A-Trust Gesellschaft für Sicherheitssysteme
im elektronischen Datenverkehr GmbH
Landstraßer Hauptstraße 5, A-1030 Wien
Tel: +43 (1) 713 21 51 - 0
Fax: +43 (1) 713 21 51 - 350
https://www.a-trust.at

# a.trust Zertifizierungsrichtlinie (Certificate Practice Statement) für qualifizierte Zertifikate a.sign premium mobile

Version: 0.9.9
Datum: 13.08.2009

# Inhaltsverzeichnis

# Tabellenverzeichnis

# Abbildungsverzeichnis

# 1 Einführung

## 1.1 Überblick

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

Eine Zertifizierungsrichtlinie gibt Auskunft über die Praktiken der Zertifizierungsstellen zur Herausgabe von a.sign premium mobile Zertifikaten. Sie dient dazu, die Praktiken intern zu fixieren und den Anwendern die Vorgehensweise der Zertifizierungsstelle zu erläutern. Somit können sich die Anwender ein Bild von den vorhandenen Sicherheitsmaßstäben machen.

Die Gliederung dieses Dokuments orientiert sich an dem internationalen Standard für Zertifizierungsrichtlinien (RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework) der Internet Society.

## 1.2 Dokumentidentifikation

| | |
|---|---|
| Name der Richtlinie: | a.trust Zertifizierungsrichtlinie (Certification Practice Statement) für qualifizierte Zertifikate a.sign premium mobile für qualifizierte Signaturen |
| Version: | 0.9.9 / 13.08.2009 |
| Object Identifier: | 1.2.040.0.17 (a.trust) .2 (CPS) .20 (a.sign premium mobile) .0.9.9 (Version) vorliegende Version |

Der a.trust OID 1.2.040.0.17 ist bei ÖNORM registriert.

## 1.3 Zertifizierungsinfrastruktur und Anwendungsbereich

### 1.3.1 Zertifizierungsstellen

Es existiert eine zentrale Zertifizierungsstelle, die die Schlüssel der Signatoren sowie die Widerrufslisten für Zertifikate signiert. a.trust stellt qualifizierte Zertifikate (gemäß SigG) aus, die auf einer sicheren Signaturerstellungseinheit basieren.

Darüber hinaus existiert eine Root-Zertifizierungsstelle, welche das Zertifikat und die Widerrufslisten für die Zertifizierungsstellen signiert. Anwenderzertifikate werden von der Root-CA nicht ausgestellt.

Die Zertifikate der Root-CA (Stammzertifikat) und der Zertifizierungsstelle (CA-Zertifikat) sind einfache Zertifikate. Die Signaturen, die auf Basis dieser Zertifikate erstellt werden, sind fortgeschrittene Signaturen.

a.trust erfüllt die Sicherheitsanforderungen nach § 18 [SigG] und hat sich dem freiwilligen Akkreditierungsverfahren gem. § 17 [SigG] bei der Aufsichtsstelle unterzogen.

### 1.3.2 Registrierungsstellen

In den Registrierungsstellen führen Registration Officers die anwenderrelevanten Arbeiten durch. Diese Aufgaben umfassen neben der sicheren Identifizierung auch die Bearbeitung der Anwenderdaten und die Weiterleitung von Informationen an die übergeordnete Zertifizierungsstelle. Die Ausstellung des Zertifikats erfolgt auf Veranlassung der Registrierungsstelle.

### 1.3.3 Widerrufsdienst

Die Anwender können sich telefonisch bzw. über Fax an den Widerrufsdienst wenden und das Zertifikat widerrufen lassen. Wollen sie eine Sperre durchführen oder aufheben lassen, so kann dies mittels eines Telefonats oder durch eine von a.trust zur Verfügung gestellte Webanwendung erfolgen.

### 1.3.4 Anwender

Unter “Anwender” sind die Personen zusammengefasst, die a.sign premium mobile Zertifikate von a.trust erhalten (Zertifikatsinhaber bzw. Signatoren), oder welche a.sign premium mobile Zertifikate nutzen bzw. den Zertifikatsangaben vertrauen (Signaturempfänger).

### 1.3.5 Anwendbarkeit

Dieses Dokument ist relevant für die Zertifizierungsstelle, die angeschlossenen Registrierungsstellen, Dienstleistungen der Zertifizierungs- und Registrierungsstelle und die Anwender. Der zertifizierte Signaturschlüssel des Signators darf ausschließlich für das Erstellen von Signaturen genutzt werden.

Elektronische Signaturen, die in Übereinstimmung mit dieser Zertifizierungsrichtlinie und unter Verwendung der von a.trust empfohlenen Komponenten und Verfahren erstellt wurden, sind qualifizierte Signaturen im Sinne des § 2 (3a) [SigG]

### 1.3.6 Zertifizierungshierarchie

Abbildung 1 zeigt eine schematische Darstellung der Zertifikatshierarchie.

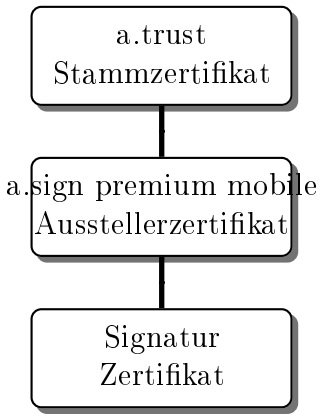


Abbildung 1: Zertifizierungshierarchie

### 1.3.7 a.trust Verzeichnisbaum

Eine schematische Darstellung des Verzeichnisbaums ist in Abbildung 2 zu finden.

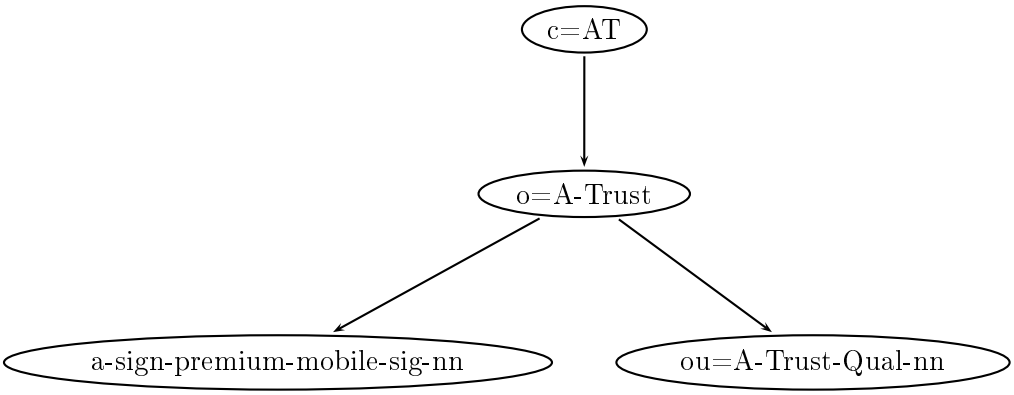


Abbildung 2: a.trust Verzeichnisbaum

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

Mit A-Trust-Qual-nn werden die (ZwischenInstanz-)CA-Zertifikate und die zugehörigen CRLs signiert.

Die Zertifikate der Zertifikatsinhaber von a.sign premium mobile Zertifikaten und die zugehörigen CRLs werden mit dem CA-Schlüssel a-sign-premium-mobile-sig-nn signiert, wobei nn die Version der Zertifizierungsstelle bezeichnet, welche mit dem zugehörigen geheimen Schlüssel digitale Signaturen erstellt.

## 1.4 Ansprechpartner und Kontaktstellen

### 1.4.1 Organisation zur Verwaltung dieses Dokuments

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

### 1.4.2 Kontaktinformation

Kontaktinformationen für a.sign premium mobile Zertifikate erhält man auf folgenden Wegen:

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

### 1.4.3 Verantwortlicher für die Anerkennung anderer Anwendungsvorgaben (Policies)

a.trust übernimmt die Entscheidung über die Anerkennung anderer Anwendungsvorgaben (Policies).

# 2 Generelle Bestimmungen

## 2.1 Verpflichtungen

### 2.1.1 Verpflichtungen des Zertifizierungsdiensteanbieters

Die Zertifizierungsstelle der a.trust befolgt die Regelungen der Zertifizierungsrichtlinie, die sich insbesondere auf die folgenden Aspekte erstreckt:

- Die Zertifikate für Signatoren werden im Einklang mit der Zertifizierungsrichtlinie erstellt und können gesperrt, widerrufen oder verlängert werden.
- Die Zertifizierungsstelle arbeitet im Einklang mit dem der Aufsichtsbehörde vorgelegten Sicherheits- und Zertifizierungskonzept.
- Die Zertifizierungsstelle beschäftigt ausschließlich qualifiziertes Personal.
- Die Zertifizierungsstelle kommt ihrer Informationspflicht hinsichtlich Signatoren 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 Signatoren und zum Signieren der Widerrufsinformationen.
- Die Zertifizierungsstelle veröffentlicht alle ausgestellten Zertifikate (sofern die Ausstellung vom Inhaber gewünscht ist). Bei Widerruf und Sperre eines Zertifikats wird der betroffene Signator benachrichtigt. Ein nicht veröffentlichtes Zertifikat wird bei einer Sperre oder einem Widerruf in die Widerrufsliste aufgenommen.
- a.trust hat insbesondere die Verpflichtung eine Liste der für eine qualifizierte Signaturerstellung und -prüfung zu verwendenden Komponenten und Verfahren zur erstellen und aktuell zu halten und diese den Signatoren und Über prüfern von Zertifikaten jederzeit zugänglich zu machen.
- a.trust informiert die Signatoren über die erfolgte freiwillige Akkreditierung bei der Aufsichtsstelle gem. § 17 [SigG].

### 2.1.2 Verpflichtungen der Registrierungsstellen

Die Registrierungsstellen der a.trust befolgen die Regelungen der 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 der Zertifizierungsrichtlinie beschrieben sind.
- Die Registrierungsstellen beschäftigen Personal mit angemessener Qualifikation.
- Das a.sign premium mobile Zertifikat wird im Zuge des Registrierungsprozesses, nach erfolgreicher Identifikation durch die Registrierungsstelle, ausgestellt. a.trust stellt dem Signator insbesondere folgende Dokumente elektronisch zur Verfügung:
  - Vertragsbedingungen,
  - Entgeltbestimmungen sowie
  - Zertifizierungsrichtlinie (Certification Practice Statement), Anwendungsvorgaben (Certificate Policy) und die Belehrungen (Merkblatt) für den Signator.

### 2.1.3 Verpflichtungen der Zertifikatsinhaber

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

- Die Signatoren verpflichten sich die Allgemeinen Geschäftsbedingungen zusammen mit der a.sign premium mobile Anwendungsvorgabe (Policy), der Zertifizierungsrichtlinie und den Entgeltbestimmungen von a.trust als Grundlage für den abgeschlossenen Vertrag anzuerkennen.
- Der Signator ist für die Richtigkeit der Angaben verantwortlich, die er bei der Registrierung macht und wirkt gemäß den in der Zertifizierungsrichtlinie angegebenen Verfahren zur Identitätsfeststellung und Authentifikation mit.
- Der Signator ist verpflichtet, seine für das Auslösen der Signatur nötigen Komponenten angemessen zu schützen. Dies umfasst insbesondere das Verhindern des Zugriffs durch unautorisierte Personen auf die SIM-Karte und das vom Signator gewählte Signaturpasswort.
- Falls nötig initiiert der Signator unverzüglich die Sperre oder den Widerruf seines Zertifikats. Wird die Sperre nicht nach einem vorgegebenen Zeitraum aufgehoben, so erfolgt automatisch ein Widerruf des Zertifikats.
- Der Signator setzt sein Zertifikat nur zu dem im Zertifikat angegebenen Zweck ein. Maßgeblich hierfür sind die zum Zeitpunkt der Ausstellung des Zertifikats gültige Zertifizierungsrichtlinie und die zugehörigen Anwendungsvorgaben (Policy).

- Der Signator ist sich bewußt, dass A-Trust eine Liste mit empfohlenen technischen Komponenten und Verfahren für die Erstellung von qualifizierten Signaturen bereitstellt und dass bei der Verwendung anderer Komponenten und Verfahren A-Trust für Schäden, die durch diese verursacht werden, nicht haftbar gemacht werden kann.
- Er muss weiters dafür Sorge tragen, dass auf dem PC-Arbeitsplatz, an welchem die qualifizierte Signatur erstellt wird, kein unbefugt eingebrachter Programmcode zur Anwendung kommt. Dazu soll er die folgenden Vorgaben von a.trust einhalten:
  - Der Signator muss alle notwendigen technischen und organisatorischen Maßnahmen ergreifen, um unbefugten Zugriff auf seinen PC-Arbeitsplatz und die darauf befindlichen Programmcodes zu verhindern.
  - a.trust verpflichtet den Signator sich an die Empfehlungen des Herstellers des von ihm verwendeten Betriebssystems sowie an die Empfehlungen der Hersteller der anderen Software-Produkte, die er installiert hat, zu halten. Der Signator ist verpflichtet die jeweiligen nationalen Ausfuhrbestimmungen sowie etwaige nationale Nutzungsbeschränkungen bei einer Verwendung im Ausland zu beachten.

### 2.1.4 Verpflichtungen der Zertifikatsnutzer

Den Zertifikatsnutzern von a.sign premium mobile Zertifikaten (Signaturempfänger) wird empfohlen, vor der Akzeptanz folgende Prüfungen durchzuführen:

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

Wenn der Überprüfer eines Zertifikats eine qualifizierte Signaturprüfung durchzuführen beabsichtigt, dann empfiehlt ihm a.trust die Verwendung der für eine qualifizierte Überprüfung einer Signatur empfohlenen Komponenten und Verfahren.

### 2.1.5 Verpflichtungen der Verzeichnisdienste

Der Verzeichnisdienst veröffentlicht in regelmäßigen Abständen

- die ausgestellten Zertifikate, die zur Veröffentlichung freigegeben sind, sowie Listen der
- gesperrten und

- widerrufenen Zertifikate.

Der Zertifikatsdienst ist verpflichtet, diese Listen in regelmäßigen Abständen, wie in dieser Zertifizierungsrichtlinie vereinbart, zu aktualisieren und hochverfügbar zu halten.

## 2.2 Haftung

Die Allgemeinen Geschäftsbedingungen bilden zusammen mit der Zertifizierungsrichtlinie, Anwendungsvorgaben (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 Signaturerstellungsdaten und die ihnen zugeordneten Signaturprüfdaten einander bei der Verwendung der von der a.trust bereitgestellten oder als geeignet bezeichneten Produkte und Verfahren in komplementärer Weise entsprechen,
- das Zertifikat bei Vorliegen der Voraussetzungen unverzüglich widerrufen wird und ein Widerrufsdienst verfügbar ist,
- die Anforderungen des SigG § 7 erfüllt und für die Erzeugung und Speicherung von Signaturerstellungsdaten technische Komponenten und Verfahren nach SigG § 18 verwendet werden,
- sie die X.509-Standards einhält,
- die Abläufe, die in der gegenständlichen Zertifizierungsrichtlinie beschrieben sind, einhält.

a.trust haftet weiters für die Korrektheit einer qualifizierten Signatur, wenn diese unter Einhaltung aller von a.trust dem Signator auferlegten Vorschriften und unter Verwendung der empfohlenen Komponenten und Verfahren erstellt wurde. 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.

a.trust haftet nicht, wenn sie nachweist, dass sie und ihre Mitarbeiter an der Verletzung ihrer Verpflichtungen kein Verschulden trifft (gemäß SigG §23 (3)).

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

a.trust haftet für die Tätigkeiten der Registrierungsstellen laut Sicherheits- und Zertifizierungskonzept.

## 2.3 Finanzielle Verantwortung

### 2.3.1 Schadensersatz der beteiligten Parteien

Keine Bestimmungen.

### 2.3.2 Treuhänderische Beziehungen

Keine Bestimmungen.

### 2.3.3 Administrative Prozesse

Keine Bestimmungen.

## 2.4 Auslegung und (gerichtliche) Durchsetzung

### 2.4.1 Zugrunde liegende Gesetzesbestimmungen

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

Qualifizierte Signaturen, die in Übereinstimmung mit dieser Zertifizierungsrichtlinie auf Basis eines qualifizierten a.sign premium mobile Zertifikats für qualifizierte Signaturen erstellt wurden, sind in ihrer Rechtswirkung gemäß § 4 Abs 1 [SigG] einer eigenhändigen Unterschrift grundsätzlich gleichgestellt und entsprechen Artikel 5.1 der EU-Richtlinie (siehe [SigRL]). Ausnahmen können sich aus vertraglichen und gesetzlichen Vereinbarungen ergeben (siehe § 4 [SigG]).

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

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

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 den Entgeltbestimmungen. Alle Entgelte, die nicht im Grundentgelt enthalten sind, werden mit der Nutzung der jeweiligen Leistung fällig.

### 2.5.1 Ausgabe und Erneuerung von Zertifikaten

Die aktuell gültige Regelung findet sich in den Entgeltbestimmungen.

### 2.5.2 Abrufen von Zertifikaten

Der Abruf von a.sign premium mobile Zertifikaten über den Verzeichnisdienst der 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 Widerruflisten und Statusinformationen ist kostenfrei.

### 2.5.5 Gebühren für weitere Dienste

a.trust stellt eine Hilfestellung in Form eines gebührenpflichtigen Call Centers bereit.

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

Tabelle 1: Homepage und Verzeichnisse

### 2.5.6 Richtlinien für Gebührenrückerstattung

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

## 2.6 Bekanntmachung und Verzeichnisdienste

### 2.6.1 Web-Seiten und Verzeichnisse

a.trust stellt folgende Web-Seiten und Verzeichnisse bereit: Die Liste der empfohlenen Komponenten und Verfahren für die sichere Signaturerstellung und –prüfung stellt a.trust auf ihrer Homepage unter

- http://www.a-trust.at/docs/

zur Verfügung.

Die Informationen betreffend den Widerrufsdienst und die Durchführung von Widerrufen stellt a.trust unter

- http://www.a-trust.at/widerruf/

zur Verfügung.

### 2.6.2 a.trust Stammzertifikat

Das Stammzertifikat ist unter

- https://www.a-trust.at/certs/A-Trust-Qual-nnx.crt oder
- http://www.a-trust.at/certs/A-Trust-Qual-nnx.crt

zu finden. Erläuterung: -nn ist die Versionsnummer der Root-CA: erhöht wird bei Generierung eines neuen Schlüssels und Veränderung des Distinguished Name; -x bezeichnet

die Version des Zertifikats: erhöht wird bei Ausstellung eines neuen Zertifikats mit unverändertem DN, unabhängig, ob ein neuer Schlüssel generiert wird, bei einer neuen CA-Version wird immer mit –a begonnen; Beispiel: A-Trust-Qual-02a.crt.

Der Download des Stammzertifikats kann auf sichere Weise über https erfolgen, ebenso wie auch über http.

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 benötigte CA-Zertifikat ist unter

- https://www.a-trust.at/certs/a-sign-premium-mobile-sig-nnx.crt oder
- http://www.a-trust.at/certs/a-sign-premium-mobile-sig-nnx.crt

zu finden (die Bedeutung von -nnx ist in Abschnitt 2.6.2 beschrieben) und kann von hier heruntergeladen werden.

### 2.6.4 Widerrufsinformationen

Verteilungspunkt für die Zertifikatssperr- und –widerrufslisten (CRLs) ab der CA-Version 02:

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

Verteilungspunkt für die Zertifikatssperr- und –widerrufslisten für CA-Version 01:

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

Sichere Abfrage der CRL über https:

- https://www.a-trust.at/html/crl_download.asp?CA=a-sign-premium-mobile-sig-nn

### 2.6.5 Suche nach einem Zertifikat

Für die Suche nach einem bestimmten Zertifikat (Suchkriterien sind wahlweise Nachname, Vorname, CIN oder Pseudonym) und den Download eines gefundenen Zertifikats steht auf der a.trust Homepage ein Formular zur Verfügung. Sichere Abfrage eines Zertifikats über https:

- https://www.a-trust.at/html/ldaptrust_all.asp?Product=a-sign-premium-mobile-sig-nn

(z. B. Product=a-sign-premium-Sig-02).

### 2.6.6 Veröffentlichung von Informationen der Zertifizierungsstelle

Die Zertifizierungsstelle veröffentlicht:

- die jeweils gültige Zertifizierungsrichtlinie,
- die jeweils gültige Anwendungsvorgabe (Certificate Policy),
- die gültige Entgeltregelung,
- die Ergebnisse der Audits durch die Aufsichtsbehörden,
- interne Auditinformationen, sofern die Sicherheit der a.trust nicht gefährdet ist,
- das Zertifikat der Zertifizierungsstelle,
- die Allgemeinen Geschäftsbedingungen,
- die Belehrungen für den Signator,
- die Information über die zu verwendenden Komponenten und Verfahren,
- eine Liste mit Kontaktstellen bzw. Registrierungsstellen,
- die Information über die freiwillige Akkreditierung bei der Aufsichtsstelle gem. § 17 [SigG].

auf ihrer Homepage www.a-trust.at.

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

Die Signatoren werden zusätzlich informiert über:

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

### 2.6.7 Frequenz der Aktualisierung

Eine Aktualisierung der Zertifizierungsrichtlinie erfolgt gemäß Kapitel 9.

### 2.6.8 Zugriffskontrollen

Zugriffskontrollen stellen sicher, dass die Anwender nur lesenden Zugriff auf die Veröffentlichungen der 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; es enthält die Zertifikate der Zertifizierungsstellen, die Widerrufslisten und die Zertifikate der Signatoren.
- Eine öffentliche Web-Seite, auf der diese Zertifizierungsrichtlinien abrufbar sind und weitere allgemeine Informationen den Anwendern zugänglich sind.

## 2.7 Interne Prüfung (Audit)

### 2.7.1 Häufigkeit des Audits

Das erstmalige Audit zur Akkreditierung der Zertifizierungsstelle erfolgt im Auftrag der Aufsichtsbehörde bei Aufnahme des Betriebs. Danach werden Audits in regelmäßigen Abständen im Auftrag der Aufsichtsbehörde durchgeführt.

Darüber hinaus werden jährlich interne, von a.trust in Auftrag gegebene, Revisionen und Audits durchgeführt.

Audits werden stichprobenhaft in allen a.trust Liegenschaften und Registrierungsstellen durchgeführt.

### 2.7.2 Identität bzw. Anforderungen an den Auditor

Die Aufsichtsbehörde bestimmt den Auditor für die in ihrem Auftrag durchzuführenden Audits.

Interne Audits, die von a.trust im Rahmen ihrer Qualitätssicherung beauftragt werden, werden im Rahmen der Revision durchgeführt.

### 2.7.3 Beziehungen zwischen Auditor und zu untersuchender Partei

Die Aufsichtsbehörde bestimmt den Auditor, der in ihrem Auftrag die Überprüfung vornimmt.

Von a.trust beauftragte Audits werden von Personen, welche über die notwendige Qualifikation verfügen, durchgeführt.

### 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 kryptografischen Komponenten.

### 2.7.5 Handlungen nach unzureichendem Ergebnis

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

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

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

### 2.7.6 Bekanntgabe der Ergebnisse

Die Aufsichtsbehörde veröffentlicht die Informationen aus dem Audit. Darüber hinaus wird die a.trust zusätzliche Informationen – sofern dadurch nicht die Sicherheit gefährdet wird – bereitstellen.

## 2.8 Vertraulichkeit

### 2.8.1 Vertraulich eingestufte Informationen

Die a.trust verpflichtet sich, die vom Signator bekannt gegebenen Daten vertraulich im Sinne des Datenschutzgesetzes zu behandeln. Die Daten, die bei der Anmeldung angegeben werden, werden ausschließlich für die Dienstleistungen der Zertifizierungsstelle benutzt. Bei der Verwendung von Pseudonymen durch den Signator muss die a.trust den ihr bekannten korrekten und vollständigen Namen des Signators 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 Zertifikatswiderruf

Gründe, die zur Sperre oder zu einem Widerruf führen, werden im Verzeichnisdienst veröffentlicht.

### 2.8.4 Offenbarung an Behörden im Rahmen gesetzlicher Pflichten

a.trust gibt die persönlichen Daten des Signators nur auf Verlangen an laut SigG berechtigte Personen weiter (gemäß SigG §11).

### 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:

- Sicherheits- und Zertifizierungskonzept
- Zertifizierungsrichtlinie
- Anwendungsvorgabe (Certificate Policy)
- Liste der empfohlenen Komponenten und Verfahren zur Erstellung und Prüfung sicherer elektronischer Signaturen

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

- Private Schlüssel des Zertifizierungsdiensteanbieters und
- Öffentliche Schlüssel des Zertifizierungsdiensteanbieters.

Die Eigentumsrechte der folgenden Schlüssel liegen beim Signator:

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

# 3 Identifizierung und Authentifikation

## 3.1 Erstregistrierung

### 3.1.1 Namenstypen

Die Angaben des Signators werden in zwei Kategorien eingeteilt. Dies sind zum einen die erforderlichen und zum anderen die optionalen Angaben. Es sind folgende Daten aufzunehmen:

- Name für das a.sign premium mobile Zertifikat: Nachname und Vorname sind erforderlich.
  Im Falle von Standard a.sign premium mobile Zertifikaten können Signatoren statt des Namens auch ein Pseudonym wählen. Der korrekte und vollständige Name muss der Registrierungsstelle und Zertifizierungsstelle auch bei Verwendung eines Pseudonyms bekannt sein.
- Die Angabe der postalischen Adresse ist erforderlich.
- Optional können im Namen des Zertifikatswerbers die Attribute OrganizationName mit dem Inhalt "Berufsbezeichnung" (z.B. Rechtsanwalt) und OrganizationalUnit mit einem eindeutigen Code (z.B. Rechtsanwaltscode) als Inhalt vergeben werden. Diese Attribute werden nur vergeben, wenn die ausstellende Registrierungsstelle, z.B. Rechtsanwaltskammer, die Korrektheit dieser Angaben sicher stellt.
  Das Attribut OrganizationName kann auch bei Behördenzertifikaten nach Bekanntgabe der Behörde vergeben werden (siehe Kapitel 4.1).

### 3.1.2 Anforderungen an Namen

Der Name des Signators muss den bei der Registrierung vorliegenden Identitätsdaten entsprechen.

Wird ein Pseudonym verwendet, so muss es wie folgt codiert werden: "Pseudonym: Pseudonymbezeichnung".

Gemäß §8 (4) SigG darf ein verwendetes Pseudonym weder anstößig noch offensichtlich zur Verwechslung mit Namen oder Kennzeichen (Markennamen) geeignet sein.

Auf Wunsch des Signators kann als Firmenpseudonym auch der Name eines Unternehmens (vollständiger Name lt. Firmenbuch oder eindeutige Abkürzung des Unternehmensnamens) in der Form "Organisationsname:Firma" eingetragen werden, sofern der Signator, durch Vorlage geeigneter Dokumente (Vollmacht eines Vertretungsbefugten) darlegen kann, dass er den Organisationsnamen im Zertifikat verwenden darf.

### 3.1.3 Regeln zur Interpretation unterschiedlicher Namensformen

Keine Bestimmungen.

### 3.1.4 Eindeutigkeit der Namen

Jeder Signator erhält eine 12-stellige Nummer (Cardholder Identification Number, abgekürzt CIN). Diese Nummer ist ein Teil des eindeutigen Namens des Signators und ermöglicht die eindeutige und unveränderliche Zuordnung von Signaturerstellungsdaten und -prüfdaten zu einem Signator.

### 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

Der Signator bestätige dass er im Recht ist, eine Signatur auszulösen, indem er einerseits im Besitz des von ihm gewählten Signaturpasswortes ist, und er den Inhalt der Verifikations-SMS, die vor jeder Anwendung des privaten Schlüssels an das bei der Registrierung angegebene Mobiltelefon (SIM-Karte) gesendet wird, kennt.

### 3.1.8 Authentisierung von Organisationen

Keine Bestimmungen.

### 3.1.9 Authentisierung von Individuen

Die Angaben des Antragstellers werden bei der Ausstellung des Zertifikates in der Registrierungsstelle durch den Registration Officer überprüft. Der Antragsteller beweist seine Identität durch das Vorlegen eines gültigen, amtlichen Lichtbildausweises. Dabei sind die folgenden Ausweise zulässig:

- ein in Österreich ausgestellter amtlicher Lichtbildausweis (eine Liste der in Österreich gültigen amtlichen Lichtbildausweise, die von a.trust akzeptiert werden, ist auf der Homepage der a.trust zu finden) oder

- ein international gültiger Reisepass in deutscher und/oder englischer Sprache.

Weiters steht die Möglichkeit zur Verfügung, dass mittels eines RSa Briefs (SigV §§11) ein für die Ausstellung der Zertifikate notwendiger Aktivierungscode an die Meldeadresse des Zertifikatswerbers versendet wird. Im Rahmen der Zustellung des RSa Briefs ist es notwendig, dass der Antragssteller seine Identität durch das Vorlegen eines gültigen, amtlichen Lichtbildausweises beweist. Alternativ hierzu kann eine Bestätigung der Identität durch eine öffentliche Einrichtung erfolgen, sofern die initiale Identitätsfeststellung und Ausgabe der Zugangsdaten zu deren Onlineportal den Anforderungen der SigV §§11 entspricht. Diese Bestätigung wird in elektronischer Form, durch die öffentliche Stelle signiert, vor der Zertifikatsausstellung an a.trust übermittelt.

Qualifizierte Zertifikate, die auf die Namen Max Mustermann, Test Zupfer, Test Test, Musterfrau Maxine lauten oder deren Namen mit „XXX“ beginnen, werden von der A-Trust zu Testzwecken ausgestellt. Aus diesem Grund wird bei Ausstellung von qualifizierten Zertifikaten auf die genannten Namen keine Identitätsprüfung durchgeführt.

## 3.2 Erneute Registrierung/Rezertifizierung

Der Signator kann nach einem Widerruf eine Ersatzbestellung durchführen. Der Vorgang verläuft analog zur Erstregistrierung. Dabei sind allfällige Änderungen in den personenbezogenen Daten anzugeben.

Es ist ebenfalls zulässig, dass der Signator ein neues Zertifikat, mittels einer qualifizierten Signatur seines bereits aktiven Zertifikates, aktiviert. In diesem Falle ist keine erneute Registrierung / Rezertifizierung erforderlich. Sollten sich personenbezogene Daten geändert haben, muss eine erneute Registrierung / Rezertifizierung erfolgen.

## 3.3 Erneute Registrierung nach Widerruf

Nach dem Widerruf eines Zertifikates kann der Signator ein neues Zertifikat beantragen. Der Vorgang entspricht den Abläufen einer erneuten Registrierung / Rezertifizierung (siehe Abschnitt 3.2).

## 3.4 Sperr- und Widerrufsantrag

Sperren, Widerrufe und Sperraufhebungen werden entsprechend Abschnitt 4.4 gehandhabt. Der Signator kann sein Zertifikat per Telefon oder Webanwendung sperren bzw. eine Sperre aufheben lassen und per Telefon oder Fax einen Widerruf veranlassen.

Dazu muss der Signator zumindest seinen Namen, Daten seines Zertifikats und sein Sperr- und Widerrufspasswort bzw. sein Sperraufhebungspasswort angeben.

Sollte er sein Sperr- und Widerrufspasswort nicht wissen, ist eine Sperre (kein Widerruf) mit folgenden Angaben möglich:

- Vollständiger Name,
- Pseudonym (falls verwendet),
- Geburtstag und
- Geburtsort.

Eine Sperre kann innerhalb von zehn Tagen wieder aufgehoben werden.

Wenn das Passwort für einen Widerruf vergessen wurde, kann der Signator keinen Widerruf durchführen, sondern nur eine Sperre und diese ohne Aufhebung in einen Widerruf übergehen lassen.

# 4 Betriebliche Anforderungen

## 4.1 Antrag auf Ausstellung von Zertifikaten

Als Antrag wird verstanden, wenn der Signator entweder selbst oder durch Dritte freiwillig seine Personendaten an die a.trust übermittelt, um in den Besitz eines a.sign premium mobile Zertifikates zu kommen. Weiters wird ebenfalls die persönliche Kontaktaufnahme mit einer Registrierungsstelle zur Aktivierung eines Zertifikats, wie auch die Nutzung einer entsprechenden Webanwendung zur Aktivierung eines Zertifikats als Antrag verstanden. Die Freiwilligkeit bestätigt der Signator mit der Unterzeichnung des zustande kommenden Signaturvertrages.

Wenn in einem a.sign premium mobile Zertifikat die Zugehörigkeit zu einer Behörde abgebildet werden soll (Behördenkennzeichen siehe Kapitel 7.1.3), so wird von einem autorisierten Behördenvertreter zusätzlich zum Antrag ein Schreiben an die a.trust Registrierungsstelle gesandt, das die Rechtmäßigkeit dieser Angabe bestätigt.

## 4.2 Ausstellung von Zertifikaten

Persönliche Ausstellung:

Für die Austellung der Zertifikate des Antragstellers wird dieser persönlich in einer Registrierungsstelle vorstellig. Der Registration Officer stellt die Zertifikate aus, wenn

- er die Identität des Antragstellers anhand eines gültigen, amtlichen Lichtbildausweises (zulässige Ausweise siehe Kapitel 3.1.9) überprüft hat,
- der Antragsteller belehrt wurde und
- die Allgemeinen Geschäftsbedingungen akzeptiert hat.

Online-Austellung:

Im Zuge der Online-Austellung ist es für den Signator notwendig die Identität mittels des Aktivierungscodes (mittels RSa Brief an den Signator übermittelt) und des beim Antrag selbstgewählten Widerrufspassworts zu bestätigen. Alternativ hierzu kann eine Bestätigung der Identität durch eine öffentliche Einrichtung erfolgen, sofern die initiale Identitätsfeststellung und Ausgabe der Zugangsdaten zu deren Onlineportal den Anforderungen des Signaturgesetzes [SigG] entspricht. Diese Bestätigung wird in elektronischer Form, durch die öffentliche Stelle signiert, vor der Zertifikatsausstellung an a.trust übermittelt. Die Webanwendung unterbindet die Eingabe von Personendaten. Es wird ausschließlich auf bereits verifizierte Personendaten zur Ausstellung des Zertifikats zurück gegriffen, die von einer vertrauenswürdigen Stelle an die a.trust zur Verwendung frei gegeben und übermittelt werden.

Die Webanwendung bietet dem Signator noch vor Aktivierung des Zertfikats die Möglichkeit sich die Belehrung und die Allgemeinen Geschäftsbedingungen anzusehen und auf einem eigenen dauerhaften Datenträger zu speichern.

In beiden Ausstellungsfällen gilt die Ausstellung als abgeschlossen, wenn der Signaturvertrag des Signators unterschrieben ist und das Zertifikat ausgestellt wurde. A-Trust unterscheidet nicht, ob der unterschriebene Signaturvertrag in physischer (Papier) oder elektronischer Form unterzeichnet vorliegt.

Ausserdem gibt es die Möglichkeit mittels einer qualifizierten Signatur ein neues Zertifikat zu beantragen. Sollten sich personenbezogene Daten geändert haben, muss eine erneute Registrierung erfolgen.

## 4.3 Akzeptanz von Zertifikaten

Keine Bestimmungen.

## 4.4 Sperren und Widerrufen von Zertifikaten

a.sign premium mobile Zertifikate können vorübergehend gesperrt werden. Diese Sperre kann auch in einen endgültigen Widerruf umgewandelt werden. Ebenso ist ein sofortiger und permanenter Widerruf des Zertifikats möglich. Der Signator wird von einer erfolgten Sperre oder einem Widerruf informiert.

### 4.4.1 Gründe für einen Widerruf

Der Widerruf eines a.sign premium mobile Zertifikats wird erforderlich, wenn

- Angaben im Zertifikat nicht mehr korrekt sind,
- der Signator nicht mehr im alleinigen Besitz des Signaturpasswortes bzw. der für die SMS-Verifikation genutzten SIM-Karte sein
- Verdacht auf eine Kompromittierung besteht bzw. eine Kompromittierung vorliegt,
- der Zertifizierungsstelle ein wesentlicher Verstoß des Signators gegen diese Richtlinien oder die Allgemeinen Geschäftsbedingungen bekannt wird,
- die Frist einer Aufhebung einer Sperre abläuft,
- das Vertragsverhältnis beendet wird oder
- die eingesetzten Algorithmen nicht mehr den Sicherheitserwartungen entsprechen und dadurch eine sichere Anwendung der Signaturerstellungsdaten nicht mehr gegeben wäre.

### 4.4.2 Wer kann einen Widerruf anordnen

Ein Widerruf eines a.sign premium mobile Zertifikats kann angeordnet werden. Durch:

- den betreffenden Signator oder eine andere Person, die das Passwort für den Widerruf kennt,
- bei Verwendung eines Organisationsnamens als Pseudonym (gemäß 3.1.2) ein Vertretungsbefugter der Organisation,
- die Zertifizierungsstelle selbst.

### 4.4.3 Prozedur für einen Widerrufsantrag

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

- Der Signator wendet sich per Telefon an den Widerrufsdienst.
- Der Signator bzw. der Vertretungsbefugte veranlasst den Widerruf per Fax.
- Bei Vergessen des Passworts für den Widerruf kann der Signator keinen Widerruf, sondern nur eine Sperre beantragen.

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

- Telefonat: Der Signator kann rund um die Uhr einen Widerruf per Telefon vornehmen. Die Authentifikation erfolgt nur über das Sperr- und Widerruf-Passwort, welches der Antragsteller bei der Bestellung bzw. Registrierung selbst festgelegt hat.
  Die für einen Widerruf benötigten Informationen lassen sich wie folgt zusammenfassen:
  - Persönliche Daten (vollständiger Name, Geburtstag und -ort),
  - Passwort für den Widerruf,
  - Identifikationsnummer des Signators (CIN), Seriennummer des Zertifikats.
- Fax: Der Signator kann von 0 bis 24 Uhr einen Widerruf per Fax vornehmen. Das Fax muss das Sperr- und Widerrufs-Passwort sowie die vollständige Seriennummer des zu widerrufenden Zertifikats beinhalten.
- Fax: Der Vertretungsbefugte bzw. eine bevollmächtigte Person kann von 0 bis 24 Uhr einen Widerruf per Fax vornehmen. Das Fax muss einen Hinweis auf seine Vertretungsbefugnis sowie die vollständige Seriennummer des zu widerrufenden Zertifikats beinhalten.

- Besuch in einer Registrierungsstelle: Der Signator benötigt dazu einen gültigen, amtlichen Lichtbildausweis. Der RO teilt dem Signator die Zertifikatsnummer und das Passwort für den Widerruf mit, womit der Signator anschließend den Widerruf beim Widerrufsdienst veranlassen kann.

### 4.4.4 Frist bis zur Bekanntgabe des Widerrufs

Die Aktualisierung der Widerrufsliste erfolgt zumindest alle zwei Stunden. Der Widerrufsdienst ist rund um die Uhr erreichbar.

### 4.4.5 Gründe für eine Sperre

Die Sperre ist eine temporäre Aufhebung der Zertifikatsgültigkeit. Sie kann bei Verdacht des Eintritts eines der unter Kapitel 4.4.1 genannten Gründe genutzt werden. Im Gegensatz zu einem Widerruf kann eine Sperre innerhalb einer festgelegten Frist auch wieder aufgehoben werden. Nach spätestens zehn Tagen wird eine Sperre durch die Zertifizierungsstelle in einen Widerruf umgewandelt.

### 4.4.6 Wer kann eine Sperre anordnen und aufheben

Die bevollmächtigten Personen für eine Sperre sind:

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

Die Aufhebung einer Sperre ist nur jener Person möglich, die das anlässlich der Sperre vereinbarte Sperraufhebungspasswort, bzw. das Widerrufspasswort kennt.

### 4.4.7 Prozedur für einen Sperrantrag

Eine Sperre kann durch den Signator vorgenommen werden. Dies geschieht dadurch, dass sich der Signator an den Widerrufsdienst wendet.

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

Der Signator kann rund um die Uhr beim Widerrufsdienst eine Sperre vornehmen. Die Authentifikation erfolgt über das Sperr- und Widerrufs-Passwort, welches der Antragsteller bei der Antragstellung selbst festgelegt hat. Desweiteren wird die eindeutige Seriennummer des Zertifikats oder die Signaturvertragsnummer des Signators benötigt. Die für eine Sperre benötigten Informationen lassen sich wie folgt zusammenfassen:

- Signaturvertragsnummer des Signators oder Seriennummer des Zertifikats
- Passwort für Sperre und Widerruf

Sollte der Signator sein Sperr- und Widerrufspasswort vergessen haben und somit eine Authentisierung nicht möglich sein, müssen weitere Daten herangezogen werden. Diese sind:

- der vollständige Name,
- das Pseudonym (falls verwendet),
- das Geburtsdatum und
- der Geburtsort.

Im Rahmen einer Sperre muss der Signator dem Widerrufsdienst ein mindestens vierstelliges Passwort mitteilen, mit dem er die Sperre wieder aufheben lassen kann. Der Widerrufsdienst trägt das Sperraufhebungspasswort in eine Datenbank ein. Das Sperraufhebungspasswort unterscheidet sich vom Sperr- und Widerrufspasswort und dient zur Berechtigungsprüfung für die Aufhebung der Sperre. Wenn die Sperre aufgehoben wurde und die Zertifikate zu einem späteren Zeitpunkt nochmals gesperrt werden, dann ist anlässlich der neuerlichen Sperre auch ein neues Sperraufhebungspasswort zu wählen.

### 4.4.8 Sperraufhebung

Innerhalb der Sperrfrist kann der Signator die Sperre des Zertifikats wieder aufheben. Dazu muss er die Sperraufhebung beim Widerrufsdienst beantragen.

Für die Identifikation muss er sein Sperraufhebungspasswort, das er anlässlich der Bekanntgabe der Sperre gewählt und dem Widerrufsdienst mitgeteilt hat, oder sein Widerrufspasswort angeben. Sollte der Signator die Passwörter nicht nennen können, so kann die Sperre nicht aufgehoben werden.

Das Sperraufhebungspasswort kann gegen Ausweisleitung auch in der Registrierungsstelle erfragt werden.

Weitere benötigte Daten sind die Zertifikats- oder die Signaturvertragsnummer des Signators.

### 4.4.9 Bekanntgabe der Sperre bzw. Sperraufhebung

Die Sperren werden in der Widerrufsliste eingetragen, bei einer Sperraufhebung sind die betreffenden Sperren in der nächsten Widerrufsliste, die nach der Aufhebung ausgestellt wird, nicht mehr enthalten.

### 4.4.10 Grenzen einer Sperrperiode

Die Sperre kann bis 23:00 Uhr des neunten auf den Tag der Sperre folgenden Tags wieder aufgehoben werden, sonst wird sie durch a.trust in einen Widerruf umgewandelt.

### 4.4.11 Aktualisierungsintervalle der Widerrufsliste

Die Intervalle der Aktualisierung der Widerrufsliste sind über die a.trust Web-Seite (http://www.a-trust.at/crl) in Erfahrung zu bringen.

### 4.4.12 Anforderungen an die Überprüfung mittels Widerrufslisten

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

Für eine positive Gültigkeitsüberprüfung ist es erforderlich, dass

- der Zeitpunkt der Ausstellung im Gültigkeitszeitraum des Ausstellerzertifikats liegt,
- das Zertifikat mit einem gültigen Zertifikat der Zertifizierungsstelle signiert wurde und
- sich das Zertifikat nicht in der aktuellen Widerrufsliste befindet.

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

Ausgehend von der Signatur der Widerrufsliste ist der vollständige Zertifizierungspfad auf Gültigkeit zu prüfen. Die von dem Nutzer lokal gespeicherten Zertifikate sollten vor ihrer Nutzung gegen eine aktuelle Widerrufsliste geprüft werden. Sofern keine erfolgreiche Gültigkeitsprüfung vorgenommen werden kann (beispielsweise aus Internet-Verbindungsprobleme), sollten keine Zertifikate akzeptiert werden. Jede Akzeptanz eines solchen Zertifikats erfolgt auf das Risiko des Zertifikatsnutzers.

### 4.4.13 Weitere Möglichkeiten zur on-line Statusabfrage

Es wird ein OCSP-Dienst über das Internet angeboten.

### 4.4.14 Anforderungen an die on-line Statusabfrage

Ein Zertifikatsnutzer sollte die Authentizität der Auskunft des Verzeichnisdiensts durch die Prüfung der in der Antwort enthaltenen Signatur verifizieren. Desweiteren ist der in

der Auskunft enthaltene Zeitpunkt, auf den sich der Status bezieht, mit dem fraglichen Prüfzeitpunkt zu vergleichen.

Sofern keine erfolgreiche Gültigkeitsprüfung vorgenommen werden kann (beispielsweise aus technischen Gründen), sollte das Zertifikat nicht akzeptiert werden. Jede Akzeptanz eines solchen Zertifikats erfolgt auf Risiko des Zertifikatsnutzers.

### 4.4.15 Weitere Verfahren zur Bekanntgabe von Widerrufen

Keine Bestimmungen.

### 4.4.16 Anforderungen an die Überprüfung der weiteren Verfahren zur Bekanntgabe von Widerrufen

Keine Bestimmungen.

### 4.4.17 Spezielle Verfahren bei Kompromittierung von privaten Schlüsseln

Bei Eintritt einer der unter Kapitel 4.4.1 genannten Gründe führt der Signator eine Sperre oder einen Widerruf durch.

## 4.5 Protokollierung sicherheitsrelevanter Ereignisse

### 4.5.1 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 Accounts,
- Änderungen bei der Rollenaufteilung,
- Änderung der Softwarekonfiguration (Installation oder Update von Software), Weiterhin werden alle mit den Systemen durchgeführten Transaktionen zusammen mit Transaktionstyp, Zeitpunkt und Informationen darüber, ob die Transaktion abgeschlossen oder abgebrochen wurde und wer die Transaktion veranlasst hat, protokolliert. Folgende Transaktionstypen sind insbesondere aufzuzeichnen:

- Zertifizierungsanträge,

- Schlüsselerzeugungen,
- Zertifikatserstellungen,
- Veröffentlichung von Zertifikaten und Widerrufslisten,
- Sperr- und Widerrufanträge,
- Ausgeführte Sperren und Widerrufe sowie
- Schlüsselwechsel.

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

- Bestätigung der Belehrung über die Sicherheitsrichtlinien durch den Registration Officer,
- Akzeptanzerklärung der Allgemeinen Geschäftsbedingungen und der Entgeltbestimmungen durch den Signator oder auch
- Änderungen an den personenbezogenen Signatordaten.

### 4.5.2 Intervalle der Überprüfung der Protokolldateien

Die Protokolle, die im laufenden Rechenzentrumsbetrieb erzeugt werden, sind regelmäßig (routinemäßig einmal pro Woche) vom Rechenzentrumspersonal auf verdächtige Vorkommnisse zu untersuchen.

Weiters werden die Protokolle, die sich aus den einzelnen Ablaufprozessen ergeben und die für die Sicherheit der Dienstleistungen von a.trust relevant sind, im Zuge der Revision auf verdächtige Vorkommnisse und Manipulationen untersucht.

### 4.5.3 Aufbewahrungszeitraum der Protokolldateien

Sicherheitsrelevante Protokolldateien werden mind. 35 Jahre 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 4.6.2 festgelegt.

### 4.5.4 Schutz der Protokolldateien

Die Protokolldateien werden an unterschiedlichen Standorten erstellt und im Rechenzentrum elektronisch aufbewahrt. Sie sind nur autorisiertem Personal zugänglich zu machen. Die Protokolldateien werden mittels digitaler Signatur vor Modifikationen geschützt.

### 4.5.5 Protokollierungssystem (intern / extern)

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

### 4.5.6 Benachrichtigung beim Auftreten sicherheitskritischer Ereignisse

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

### 4.5.7 Bewertungen zur Angreifbarkeit

Keine Bestimmungen.

## 4.6 Archivierung

### 4.6.1 Archivierte Daten

Archiviert werden:

- Persönliche Signatordaten, die zur Zertifizierung verwendet wurden (Lichtbildausweis),
- Zertifizierungsanträge (Antragstellerformular und Vertrag),
- alle von der Zertifizierungsstelle ausgestellten Zertifikate (Zertifikate der Zertifizierungsstelle und Dienste und Zertifikate der Signatoren),
- Sperr- und Widerrufanträge mit Datum und Uhrzeit des Eintreffens (inklusive entsprechender Protokolldateien),
- alle ausgestellten Widerrufslisten,
- Datum und Uhrzeit der Veröffentlichung der Zertifikate und Widerrufslisten (inklusive entsprechender Protokolldateien) und
- Datum und Uhrzeit von Schlüsselwechseln der Zertifizierungsstelle.

Im Zuge einer Onlineaktivierung werden die signierten Identifikationsdaten archiviert. Je nach Art der Aktivierung werden vom RO signierte Ausweisdaten oder Daten, die zur Identifikation des Signators herangezogen werden, archiviert.

Zusätzlich werden die Anträge auf Ausstellung des Zertifikats und die Registrierungsunterlagen für den in Abschnitt 4.6.2 genannten Zeitraum aufbewahrt.

### 4.6.2 Aufbewahrungszeiten

Die Aufbewahrungszeiten richten sich nach dem Signaturgesetz und betragen mindestens 30, aber maximal 35 Jahre (5 Jahre maximale Zertifikatsgültigkeit + 30 Jahre).

Für die einzelnen Aufbewahrungszeiten sind folgende Aspekte zu berücksichtigen:

- Die Daten müssen mindestens so lange aufbewahrt werden, wie sie im Anwendungszeitraum benötigt 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. Zu diesem Zweck werden ausschließlich technische Formate verwendet, deren zugrunde liegende Spezifikationen öffentlich verfügbar sind.

### 4.6.3 Schutzvorkehrungen

Das Archiv befindet sich in gesicherten Räumlichkeiten. Der Zugriff ist nur autorisierten Personen gestattet. Die archivierten Protokolldateien sind entsprechend den Richtlinien aus Abschnitt 4.5.4 geschützt.

Elektronische Dokumente sind durch digitale Signaturen vor Modifikationen geschützt.

Systemzugriff auf das Archiv, zu Administrationszwecken, ist ausschließlich im “4-Augen Prinzip” autorisierter Personen möglich.

### 4.6.4 Anforderungen, die Daten mit Echtzeitangaben zu versehen

Alle Zertifikatsanträge sind mit einer Echtzeitangabe versehen. Dies betrifft insbesondere die Sperr- und Widerrufsanträge sowie die Ausstellung der Widerrufslisten.

### 4.6.5 System zur Erfassung der Archivierungsdaten (intern / extern)

Das System für das Zertifikatsmanagement ist für die Archivierung aller zu archivierenden Daten verantwortlich. Ausgenommen davon sind die Originalunterlagen, welche in der Registrierungsstelle aufgehoben werden.

### 4.6.6 Prozeduren zum Abrufen und Überprüfen von Daten

Bei Archivierung von elektronischen Daten über lange Zeiträume ist damit zu rechnen, dass 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 bei Einstellung der Tätigkeit der Zertifizierungsstelle über den festgelegten Archivierungszeitraum bestehen bleibt.

## 4.7 Schlüsselwechsel von CA- und Root-Schlüssel

Ein Schlüsselwechsel erfolgt im Zusammenhang mit dem Ausfall eines Hardware Security Moduls oder wenn die verwendeten Schlüssellängen bzw. Algorithmen nicht mehr den Sicherheitsanforderungen entsprechen sollten oder aber im Falle einer nicht vorhersehbaren Kompromittierung von Schlüsseln. In letzterem Fall ist unbedingt ein Widerruf der betroffenen Zertifikate erforderlich. Die Gründe für den Widerruf von Root- und CA-Zertifikaten sind in Kapitel 4.8.2 aufgelistet. Die Zertifizierungsstellen erneuern außerdem regelmäßig ihre Zertifikate. Dies sollte vor dem Ablauf der im Zertifikat festgelegten Gültigkeitsdauer geschehen. Rechtzeitig vor der Erneuerung wird dies auf der Web-Seite (siehe Abschnitt 2.6.6) angekündigt. Die Gültigkeitsdauer der Zertifikate ist Kapitel 6.3 zu entnehmen.

Der Überprüfer eines Zertifikats erhält das neue Zertifikat über den Verzeichnisdienst. Er kann über die Zertifizierungskette die Gültigkeit des Zertifikats überprüfen.

Um sich von der Authentizität des Zertifikats der Root-CA zu überzeugen hat der Signator die Möglichkeit der Abfrage des in den Medien (Wiener Zeitung) oder auf der a.trust-Homepage veröffentlichten Fingerprints des öffentlichen Schlüssels.

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

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

Hinsichtlich der Generierung und Aufbewahrung im Hardware Security Modul gibt es keinen Unterschied zwischen dem CA-Schlüssel (Zertifizierungsschlüssel für Zertifikate der Signatoren) und dem Root-CA-Schlüssel (Zertifizierungsschlüssel für Zertifikate der Zertifizierungsstellen).

## 4.8 Kompromittierung und Notfallplan

### 4.8.1 Rechner, Software und/oder Daten sind korrumpiert

Regelungen bei Kompromittierung bzw. Verdacht auf Kompromittierung von Schlüsseln sind in Abschnitt 4.8.3 aufgeführt.

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

Bei Zertifikaten sind die betroffenen Signatoren zu informieren. Es erfolgt ein unmittelbarer Widerruf der betroffenen Zertifikate, falls die fehlerhaften Angaben im Zertifikat sind.

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 die Publikation unkorrekter Daten zu verhindern. Die Wiederaufnahme des Dienstes ist mit der Veröffentlichung der neuen Widerrufsliste verbunden. In Abhängigkeit der Fehler und der Ausfallzeit der Verzeichnisdienste werden die Anwender informiert.

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

### 4.8.2 Widerruf von Zertifikaten zu Zertifizierungsstellen- und Dienste-Schlüsseln

Zertifikate der Zertifizierungsstelle werden in den folgenden Fällen widerrufen:

- bei Kompromittierung oder Verdacht auf Kompromittierung der entsprechenden Schlüssel,
- wenn die eingesetzten Algorithmen nicht mehr den Sicherheitsanforderungen entsprechen, so dass eine sichere Anwendung nicht gewährleistet werden kann oder
- 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 4.8.3 zu berücksichtigen. Bei Widerruf des Zertifikats wegen Einstellung der Tätigkeit der Zertifizierungsstelle ist Abschnitt 4.9 zu beachten.

Ist ein Widerruf geplant, so werden die Signatoren rechtzeitig über den bevorstehenden Widerruf informiert. Ein ungeplanter Widerruf erfordert eine umgehende Benachrichtigung der Signatoren. 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 gelöscht.

### 4.8.3 Widerruf von Zertifikaten der Dienste

Werden Zertifikate der Dienste der Zertifizierungsstelle (das sind Verzeichnis- und Widerrufsdienst) widerrufen, so werden die Dienste ohne gültigen Schlüssel (CA-Schlüssel zur Signatur von Zertifikaten und CRLs) 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.

### 4.8.4 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.

### 4.8.5 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 4.7 durchgeführt, die sich aber in folgenden Punkten von einem regulären Wechsel unterscheidet:

- Eine rechtzeitige Information der Signatoren über den Schlüsselwechsel ist bei einem unmittelbaren Widerruf nicht möglich. Die Signatoren werden im Zusammenhang mit der Widerrufsinformation auch umgehend über den Schlüsselwechsel informiert.
- Es findet keine Zertifizierung anderer Schlüssel der Zertifizierungsstelle mit dem ungültigen Zertifikat statt. Die Signatoren 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.

### 4.8.6 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 erfolgt das Abschalten des Verzeichnisdiensts und die Einstellungen 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.

### 4.8.7 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.

## 4.9 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 Benachrichtgung 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. Eine darüber hinausgehende Übertragung der Verpflichtung an Drittparteien ist nicht notwendig.

# 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<br>Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH.<br>Landstraßer Hauptstraße 5<br>A-1030 Wien |
| Registrierung, Widerrufsdienst | Die Registrierungsstellen und den Widerrufsdienst finden Sie auf der Web-Seite der a.trust https://www.a-trust.at/ veröffentlicht. |
| Zertifizierung, Brief-Versand (Antragstellerformular, Sperr- und Widerrufsinformation, PUKs, etc.) | Raiffeisen Informatik<br>Obere Donaustraße 37<br>A-1020 Wien<br><br>Ausfallrechenzentrum:<br>Raiffeisen Informatik<br>Friedrich Wilhelm Raiffeisen Platz 1<br>A-1020 Wien |
| Kartenproduktion<br>Initialisierung<br>Zentrale Personalisierung | Austria Card<br>Lamezanstr. 4-8<br>A-1232 Wien<br><br>Giesecke & Devrient GmbH<br>Prinzregentenstraße 159<br>D-81677 Munich |

Tabelle 2: Örtlichkeiten

### 5.1.2 Zugangskontrollen

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

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

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

### 5.1.3 Stromversorgung und Klimaanlage

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

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

### 5.1.4 Wasserschäden

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

### 5.1.5 Feuer

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

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

### 5.1.6 Datenträger

Als Datenträger werden folgende Medien eingesetzt:

- Papier
- Festplatten
- DVDs
- WORMs

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

### 5.1.7 Müllentsorgung

Die Daten auf den elektronischen Datenträgern werden sachgemäß vernichtet und die Datenträger dann einem spezialisierten Unternehmen zur sachgerechten Entsorgung übergeben. Papierdatenträger werden in vorhandenen Aktenvernichtern entsorgt oder einem spezialisierten Unternehmen zur sachgemäßen Entsorgung übergeben.

### 5.1.8 Redundante Auslegung

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

## 5.2 Verfahrensorientierte Sicherheitsvorkehrungen

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

### 5.2.1 Funktionen der a.trust

| Rolle | Funktion |
|---|---|
| Geschäftsführung | Kommerzieller Erfolg des Unternehmens<br>Marketing und Vertrieb<br>Betrieb<br>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<br>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

### 5.2.3 Sonstige (nicht sicherheitskritische) Funktionen

### 5.2.4 Anzahl erforderlicher Personen für sicherheitsrelevante Tätigkeiten

Tabelle 6 stellt sicherheitsrelevante Tätigkeiten dar und ordnet diesen die dafür zuständigen Rollen zu. Weiters wird aufgezeigt, ob für diese Tätigkeit das Vieraugenprinzip notwendig ist und ob diese Tätigkeit im Hochsicherheitsbereich des a.trust Rechenzentrums ausgeübt wird.

| Tätigkeit | Personen | Vier-augen-prinzip | Hoch-sicher-heit |
|---|---|---|---|
| Registrierung und Identifizierung von Zertifikatswerbern | RO | Nein | Nein |

| Tätigkeit | Personen | Vier-augen-prinzip | Hoch-sicher-heit |
|---|---|---|---|
| Widerrufen von Anwenderzertifikaten | RCA, RO | Nein | Nein |
| Erzeugung der Schlüssel für Root-CA und Zertifizierungsstellen sowie Schlüsselwechsel | SO, SO | Ja | Ja |
| Aktivierung der Schlüssel für Root-CA und Zertifizierungsstellen | SO, SO | Ja | Ja |
| Löschen der Schlüssel für Root-CA und Zertifizierungsstellen | SO, SO | Ja | Ja |
| Zertifizierung für die Root-CA und die Zertifizierungsstellen | SO, SO | Ja | Ja |
| Widerruf von Zertifikaten der CA | SO, SO | Ja | Ja |
| Vergabe der Berechtigungen für RO und RCA | SO, SO | Ja | Ja |
| Inbetriebnahme eines kryptographischen Moduls (Signaturerstellungseinheit der CA) | SO, SO | Ja | Ja |
| Ab- und Anschalten von Komponenten, insbesondere Verzeichnisdiensten | Sicherheitssystem-administrator | Nein | Nein |
| Austausch von Hardware-Komponenten | Sicherheitssystem-administrator (2x) | Ja | Ja |
| Austausch von Software-Komponenten | Sicherheitssystem-administrator (2x) | Ja | Ja |
| Überprüfung von Protokolldateien auf verdächtige Vorkommnisse | Systemadministrator | Nein | Nein |
| Überprüfung der Protokolldateien auf Manipulation | Systemadministrator | Nein | Nein |
| Anfertigung eines Backups der Protokolldateien und Lagerung desselben | Sicherheitssystem-administrator (2x) | Ja | Ja |
| Qualitätsprüfung der verwendeten Schlüssellängen und Parameter zur Schlüsselerzeugung | SO | Nein | Nein |
| Wartung oder Austausch eines kryptographischen Moduls | SO, SO | Ja | Ja |

Tabelle 6: Anzahl erforderlicher Personen

| Rolle | Funktion |
|---|---|
| Sicherheitsbeauftragter | siehe Tabelle 3 |
| Revision | siehe Tabelle 3 |
| Datenschutz | siehe Tabelle 3 |
| Security Officer (SO) | Zutritt in die Hochsicherheitszone<br>Verantwortlichkeit für die Generierung und Zertifizierung der Schlüssel von a.trust und Widerruf dieser Zertifikate<br>Verwaltung der Hardware Security Module<br>Vergabe der RO- und RCA-Berechtigung<br>Ansprechpartner für sicherheitsrelevante Fragen<br>Beaufsichtigung der Einhaltung der im CPS festgelegten Vorgehensweisen |
| Sicherheits-systemadministrator | Zutritt in die Hochsicherheitszone<br>Beaufsichtigung von Systemadministrator und Systemoperator |
| Revocation Center Agent (RCA),<br>Mitarbeiter im Widerrufsdienst | Ansprechpartner für die Zertifikatsinhaber hinsichtlich der Annahme von Anträgen für Widerruf und Sperre |
| Registration Officer (RO),<br>Mitarbeiter der Registrierungsstelle | Entgegennahme von Zertifikatsanträgen Identifikation von Zertifikatswerbern im Rahmen der Registrierung Belehrung der Zertifikatsinhaber |

Tabelle 4: Sicherheitskritische Funktionen

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

Tabelle 5: Sonstige Funktionen

### 5.2.5 Identifikation 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

Gemäß SigV §10 (4) dürfen im Rahmen der bereitgestellten Signatur- und Zertifizierungsdienste keine Personen beschäftigt werden, die wegen einer mit Vorsatz begangenen strafbaren Handlung zu einer Freiheitsstrafe von mehr als einem Jahr oder wegen strafbarer Handlungen gegen das Vermögen oder gegen die Zuverlässigkeit von Urkunden und Beweiszeichen zu einer Freiheitsstrafe von mehr als drei Monaten verurteilt wurden. Verurteilungen, die nach den Bestimmungen des Tilgungsgesetzes 1972 getilgt sind oder der beschränkten Auskunft unterliegen, bleiben außer Betracht.

### 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.

Im Hinblick auf die Qualitätssicherung der a.trust Dienstleistungen wird auf die Schulung der Mitarbeiter der Registrierungsstelle und des Widerrufsdienstes als primäre Schnittstelle zum Signator besonderer Wert gelegt.

Die Mitarbeiter der Registrierungsstelle müssen einen, vom a.trust Schulungsbeauftragten abgehaltenen, Kurs absolvieren, der die Grundvoraussetzung für die Ausübung der Rolle des RO darstellt. In jeder RA stehen außerdem speziell geschulte Zentrale Registration Officer zur Verfügung, die die anderen ROs bei Problemen und Fragen unterstützen. Jeder RO hat außerdem Checklisten und Merkblätter zur Verfügung, die ihn in standardisierter Weise durch den Registrierungsprozesses durchführen sollen.

Auch die Mitarbeiter des Widerrufsdienstes (RCA) erhalten eine Einschulung durch den a.trust Schulungsbeauftragten. Weiters erhalten sie die für ihre Tätigkeit benötigten Unterlagen (Betriebskonzept für den Widerrufsdienst) und ebenfalls eine standardisierte Aufstellung des Ablaufs der Kommunikation mit dem Signator.

### 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 je nach Örtlichkeit und Rolle,
- Sicherheitskonzept,
- Zertifizierungsrichtlinie und
- Schulungsunterlagen.

# 6 Technische Sicherheitsvorkehrungen

## 6.1 Schlüsselgenerierung und Installation

### 6.1.1 Schlüsselgenerierung

#### 6.1.1.1 Schlüssel der Signatoren

Die Schlüssel werden in einer sicheren Signaturerstellungseinheit erzeugt und nur in verschlüsselter Form gespeichert. Siehe auch Kapitel 6.2.1.

#### 6.1.1.2 Schlüssel der Zertifizierungsstelle

Die Schlüssel der Zertifizierungsstelle werden im Hardware Security Modul in der Zertifizierungsstelle generiert. Für die geheimen Schlüssel der Zertifizierungsstelle gibt es keine Exportmöglichkeit und auch keine Backups. Die Erzeugung von Schlüsseln in der Zertifizierungsstelle erfolgt immer unter der Aufsicht von zwei befugten a.trust Mitarbeitern und muss von der Geschäftsführung der a.trust angeordnet werden.

### 6.1.2 Zurverfügungsstellung privater Schlüssel

Der private Signaturschlüssel verläßt die sichere Signaturerstellungseinheit im Rechenzentrum des Zertifizierungsdiensteanbieters nie. Der private Signaturschlüssel kann nur durch die korrekte Eingabe des Signaturpasswortes und Verifikations-SMS benutzt werden. Dieses Wissen besitzt nur der Signator.

### 6.1.3 Zurverfügungsstellung öffentlicher Schlüssel an Zertifikatsaussteller

Alle Schlüssel der Zertifizierungsstelle werden zentral erzeugt und müssen deshalb nicht an die Zertifizierungsstelle ausgeliefert werden.

### 6.1.4 Zurverfügungsstellung öffentlicher Schlüssel von der Zertifizierungsstelle an die Signatoren

Das Zertifikat des Schlüssels der Root-CA sowie aller Zertifizierungsstellen werden in einem Verzeichnis im Internet veröffentlicht, damit es allgemein zugänglich ist und alle Zertifikatsnutzer Zertifikate dagegen prüfen können. Ein Fingerprint des öffentlichen Schlüssels der Root-CA wird außerdem in einer Ausgabe der Wiener Zeitung veröffentlicht.

### 6.1.5 Schlüssellängen

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

Der von a.trust zur Erstellung der Signatur über die Zertifikate und Widerrufslisten verwendete Hash-Algorithmus ist SHA-1.

Die ECDSA-Schlüssel der Signatoren entsprechen einer Länge von zurzeit 256 Bit.

Diese Mindestlängen können sich ändern, wenn die eingesetzten Algorithmen nicht mehr den Sicherheitserwartungen entsprechen oder sich die gesetzlichen Vorgaben ändern.

### 6.1.6 Parameter zur Schlüsselerzeugung

Für ECC-Schlüssel werden die Anforderungen an die ECC Schlüsselgenerierung lt. ANSI X9.62, The Elliptic Curve Digital Signature Algorithm (ECDSA), Abschnitt 'Key Pair Generation' erfüllt (siehe [ANSI X9.62]). Die verwendete Kurve ist für prime256v1 gem. [ANSI X9.62].

### 6.1.7 Qualitätsprüfung der Parameter

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

### 6.1.8 Hardware/Software Schlüsselerzeugung

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

Die Schlüssel der Signatoren werden in der sicheren Signaturerstellungseinheit im Rechenzentrum des Zertifizierungsdiensteanbieters erzeugt.

### 6.1.9 Verwendungszweck der Schlüssel (nach X.509 v3 usage Feld)

Der Verwendungszweck für den zertifizierten Schlüssel wird in den X.509 V3 Zertifikaten in der Extension „keyUsage“ angegeben.

#### 6.1.9.1 Verwendung der Schlüssel der Root-CA

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

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

gesetzt sind.

#### 6.1.9.2 Verwendung der Schlüssel der Zertifizierungsstellen

Die Schlüssel der Zertifizierungsstelle werden ausschließlich zum Signieren von Zertifikaten und Widerrufslisten eingesetzt. Deshalb werden die Bits

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

gesetzt.

#### 6.1.9.3 Verwendung des Schlüssels des Signators

Der Schlüssel des Signators dient zur Erstellung einer digitalen Signatur. Deshalb werden die Bits

- nonRepudiation und
- digitalSignature

gesetzt.

## 6.2 Schutz der privaten Schlüssel

### 6.2.1 Standards des kryptografischen Moduls

#### 6.2.1.1 Schlüssel der Zertifizierungsstelle

Als kryptografische Module werden Hardware Security Module eingesetzt.

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

Der Schlüssel einer Zertifizierungsstelle dient zur Signatur von Zertifikaten und Widerrufslisten. Er wird nur in einer sicheren Umgebung eingesetzt.

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

#### 6.2.1.2 Schlüssel der Signatoren

Die Schlüssel der Signatoren werden auf einer den Anforderungen entsprechenden sicheren Signaturerstellungseinheit gespeichert. Es handelt sich hierbei um eine von einer Bestätigungsstelle (wie z.B. A-SIT) nach §18(5) [SigG] bescheinigtes System, welche eine sichere Signaturerstellungseinheit darstellt und die Erzeugung und Speicherung der Signaturerstellungsdaten ermöglicht.

### 6.2.2 Aufteilung privater Schlüssel auf mehrere Personen

#### 6.2.2.1 Schlüssel der Zertifizierungsstelle

Die privaten Schlüssel befinden sich in einem Hardware Security Modul. Für die Aktivierung des Schlüssels der Root-CA oder einer Zertifizierungsstelle ist ein Vieraugenprinzip erforderlich. Eine einzelne Person darf nicht über die Mittel verfügen, einen dieser privaten Schlüssel zu nutzen.

#### 6.2.2.2 Schlüssel der Signatoren

Für Signatorenschlüssel ist ausschließlich die Kontrolle einer einzelnen Person, des Signators, gefordert.

### 6.2.3 Hinterlegung privater Schlüssel

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

### 6.2.4 Backup privater Schlüssel

Es gibt keine Backup-Möglichkeiten - weder für private Schlüssel der Zertifizierungsstelle noch für Signaturschlüssel von Signatoren.

### 6.2.5 Archivierung privater Schlüssel

Eine Archivierung privater Schlüssel findet nicht statt.

### 6.2.6 Einbringung privater Schlüssel in das kryptografische Modul

Die eingesetzte kryptografische Hardware ist so beschaffen, dass die privaten Schlüssel nur innerhalb dieses Mediums generiert werden können.

#### 6.2.6.1 Schlüssel der Zertifizierungsstelle

Die privaten Schlüssel der Zertifizierungsstelle zum Signieren von Zertifikaten und Widerrufslisten werden in einem Hardware Security Modul erzeugt und dort gespeichert. Die Anwendung erfolgt ebenfalls direkt im Hardware Security Modul. Das gilt in gleicher Weise für den Root-Schlüssel wie auch die Schlüssel der Zertifizierungsstelle zur Signatur der qualifizierten Anwenderzertifikate.

#### 6.2.6.2 Schlüssel der Signatoren

Die privaten Signaturschlüssel der Signatoren werden in einer sicheren Signaturerstellungseinheit im Hochsicherheitsbereich des Zertifizierungsdiensteanbieters generiert und sind vor dem Auslesen geschützt.

### 6.2.7 Methode zur Nutzung privater Schlüssel

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

Die Schlüssel der Signatoren werden durch ein Signaturpassword und eine Verifikations-SMS geschützt.

### 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.

Die privaten Schlüssel der Signatoren werden deaktiviert, wenn die vorgegebene Anzahl von Fehlversuchen bei der Signaturauslösung überschritten wird.

### 6.2.9 Methode zur Vernichtung privater Schlüssel

Der Signator hat die Option den zu einem Widerrufenen oder abgelaufenen Zertifikat gehörenden Schlüssel über eine Serviceseite löschen zu lassen.

## 6.3 Verwendungszeitraum öffentlicher und privater Schlüssel

Als Gültigkeitsmodell wird das Kettenmodell eingesetzt. Zur Überprüfung der Gültigkeit eines Zertifikats wird dabei die übergeordnete Instanz herangezogen. Dabei muss das übergeordnete Zertifikat nur zum Zeitpunkt der Ausstellung des zu überprüfenden Zertifikats gültig gewesen sein. Ein übergeordnetes Zertifikat kann widerrufen werden, ohne dass die ihm untergeordneten, und vor dem Widerruf ausgestellten, Zertifikate dadurch ihre Gültigkeit verlieren.

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

| Zertifikatstyp | Gültigkeitsdauer |
|---|---|
| Root-CA | 10 |
| Zertifizierungsstellen | 10 |
| Zertifikatsinhaber | 10 |

Tabelle 7: Gültigkeitsdauer von Zertifikaten

Eine Verlängerung der Gültigkeitsdauer eines Zertifikats (erneute Zertifizierung des öffentlichen Schlüssels) kann erfolgen, wenn die kryptografische Sicherheit der verwendeten Verfahren über die gesamte neue Gültigkeitsdauer ausreichend sicher gestellt ist und keine Hinweise auf Kompromittierung des zugehörigen privaten Schlüssels bestehen.

## 6.4 Aktivierungsdaten

### 6.4.1 Erzeugung und Installation der Aktivierungsdaten (PINs)

#### 6.4.1.1 Aktivierungsdaten für Schlüssel der Zertifizierungsstelle

Die Schlüssel der Zertifizierungsstelle können ausschließlich im Vieraugenprinzip durch zwei Beauftragte mittels Chipkarte und PIN aktiviert werden. Die Aktivierungsdaten werden direkt in einem HSM vom CA-System erzeugt. Erzeugte Aktivierungsdaten werden nicht schriftlich festgehalten.

Es werden genügend Chipkarten zur Aktivierung erzeugt, damit die Schlüssel der Zertifizierungsstelle nicht durch Zerstörung oder Verlust von Chipkarten unbrauchbar werden.

#### 6.4.1.2 Aktivierungsdaten für Schlüssel der Signatoren

Die Signatoren aktivieren ihren privaten Schlüssel über ein Signaturpasswort und eine Verigikations-SMS.

### 6.4.2 Schutz der Aktivierungsdaten

#### 6.4.2.1 Aktivierungsdaten für Schlüssel der Zertifizierungsstelle

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

#### 6.4.2.2 Aktivierungsdaten für Schlüssel der Signatoren

Das Signaturpassowrt wird nur gehashed gespeichert.

Das selbst gewählte Signatur-Passwort jedes a.sign premium mobile Signators ist niemand anderem als dem Signator bekannt und vom Signator unbedingt entsprechend geheim zu halten.

### 6.4.3 Weitere Aspekte zu den Aktivierungsdaten

Keine Bestimmungen.

## 6.5 Computer Sicherheitsbestimmungen

### 6.5.1 Spezifische Sicherheitsanforderungen an die Computer

Keine Bestimmungen.

### 6.5.2 Bewertung der Computersicherheit

Keine Bestimmungen.

## 6.6 Life-Cycle der Sicherheitsvorkehrungen

### 6.6.1 Systementwicklung

Die Vorgaben zur Systementwicklung orientieren sich an den Sicherheitsvorgaben der a.trust. Die folgenden Richtlinien müssen bei der Entwicklung eingehalten werden:

- Das Entwicklungssystem muss vom Echtsystem getrennt sein
- Die Übernahme der neu entwickelten/geänderten Software in das Echtsystem findet nach erfolgreich abgeschlossenem Test und nach erteilter Freigabe durch die Betriebsleitung statt.

### 6.6.2 Sicherheitsmanagement

Bestimmte organisatorische Regelungen hinsichtlich der Benutzung von Software müssen eingehalten werden:

- benutzt wird ausschließlich freigegebene Software aus bekannten Quellen,
- die Möglichkeit des unautorisierten Einspielens von Software wird verhindert,
- die Integrität von Standardsoftware wird sicher gestellt,

- Software-Bestände werden regelmäßig überprüft,
- Lizenzverwaltung und Versionskontrolle von Software werden durchgeführt,
- Mitarbeiter werden vor der Programmnutzung auf die Verwendung geschult,
- Handbücher müssen in ausreichender Zahl zur Verfügung stehen,
- Original-Software-Versionen werden sicher aufbewahrt,
- ggf. werden Sicherungskopien von Software angelegt,
- unerlaubte Zugriffe auf Software z.B. zur Erstellung von Raubkopien müssen verhindert werden,
- Regelungen für den Betrieb werden erlassen (Durchführung von Datensicherungen, Wechsel von Passwörtern).

### 6.6.3 Bewertung

Für die Bewertung von Software sind die folgenden Tätigkeiten durchzuführen:

- Entwicklung eines Testplans für Software,
- Testen der Software,
- Freigabe der Software.

## 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 kryptografischen Moduls

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

# 7 Profile von Zertifikaten und Widerrufslisten

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

## 7.1 Zertifikatsprofile

### 7.1.1 CA-Zertifikate

| **Attribut** | **Inhalt** | **Erläuterung** |
|---|---|---|
| Version | v3(2) | Die Versionsnummer wird auf '2' gesetzt, um ein X.509 Zertifikat der Version 3 anzuzeigen |
| Seriennummer | Seriennummer des Zertifikats | Eindeutig innerhalb der a.trust Zertifizierungsinfrastruktur |
| Algorithmus | $\geq$ SHA-1 | Für die Signatur über das Zertifikat verwendeter Algorithmus |
| Aussteller des Zertifikats | CN = CommonName<br>OU = OrganizationalUnit<br>O = Organization<br>C = AT | CommonName, OrganizationalUnit:<br>A-Trust-Qual-nn<br>Organization:<br>A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH<br>(für CA-Version 01): A-Trust |
| Gültig von<br>Gültig bis | Beginn und Ende der Gültigkeit des Zertifikats | Der Gültigkeitszeitraum beträgt höchstens zehn Jahre |
| Zertifikatsinhaber | CN = CommonName<br>OU = OrganizationalUnit<br>O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH<br>C = AT | CommonName, OrganizationalUnit:<br>a-sign-premium-mobile-sig-nn<br>-nn bezeichnet die Generation der CA |
| Öffentlicher Schlüssel | $\geq$ RSA 2048 Bit | Öffentlicher Schlüssel des Zertifikatsinhabers (der CA) |

Tabelle 8: Profil für CA-Zertifikat

### 7.1.2 Zertifikate der Zertifikatsinhaber

| Attribut | Inhalt | Erläuterung |
|---|---|---|
| Version | v3(2) | Die Versionsnummer wird auf '2' gesetzt, um ein X.509 Zertifikat der Version 3 anzuzeigen |
| Seriennummer | Seriennummer des Zertifikats | Eindeutig innerhalb der a.trust Zertifizierungsinfrastruktur |
| Algorithmus | $\geq$ SHA-1 | Für die Signatur über das Zertifikat verwendeter Algorithmus |
| Aussteller des Zertifikats | CN = CommonName<br>OU = OrganizationalUnit<br>O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH<br>C = AT | CommonName, OrganizationalUnit: a-sign-premium-mobile-sig-nn<br>-nn bezeichnet die Generation der CA. |
| Gültig von<br>Gültig bis | Beginn und Ende der Gültigkeit des Zertifikats | Der Gültigkeitszeitraum beträgt höchstens zehn Jahre |
| Zertifikatsinhaber (subject) | C = CountryName<br>T = Title<br>SN = SurName<br>G = GivenName<br>CN = CommonName<br>Seriennummer = SerialNumber<br>O = OrganizationName<br>OU = OrganizationalUnitName | CountryName: AT etc., enthält das Land, in dem das zur Registrierung vorgelegte Identifikationsdokument ausgestellt wurde. Title: Titel (Dr. etc.)<br>SurName: Zuname<br>GivenName: Vorname<br>CommonName: entweder Vorname + Zuname oder Pseudonym<br>Titel, Zuname, Vorname entfallen bei Verwendung eines Pseudonyms |
| Öffentlicher Schlüssel | $\geq$ ECC 192 Bit | Öffentlicher Schlüssel des Zertifikatsinhaber |

Tabelle 9: Profil für a.sign premium mobile Zertifikate

### 7.1.3 Erweiterungen (certificate extensions)

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

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

Tabelle 10: Erweiterungen (CA-Zertifikate)

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

| Erweiterung | Im Zertifikat vorhanden | Klassifikation | |
|---|---|---|---|
| | | kritisch | nicht kritisch |
| **Standarderweiterungen** | | | |
| authorityKeyIdentifier | Ja | | X |
| subjectKeyIdentifier | Ja | | X |
| keyUsage | Ja | X | |
| certificatePolicies | Ja | | X |
| basicConstraints | Ja | | X |
| cRLDistributionPoints | Ja | | X |
| subjectAltName | optional | | X |
| **Private Extensions** | | | |
| authorityInfoAccess | Ja | | X |
| qc-Statement | Ja | X | |
| 1.2.40.0.10.1.1.1 | Ja | | X |

Tabelle 11: Erweiterungen a.sign premium mobile Zertifikat

Die Erweiterung subjectDirectoryAttributes enthält bei a.sign premium mobile Zertifikaten optional das Geburtsdatum des Signators, verpflichtend bei Minderjährigen.

Die Codierung der Object Identifier der anzuwendenden Policies ist in Kapitel 7.1.5 beschrieben.

Optional können a.sign premium mobile Zertifikate eine Zertifikatserweiterung enthalten, welche den Signator als Mitarbeiter einer Behörde ausweist (Behördenkennzeichen – OID 1.2.40.0.10.1.1.1). In dieser Erweiterung kann weiters optional auch ein Verwaltungsbezeichner enthalten sein, der die Zugehörigkeit zu einer Organisationseinheit der öffentlichen Verwaltung angibt.

### 7.1.4 Identifikation der Policy

Hier werden die Policies, die durch diese Zertifizierungsrichtlinie abgedeckt werden, benannt:

Die Erweiterung certificatePolicies im Zertifikat wird mit

- OID 0.4.0.1456.1.1 gem. [ETSI]
  itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(1456) policy-identifiers(1) qcp-public-with-sscd (1)

und mit

- OID 1.2.040.0.17.1.20 gem. [Policy]
  1.2.040.0.17 (a.trust).1 (Policy).20 (a.sign premium mobile)

codiert.

### 7.1.5 Semantik für die Verfahrensweise bei Certificate Policy Extension

Da die Extension certificatePolicies als "nicht-kritisch" markiert ist, sind keine weiteren Bestimmungen diesbezüglich erforderlich.

## 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 Nachsignieren

Keine Bestimmungen.

# 9 Administration dieser Spezifikation

## 9.1 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 betreffen 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.

## 9.2 Verfahren zur Publizierung und Bekanntgabe

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

## 9.3 Genehmigung und Eignung einer Zertifizierungsrichtlinie

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

# A Anhang

## A.1 Begriffe und Abkürzungen

| | |
|---|---|
| Aktivierungsdaten | Daten, die zur Aktivierung der Schlüssel benötigt werden (PIN). |
| Anwender | Person, die die Dienstleistungen der Zertifizierungsstelle der a.trust nutzt. Anwender sind sowohl Zertifikatsinhaber als auch Zertifikatsnutzer. |
| Audit | Von externen Personen durchgeführte Sicherheitsüberprüfung. |
| CA (Certification Authority), Zertifizierungsdiensteanbieter | Eine Person oder Stelle, die Zertifikate ausstellt oder anderweitige elektronische Signaturdienste öffentlich anbieten darf. |
| CA-Schlüssel | Schlüssel der CA, die zur Ausstellung von Zertifikaten und dem Unterschreiben von Widerrufslisten (Zertifizierung) verwendet werden. |
| CA-Zertifikat, Zertifizierungsstellenzertifikat | Zertifikat der Zertifizierungsstelle, das zur Signatur der Zertifikate der Signatoren und der zugehörigen CRLs dient |
| Certification Policy, Policy | Ein Regelwerk, das den Einsatzbereich eines Zertifikates für eine bestimmte Benutzergruppe und/oder Anwendungsklasse festhält. |
| Certification Practice Statement, CPS, Zertifizierungsrichtlinie | Aussagen über die bei der Ausstellung von Zertifikaten von einem Zertifizierungsdiensteanbieter eingehaltenen Vorgehensweise |
| Dienste (CA-Dienste) | Überbegriff für angebotene Dienstleistungen wie Verzeichnisdienst, Statusauskunft und Zeitstempeldienst |
| Dienste-Schlüssel | Schlüssel eines Dienstes (z. B. Signaturschlüssel zur Signatur von Statusauskünften) |
| Digitale Signatur | Elektronische Signatur, die mit Hilfe von Verfahren der asymmetrischen Kryptographie erzeugt wird. |
| E-Mail | Electronic Mail; Nachrichten, die in digitaler Form über computerbasierte Kommunikationswege versandt oder empfangen werden. |
| Elektronische Signatur | Eine Signatur in digitaler Form, die in Daten enthalten ist, Daten beigefügt wird oder logisch mit ihnen verknüpft ist und von einem Unterzeichner verwendet wird, um zu bestätigen, dass er den Inhalt dieser Daten billigt. Sie ist so mit den Daten verknüpft, dass eine nachträgliche Veränderung der Daten offenkundig wird. |
| Gültigkeitsmodell | Modell, nach dem die Prüfung der Gültigkeit von Zertifikaten und Signaturen vorgenommen wird. |

| | |
|---|---|
| Hardware Security Modul, HSM | Elektronisches System zur sicheren Speicherung von Schlüsseln und zur Berechnung und Verifizierung von Signaturen. |
| Integrität (von Daten) | Ein Zustand, in dem Daten weder von Unbefugten verändert noch zerstört wurden. |
| 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. |
| Kompromittierung | Eine unautorisierte Offenlegung von oder der Verlust der Kontrolle über sicherheitskritische Informationen und geheim zuhaltende Daten. |
| LDAP | Lightweight Directory Access Protocol ist ein Standard protokoll für Verzeichnisdienste (LDAP Server) im Internet. |
| OCSP | Online Certificate Status Protocol, Protokoll für die Statusauskunft |
| OID | Object Identifier, eine Ganzzahl, durch die ein Objekt (z.B. Policy) eindeutig identifiziert wird. |
| Öffentlicher Schlüssel | Öffentlicher Teil eines Schlüsselpaares. Er ist Bestandteil eines Zertifikates und wird zur Überprüfung von Digitalen Signaturen bzw. zur Verschlüsselung von Nachrichten/Daten verwendet. |
| PIN | Personal Identification Number (Aktivierungsdaten) |
| Privater Schlüssel, geheimer Schlüssel | Geheimer Teil eines Schlüsselpaares, der zum digitalen Signieren sowie zum Entschlüsseln von Nachrichten/Dokumenten erforderlich ist und geheim gehalten werden muss. |
| Public-Key Infrastructure, PKI | Ein kryptografisches System, das ein Paar von durch einen mathematischen Algorithmus verbundenen Schlüsseln benutzt. Der öffentliche Teil dieses Schlüsselpaars kann jedermann zugänglich gemacht werden, der Informationen verschlüsseln oder eine digitale Signatur prüfen will, der geheime (private) Teil wird von seinem Besitzer sicher bewahrt und kann Daten entschlüsseln oder eine digitale Signatur erstellen. |
| Qualifiziertes Zertifikat | Zertifikat, welches den Bestimmungen des § 5 des Österr. Signaturgesetzes entspricht. |

| | |
|---|---|
| Registrierungsstelle, Registration Authority, RA | Eine vertrauenswürdige Einrichtung, welche die Überprüfung der Identität der Zertifikatsbewerber im Namen des Zertifizierungsdiensteanbieters unter Berücksichtigung der Zertifizierungsrichtlinien durchführt und selbst keine Zertifikate ausstellt. |
| RFC | Request for Comments, Artikel über Standards und Protokolle im Internet. Neue Standards werden zunächst vorgeschlagen und zur Diskussion gestellt (daher "mit der Bitte um Stellungnahme"). Erst nachdem sie ausdiskutiert und für gut befunden worden sind, werden sie unter einer RFC-Nummer veröffentlicht. |
| Root-CA, Root-Zertifizierungsstelle | Die Root-CA ist die oberste CA in der Zertifizierungshierarchie der a.trust. Sie stellt die Zertifikate für die nachgeordneten CAs aus. |
| Root-Zertifikat, Stammzertifikat, Root-CA Zertifikat | Zertifikat des Root-Keys, der zur Signatur der Zertifikate der Zertifizierungsstellen und der zugehörigen CRLs dient |
| RSA | Signatur- und Verschlüsselungsverfahren; benannt nach Rivest, Shamir und Adleman |
| Schlüsselpaar | Ein privater Schlüssel und der dazugehörige öffentliche Schlüssel. Abhängig vom verwendeten Algorithmus kann man mit Hilfe des öffentlichen Schlüssels eine digitale Unterschrift, die mit dem dazu gehörigen privaten Schlüssel erstellt wurde, verifizieren bzw. mit dem privaten Schlüssel Daten entschlüsseln, welche mit dem zugehörigen öffentlichen Schlüssel verschlüsselt wurden. |
| Signator | Eine Person, die eine elektronische Signatur erstellt, Zertifikatsinhaber |
| Signaturerstellungsdaten | Signaturerstellungsdaten sind einmalige Daten wie Codes oder private Signaturschlüssel, die von dem Signator zur Erstellung einer elektronischen Signatur verwendet werden. |
| Signaturprüfdaten | Signaturprüfdaten sind Daten wie Codes oder öffentliche Signaturschlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden. |
| Sperre | Eine Sperre ist ein zeitlich begrenztes vorübergehendes Aussetzen der Gültigkeit eines Zertifikats. |
| Statusauskunft | Dienst, bei dem die Anwender Auskunft über den aktuellen Status (gültig oder gesperrt) eines Zertifikates abrufen können. |

| | |
|---|---|
| URI | Uniform Resource Identifier, spezifiziert eine bestimmte Datei auf einem bestimmten Server, Oberbegriff für URL (Uniform Resource Locator) und URN (Universal Resource Name). |
| Verifizierung (einer digitalen Signatur) | Feststellung, dass eine digitale Signatur mit dem privaten Schlüssel, der zu dem in einem gültigen Zertifikat beinhalteten öffentlichen Schlüssel gehört, erstellt wurde und die Nachricht sich nach der Signatur nicht verändert hat. |
| Verzeichnis (-dienst) | Dienst, bei dem die Anwender Zertifikate der CA oder anderer Anwender sowie CRLs abrufen können. Der Zugriff wird über LDAP realisiert. |
| Widerruf | Der irreversible Vorgang der vorzeitigen Beendigung der Gültigkeit eines Zertifikats ab einem bestimmten Zeitpunkt. |
| X.509 | Der ITU-Standard für Zertifikate. X.509 v3 beschreibt Zertifikate, die mit verschiedenen Zertifikatserweiterungen erstellt werden können |
| 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, auch Signator genannt. |
| Zertifikatsnutzer, Signaturempfänger | Anwender, der Zertifikate über die Schlüssel und Daten anderer nutzt, um Signaturen zu prüfen. |
| Zertifikats-Widerrufsliste, CRL | Eine digital signierte Datenstruktur, die widerrufene und gesperrte Zertifikate anführt, welche von einem bestimmten Zertifizierungsdiensteanbieter ausgestellt wurden. |

## A.2 Referenzdokumente

[Policy] a.trust Certificate Policy für qualifizierte a.sign premium mobile Zertifikate für sichere Signaturen

[ETSI] Policy requirements for certification authorities issuing qualified certificates – ETSI TS 101 456, V1.1.1 (2000-12)

[SigG] Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG). BGBl. I Nr. 190/1999 (NR: GP XX RV 1999 AB 2065 S. 180. BR: AB 6065 S. 657.)

[SigV] Verordnung zum Signaturgesetz, BGBl II 2000/30, 02. 02. 2000 und BGBl. II Nr. 527/2004, 30. 12.2004

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

[DSG] Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000). BGBl. I Nr. 165/1999 (NR: GP XX RV 1613 AB 2028 S. 179. BR: 5992 AB 6034 S. 657.)

[FIPS 140-1] FIPS PUB 140-1, Security Requirements For Cryptographic Modules, 1994 January 11

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

[A-SIT-Starcos1] A-SIT Bescheinigung nach §18(5) SigG: Smart Card mit Chip Philips Smart Card Controller P8WE5032V0G und Betriebssystem STARCOS SPK 2.3 und Digital Signature Application TrustSign, 11.12.2007

[A-SIT-Starcos e-card] A-SIT Bescheinigung nach §18(5) SigG: Sichere Signaturerstellungseinheit STARCOS 3.1 ECC with EU compliant Electronic Signature Application V4.0, Version 1.0 und Versoin 2.0, 05.11.2007 und 09.03.2006

[A-SIT-ACOS-03] A-SIT Bescheinigung nach §18(5) SigG: Sichere Signaturerstellungseinheit ACOS EMV-A03V0 Konfiguration B, 13.12.2006 und Sichere Signaturerstellungseinheit ACOS EMV-A03V1 Konfiguration B, 13.02.2006

[ACOS-04] T-Systems GEI GmbH bestätigt nach §15 Abs. 7 S. 1, 17 Abs. 1 SigG sowie §15 Abs. 1 und 4, §11 Abs. 3 SigV (Deutschland): Signaturerstellungseinheit ACOS EMV-A04V1 Konfiguration B, 18.07.2008 (Nachtrag: 18.12.2008)

[ISO9796-2] ISO/IEC: Information technology - Security techniques - Digital signature schemes giving message recovery - Part 2: Mechanisms using a hash function

[PKCS1] RSA Laboratories: PKCS #1: RSA Encryption Standard; Version 1.5

[ANSI X9.62] American National Standards Institute, ANSI X9.62-1998, "Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm", January 1999

[Alg_Empfehlung] Empfohlene Algorithmen und Parameter für elektronische Signaturen, in aktueller Version, RTR GmbH/A-SIT