.7.2 Schlüssel der Zertifikatsinhaber

Der private Signaturschlüssel des Zertifikatsinhabers, der sich auf der trust|mark Karte befindet, wird direkt in der trust|mark Karte generiert und ist vor dem Auslesen geschützt.

Der private Verschlüsselungsschlüssel des Zertifikatsinhabers, der sich auf einer trust|mark oder trust|sign Karte befindet, wird in einem Hardware Security Modul erzeugt und zur Wiederverwendung auf der nächsten Karte außerhalb des Security Moduls in verschlüsselter Form gespeichert.

Der zum trust|mark|vsc Zertifikat gehörige private Schlüssel des Zertifikatsinhabers, welcher sich nicht im Chip einer Karte befindet, wird in der Software der Registrierungsstelle erzeugt, auf der Festplatte des PCs des Zertifikatsinhabers gespeichert und weder in ein Hardware Security Modul eingebracht noch in einem solchen aufbewahrt.

Der private Schlüssel zu einem trust|mark|server Zertifikat befindet sich nur beim Zertifikatsinhaber und bleibt A-Trust unbekannt.

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 kartenbasierten Schlüssel der trust|mark|token Zertifikatsinhaber werden durch die korrekte Eingabe einer PIN aktiviert. Diese PIN ist jedes Mal vor der Erstellung einer Signatur oder der Durchführung einer Entschlüsselung einzugeben. Nach jeweils drei aufeinanderfolgenden Fehlversuchen ist die PIN gesperrt. Die PIN kann durch die korrekte Eingabe der PUK für drei weitere Versuche freigegeben werden. Dieser Vorgang kann maximal dreimal hintereinander wiederholt werden, denn wenn die Anzahl von drei PUK-Fehleingaben überschritten ist, ohne dazwischen eine korrekte PIN eingegeben zu haben, ist der PUK ebenfalls gesperrt.

Der in der Software vorhandene Schlüssel des trust|mark|vsc Zertifikatsinhabers benötigt eine PIN-Eingabe zum Zweck der Installation im A-Trust Client und in Folge für die Erstellung einer Signatur oder die Durchführung einer Entschlüsselung.

Die A-Trust Client Software ist per Download von der A-Trust „Members Area“ zu erhalten (siehe auch Kapitel 4.2.2).

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

trust|mark|vsc Zertifikate besitzen keine PIN Prüfungsapplikation, die die Anzahl der PIN-Fehlversuche begrenzt.

6.2.9 Methode zur Vernichtung privater Schlüssel

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

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

Für die Löschung der geheimen Schlüssel zu trust|mark|vsc und trust|mark|server Zertifikaten sind die Zertifikatsinhaber verantwortlich.

6.3 Weitere Aspekte zum Schlüsselmanagement

6.3.1 Archivierung öffentlicher Schlüssel

Siehe Abschnitt 4.6.

6.3.2 Verwendungszeitraum öffentlicher und privater Schlüssel

Als Gültigkeitsmodell wird das Kettenmodell eingesetzt. Zur Überprüfung der Gültigkeit eines Zertifikats wird dabei die übergeordnete Instanz herangezogen. Dabei muss das übergeordnete Zertifikat nur zum Zeitpunkt der Ausstellung des zu überprüfenden Zertifikats gültig gewesen sein. Ein übergeordnetes Zertifikat kann gesperrt 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
A-Trust Root-CA	3
A-Trust Zertifizierungsstellen	3
trust|mark|server	3
trust|mark|token	3
trust|mark|vsc	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 A-Trust Root-CA und der A-Trust Zertifizierungsstellen für trust|mark|token, trust|mark|vsc und Signaturserver Zertifikate 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.

Die Schlüssel der Zertifizierungsstelle für Webserver Zertifikate werden von einem Beauftragten mittels Eingabe einer PIN aktiviert.

6.4.1.2 Aktivierungsdaten für trust|mark|token Zertifikate

Die Zertifikatsinhaber aktivieren ihren privaten Schlüssel über eine PIN.

Die Initial (bzw. Transport)-PIN für den Signaturschlüssel der trust|mark Karte wird in einem Hardware Security Modul erzeugt. Die Zertifikatsinhaber erhalten diese mit der Benachrichtigung, dass ihre trust|mark 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 PIN ist eine Signatur möglich. Vor der Änderung und innerhalb von drei Monaten ab Kartenerstellung kann der Zertifikatsinhaber diese PIN nachdrucken lassen.

Die PIN für den Verschlüsselungsschlüssel der trust|mark und der trust|sign 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.

6.4.1.3 Aktivierungsdaten für trust|mark|vsc Zertifikate

Die Zertifikatsinhaber installieren ihr Zertifikat und die Schlüssel auf ihrem PC, in die Systemumgebung des A-Trust Client, mit einer alphanummerischen PIN, die von der Registrierungsstelle telefonisch mitgeteilt wird.

In Kombination mit dem A-Trust Client erfordert jede Signaturerstellung und Entschlüsselung die Eingabe dieser PIN. Dem Zertifikatsinhaber wird dringend empfohlen, die von der Registrierungsstelle mitgeteilte PIN auf einen selbst gewählten 2 bis 32 Stellen langen, alphanummerischen Wert (Groß- und Kleinschreibung wird unterschieden) zu ändern. Die PIN kann mittels A-Trust Client jederzeit vom Zertifikatsinhaber geändert werden. Sollte der Zertifikatsinhaber die PIN vergessen haben, so muss das Zertifikat widerrufen und ein neues beantragt werden.

6.4.2 Schutz der Aktivierungsdaten

6.4.2.1 Aktivierungsdaten für Schlüssel der Zertifizierungsstelle

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

6.4.2.2 Aktivierungsdaten für Schlüssel der 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 A-Trust CA-Zertifikate

Attribut	Inhalt	Erläuterung
Version	v3(2)	Die Versionsnummer wird auf „2“ gesetzt, um ein X.509 Zertifikat der Version 3 anzuzeigen
Seriennummer	Seriennummer des Zertifikats	Eindeutig innerhalb der A-Trust Zertifizierungsinfrastruktur
Algorithmus	SHA-1	Für die Signatur über das Zertifikat verwendeter Algorithmus
Aussteller des Zertifikats	CN = A-Trust-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 A-Trust 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 = TrustMarkToken-xxx-nn bzw. CN = TrustMark-xxx-nn OU = TrustMarkToken-xxx-nn bzw. OU = TrustMark-xxx-nn O = A-Trust C = AT	-xxx erhält den Wert Sig für Signaturschlüssel oder Enc für Encryption Key bzw. VSC für Virtual Smartcard bzw. WebServer oder Sigserver für Server Zertifikate -nn bezeichnet die Generation des zertifizierten Schlüssels
Öffentlicher Schlüssel	RSA 2048 Bit	Öffentlicher Schlüssel des Zertifikatsinhabers

Tabelle 8 Profil für CA-Zertifikat

7.1.2 Zertifikate für Zertifikatsinhaber

7.1.2.1 trust|mark|token 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 = TrustMarkToken-xxx-nn OU = TrustMarkToken-xxx-nn O = A-Trust C = AT	-xxx erhält den Wert Sig für Signaturschlüssel und Enc für Encryption Key -nn bezeichnet die Generation des Schlüssels, der von A-Trust für die Signatur des Zertifikats verwendet wurde. Bei jeder Ausstellung eines neuen A-Trust CA-Schlüssels wird diese Generationsnummer um eins erhöht.
Gültig von Gültig bis	Beginn und Ende der Gültigkeit des Zertifikats	Der Gültigkeitszeitraum beträgt höchstens drei Jahre
Zertifikatsinhaber	C = CountryName T = Title SN = SurName G = GivenName CN = CommonName Seriennummer = SerialNumber	CountryName: AT etc. Title: Titel (Dr. etc.) SurName: Zuname GivenName: Vorname CommonName: Vorname + Zuname Titel, Zuname, Vorname entfallen bei Verwendung eines Pseudonyms CommonName: entweder Vorname + Zuname oder Pseudonym (Codierung siehe Abschnitt 3.1.2) SerialNumber: eindeutige Identifikationsnummer des Zertifikatsinhabers: siehe auch Abschnitt 3.1.4
Öffentlicher Schlüssel	RSA 1024 Bit	Öffentlicher Schlüssel des Zertifikatsinhabers

Tabelle 9 Profil für trust|mark|token Zertifikat

7.1.2.2 trust|mark|vsc 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 = TrustMark-VSC-nn OU = TrustMark-VSC-nn O = A-Trust C = AT	-nn bezeichnet die Generation des Schlüssels, der von A-Trust für die Signatur des Zertifikats verwendet wurde. Bei jeder Ausstellung eines neuen A-Trust CA-Schlüssels wird diese Generationsnummer um eins erhöht.
Gültig von Gültig bis	Beginn und Ende der Gültigkeit des Zertifikats	Der Gültigkeitszeitraum beträgt höchstens drei Jahre
Zertifikatsinhaber	C = CountryName T = Title SN = SurName G = GivenName CN = CommonName E = EmailAddress	CountryName: AT etc. Title: Titel (Dr. etc.) SurName: Zuname GivenName: Vorname CommonName: Vorname + Zuname EmailAddress: Primäre E-Mailadresse des Zertifikatsinhabers
Öffentlicher Schlüssel	RSA 1024 Bit	Öffentlicher Schlüssel des Zertifikatsinhabers

Tabelle 10 Profil für trust|mark|vsc Zertifikat

7.1.2.3 trust|mark|server 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 = TrustMark-WebServer-nn OU = TrustMark-WebServer-nn O = A-Trust C = AT	-nn bezeichnet die Generation des Schlüssels, der von A-Trust für die Signatur des Zertifikats verwendet wurde. Bei jeder Ausstellung eines neuen A-Trust CA-Schlüssels wird diese Generationsnummer um eins erhöht.
Gültig von Gültig bis	Beginn und Ende der Gültigkeit des Zertifikats	Der Gültigkeitszeitraum beträgt höchstens drei Jahre
Zertifikatsinhaber	C = CountryName CN = CommonName O = Organisation	CountryName: AT, DE etc. CommonName: Name der Domain Organisation: Name der Organisation (lt. Eintragung im Firmenbuch oder Abkürzung)
Öffentlicher Schlüssel	mind. RSA 512 Bit	Öffentlicher Schlüssel des Zertifikatsinhabers

Tabelle 11 Profil für trust|mark|server Zertifikat für Webserver

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 = TrustMark-SigServer-nn OU = TrustMark-SigServer-nn O = A-Trust C = AT	-nn bezeichnet die Generation des Schlüssels, der von A-Trust für die Signatur des Zertifikats verwendet wurde. Bei jeder Ausstellung eines neuen A-Trust CA-Schlüssels wird diese Generationsnummer um eins erhöht.
Gültig von Gültig bis	Beginn und Ende der Gültigkeit des Zertifikats	Der Gültigkeitszeitraum beträgt höchstens drei Jahre
Zertifikatsinhaber	C = CountryName CN = CommonName O = Organisation OU = Organisationsuntereinheit E = E-Mailadresse	CountryName: AT, DE etc. CommonName: Name der Organisation bzw. Kurzform, Schlüsselkennung (Sig oder Enc) und eine organisationsintern eindeutige Zusatzinformation, z. B. „XYZ-Bank Sig 0001“ Organisation: Name der Organisation (lt. Eintragung im Firmenbuch oder Abkürzung) Organisationsuntereinheit: Abteilung etc.
Öffentlicher Schlüssel	mind. RSA 1024 Bit	Öffentlicher Schlüssel des Zertifikatsinhabers

Tabelle 12 Profil für trust|mark|server Zertifikat für Signaturserver

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 13 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

	Zertifikatstyp		Klassifikation	
Private Extensions				
authorityInfoAccess	Ja	Ja		X

Tabelle 14 Erweiterungen (trust|mark|token Zertifikate)

Erweiterung	Im Zertifikat vorhanden	Klassifikation	
		kritisch	Nicht kritisch
Standarderweiterungen			
authorityKeyIdentifier	Ja		X
subjectKeyIdentifier	Ja		X
keyUsage	Ja	X	
certificatePolicies	Ja		X
subjectAltName	Optional		X
basicConstraints	Ja		X
cRLDistributionPoints	Ja		X
Private Extensions			
authorityInfoAccess	Ja		X
1.2.40.0.10.1.1.1 (Behördenkennzeichen)	optional		X

Tabelle 15 Erweiterungen (trust|mark|vsc Zertifikate)

Erweiterung	Im Zertifikat vorhanden	Klassifikation	
		kritisch	Nicht kritisch
Standarderweiterungen			
authorityKeyIdentifier	Ja		X
subjectKeyIdentifier	Ja		X
keyUsage	Ja	X	
certificatePolicies	Ja		X

		Klassifikation	
basicConstraints	Ja		X
cRLDistributionPoints	Ja		X
Private Extensions			
authorityInfoAccess	Ja		X

Tabelle 16 Erweiterungen (trust|mark|server Zertifikate)

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

Die Erweiterung subjectDirectoryAttributes enthält bei trust|mark|token Zertifikaten optional das Geburtsdatum des Zertifikatsinhabers.

trust|mark|vsc Zertifikate können eine Zertifikatserweiterung erhalten, welche die Behördeneigenschaft ausdrückt (Behördenkennzeichen). Diese Erweiterung ist zwingend für Behördenzertifikate, bei den anderen Zertifikaten darf sie nicht vorhanden sein.

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 trust|mark der A-Trust. A-Trust stellt sicher, dass diese Zertifizierungsrichtlinie für die betroffenen Certificate Policies geeignet ist.

9 Anhang

A Glossar

Aktivierungsdaten	Daten, die zur Aktivierung der Schlüssel benötigt werden (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 und/oder Klasse von Applikationen gleicher Sicherheitsanforderungen anzeigt.
Chipkarte	Chipkarte / Smart Card auf der die Schlüssel des jeweiligen Anwenders sicher gespeichert sind und auf denen die Signatur berechnet wird.
Dienste (CA-Dienste)	Überbegriff für angebotene Dienstleistungen wie Verzeichnisdienst, Statusauskunft und Zeitstempeldienst
Dienste-Schlüssel	Schlüssel eines Dienstes (bspw. Signaturschlüssel zur Signatur von Statusauskünften)
Gültigkeitsmodell	Modell nach dem die Prüfung der Gültigkeit von Zertifikaten und Signaturen vorgenommen wird.
Kettenmodell	Gültigkeitsmodell nach dem eine gültige Anwendung des Schlüssels dann erfolgt, wenn zum Zeitpunkt der Anwendung das Zertifikat gültig ist und das übergeordnete Zertifikat zum Zeitpunkt der Erstellung des eingesetzten Zertifikats gültig war.
Policy	siehe Certificate Policy

Registrierungsstelle	In der Registrierungsstelle werden Anwender registriert und identifiziert, bevor sie die Zertifikate erhalten. Die Registrierungsstelle kann auch zusätzliche Aufgaben übernehmen, wie z. B. die Annahme und Weiterleitung von Änderungsanträgen.
Root-CA	Die Root-CA ist die oberste CA in der Zertifizierungshierachie der A-Trust. Sie stellt die Zertifikate für die nachgeordneten CAs aus.
Signaturerstellungsdaten	Signaturerstellungsdaten sind einmalige Daten wie Codes oder private Signaturschlüssel, die von dem Zertifikatsinhaber zur Erstellung einer elektronischen Signatur verwendet werden.
Signaturprüfdaten	Signaturprüfdaten sind Daten wie Codes oder öffentliche Signaturschlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden.
Statusauskunft	Dienst, bei dem die Anwender Auskunft über den aktuellen Status (gültig oder gesperrt) eines Zertifikates abrufen können. Der Zugriff wird über OCSP realisiert, bzw. dienen hiezu auch CRLs, die über den Verzeichnisdienst abrufbar sind.
trust|mark|server	Produktname für Serverzertifikate (Webserver oder Signaturserver) von A-Trust
trust|mark|token	Produktname für nicht qualifizierte Kartenzertifikate von A-Trust
trust|mark|vsc (Virtual Smart Card)	Produktname für Softwarezertifikate von A-Trust
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	Anwender, dessen Schlüssel und persönliche Daten im Zertifikat der A-Trust festgehalten sind.
Zertifikatsnutzer	Anwender, der Zertifikate der A-Trust über die Schlüssel und Daten anderer nutzt, um Signaturen zu prüfen.
Zertifizierungsrichtlinie	Gleichbedeutend mit „Certification Practice Statement“: Richtlinien über die Praktiken der Zertifizierungsstelle zur Herausgabe von Zertifikaten.
Zertifizierungsstelle	Die Zertifizierungsstelle generiert die Schlüssel der Anwender und stellt in Zertifikaten die Zuordnung von Anwendern zu Schlüsseln sicher. Zusätzlich übernimmt sie noch weitere Dienstleistungen, wie z.B. das Veröffentlichen von Zertifikaten oder 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