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

a.trust

Certificate Policy für a.sign Company Root Zertifikate

Version: 1.0

Datum: 30.03.2004

Inhaltsverzeichnis

1 Einführung

1.1 Überblick

Eine Certificate Policy enthält ein Regelwerk, das den Einsatzbereich eines Zertifikats für eine bestimmte Benutzergruppe und/oder Anwendungsklasse mit gemeinsamen Sicherheitsanforderungen definiert.

Die a.sign Company Root Policy gilt für nicht qualifizierte (einfache) Zertifikate entsprechend den Definitionen der EU-Richtlinie [SigRL] und dem österreichischen Bundesgesetz über elektronische Signaturen [SigG].

1.2 Identifikation

Name der Policy:	a.sign Company Root Certificate Policy
Version:	1.0/30.03.2004
Object Identifier:	**1.2.040.0.17** (a.trust)**.1** (Certificate Policy)**.15** (a.sign Company Root)**.1.0** (Version) vorliegende Version

Der a.trust OID 1.2.040.0.17 ist bei ÖNORM registriert.

1.3 Anwendungsbereich

Die Certificate Policy gilt für das a.sign Company Root-Zertifikat, und die damit signierten Zertifikate, welche von a.trust an Unternehmen (Zertifikatsinhaber) ausgestellt werden. Die Zertiifkatsinhaber zertifizieren mit diesen Zertifikaten ihrerseits Zertifikate für Endbenutzer.

Das a.sign Company Root- und die damit signierten Zertifikate sind einfache Zertifikate, die geheimen Schlüssel der Zertifikatsinhaber befinden sich in zertifizierten Hardware Security Modulen.

1.4 Übereinstimmung mit der Policy

a.trust verwendet den Object Identifier aus Kapitel 1.2 nur für die Erstellung von Zertifikaten, anlässlich deren Ausgabe die Regelungen der gegenständlichen Policy Beachtung fanden.

Die Zertifikate, die vom Zertifikatsinhaber an Endbenutzer ausgestellt werden, unterliegen der Certificate Policy, die der Zertifikatsinhaber erstellt, aktualisiert und veröffentlicht.

2 Verpflichtungen und Haftungsbestimmungen

2.1 Verpflichtungen der a.trust

a.trust verpflichtet sich sicherzustellen, dass alle Anforderungen, die im Abschnitt 3 dargelegt sind, erfüllt werden.

a.trust ist verantwortlich für die Einhaltung aller Richtlinien, die in der gegenständlichen Policy beschrieben sind; dies gilt auch für jene Funktionen, deren Ausführung an Vertragspartner ausgegliedert wurde.

Es sind keine zusätzlichen Verpflichtungen direkt oder durch Referenzierung in den Zertifikaten ausgewiesen, dementsprechend bestehen auch keine zusätzlichen Verpflichtungen aus diesem Titel.

a.trust erbringt die Zertifizierungsdienste in Übereinstimmung mit dem Certification Practice Statement für a.sign Company Root (siehe [CPS]).

2.2 Verpflichtungen des Zertifikatsinhabers

Der Zertifikatsinhaber ist das Unternehmen, an welches ein von a.sign Company Root ausgestelltes Zertifikat ausgegeben wird. a.trust bindet den Zertifikatsinhaber vertraglich an die Einhaltung der nachfolgend angeführten Verpflichtungen.

Die dem Zertifikatsinhaber auferlegten Verpflichtungen umfassen die folgenden Punkte:

1. die Angabe vollständiger und korrekter Informationen in Übereinstimmung mit den Anforderungen dieser Policy,

2. den Einsatz eines zertifizierten Hardware Security Moduls zur Generierung und Aufbewahrung des von a.trust zertifizierten Schlüssels,

3. die ausschließliche Nutzung des zertifizierten Schlüssels für die im Zertifikat festgelegte Verwendung,

4. die Anwendung entsprechender Vorsicht, um den unbefugten Gebrauch des privaten Schlüssels zu verhindern,

5. die Erstellung eines Sicherheitskonzepts und eines Betriebskonzepts zur Beschreibung der Infrastruktur der Zertifikatsausstellung und der getroffenen Maßnahmen zur Gewährleistung der Sicherheit der Dienstleistungen im Namen von a.trust,

6. die Erstellung einer Certificate Policy und eines Certification Practice Statements zur Ausstellung der Endbenutzerzertifikats,

7. die Übergabe der Dokumentation des Betriebes (insbes. Sicherheitskonzept und Betriebskonzept) in der jeweils gültigen Version an a.trust,

8. a.trust muss es ermöglicht werden, Kontrollen der Einhaltung aller Sicherheitsmaßnahmen und Besichtigung der Örtlichkeiten, in denen die Registrierungs-, Zertifizierungs- und Widerrufsdienste durch den Zertifikatsinhaber erbracht werden, durchzuführen.

9. a.trust ist unverzüglich zu benachrichtigen, wenn vor Ablauf der Gültigkeitsdauer des Zertifikats einer der nachfolgenden Fälle eintritt:

   - der private Schlüssel wurde kompromittiert oder eine Kompromittierung wird vermutet,
   - die Kontrolle über den privaten Schlüssel durch Kompromittierung der Aktivierungsdaten (PIN) oder durch andere Umstände ging verloren,
   - die im Zertifikat beinhalteten Informationen sind nicht korrekt.

2.3 Verpflichtungen des Überprüfers von Zertifikaten

Ein Überprüfer, der ein von a.trust ausgestelltes Zertifikat zur Verifizierung der Signatur über ein Zertifikat verwendet, kann diesem nur dann vertrauen, wenn er

- eine Überprüfung der Gültigkeitsperiode und des Widerrufsstatus des Zertifikats unter Verwendung der von a.trust bereitgestellten Abfragemöglichkeiten vornimmt
- und sämtliche anderweitig vorgeschriebene Vorsichtsmaßnahmen (siehe [CPS]) einhält.

Wenn die Signaturprüfung mittels automatisierter Verarbeitung erfolgt, dann liegt es im Ermessen des Betreibers dieser Überprüfung, mit welchen Verfahren sie durchgeführt wird.

2.4 Haftung

a.trust haftet als Aussteller des a.sign Company Root und der mit dessen privaten Schlüssel signierten Zertifikate

- für die Einhaltung der zugehörigen Zertifizierungsrichtlinie (siehe [CPS]), insbesondere für die darin festgelegten Maßnahmen zur umgehenden Veröffentlichung von Widerrufslisten und für die Einhaltung der in der Zertifizierungsrichtlinie genannten Standards (ITU X.509),

- dafür, dass die im Zertifikat enthaltenen Daten des Zertifikatsinhabers zum Zeitpunkt der Ausstellung korrekt waren und durch a.trust überprüft wurden.

a.trust haftet nicht, falls sie nachweisen kann, dass sie an der Verletzung der oben angeführten Verpflichtungen keine Schuld trifft.

3 Anforderung an die Erbringung von Zertifizierungsdiensten

Diese Policy ist auf die Erbringung von einfachen Zertifizierungsdiensten ausgerichtet. Dies umfasst die Bereitstellung von Registrierungsdiensten, Zertifikatsausstellung, Widerrufsdiensten und Abfragediensten über den Zertifikatsstatus.

3.1 Certification Practice Statement

3.1.1 Maßnahmen der a.trust

a.trust hat die nachfolgend aufgelisteten Maßnahmen ergriffen, um die für die Erbringung von Zertifizierungsdiensten nötige Sicherheit und Verlässlichkeit zu gewährleisten:

1. a.trust hat eine Risikoanalyse erstellt, um die möglichen Risiken abzuschätzen und die sich daraus ergebenden Sicherheitsanforderungen und Umsetzungsmaßnahmen zu bestimmen.

2. a.trust hat in ihrem Sicherheitskonzept alle nötigen Vorgangsweisen und Prozeduren, um die Anforderungen aus der Certificate Policy zu erfüllen, dargestellt.

3. Das Certification Practice Statement für a.sign Company Root Zertifikate (siehe [CPS]) benennt die Verpflichtungen aller externen Vertragspartner, welche Dienstleistungen für a.trust unter Beachtung der jeweils anwendbaren Policies und Richtlinien erbringen.

4. a.trust macht allen Zertifikatsinhabern und Überprüfern von elektronischen Signaturen und Zertifikaten das Certification Practice Statement und jegliche Dokumentation, die die Übereinstimmung mit dieser Policy dokumentiert, zugänglich (siehe Kapitel 3.3.4).

5. Die Geschäftsführung der a.trust stellt das alleinige Entscheidungsgremium dar, dem die Genehmigung des Certification Practice Statements für den Dienst a.sign Company Root obliegt.

6. Die Geschäftsführung der a.trust trägt auch die Verantwortung für die ordnungsgemäße Implementierung der Zertifizierungsrichtlinie.

7. a.trust hat einen Revisionsprozess zur Überprüfung der Vorgangsweisen der Zertifizierung aufgesetzt, der auch Maßnahmen zur Wartung der Zertifizierungsrichtlinie umfasst.

8. a.trust wird über Änderungen des Certification Practice Statements informieren und eine überarbeitete Version entsprechend Punkt 4 dieses Absatzes unverzüglich zugänglich machen.

3.1.2 Maßnahmen der Zertifikatsinhaber

a.trust stellt sicher, dass der Zertifikatsinhaber, dem von a.trust Company Root ein Zertifikat ausgestellt wird, die nachfolgend aufgelisteten Maßnahmen zur Gewährleistung der Sicherheit und Verlässlichkeit der Zertifizierungsdienste ergreift:

1. Erstellung einer Risikoanalyse, um die möglichen Risiken abzuschätzen und die sich daraus ergebenden Sicherheitsanforderungen und Umsetzungsmaßnahmen zu bestimmen.

2. Erstellung eines Sicherheitskonzepts mit der Darstellung aller nötigen Vorgangsweisen und Prozeduren, um die Anforderungen aus der gegenständlichen Certificate Policy zu erfüllen.

3. Beachtung sämtlicher Verpflichtungen, die sich aus der Policy und den anwendbaren Richtlinien ergeben.

4. Allen Signatoren und Überprüfern von elektronischen Signaturen und Zertifikaten werden das Certification Practice Statement, die Certificate Policy und jegliche relevante Dokumentation zugänglich gemacht.

3.2 Verwaltung der Schlüssel zur Erbringung von Zertifizierungsdiensten

3.2.1 Erzeugung der CA Schlüssel

Die Generierung der von a.trust zur Erbringung von Zertifizierungsdiensten verwendeten Schlüssel erfolgt in Übereinstimmung mit den Bestimmungen der §§ 6 und 8 [SigV]:

1. Die Erzeugung der Schlüssel wird von dazu autorisiertem Personal (siehe Kapitel 3.4.3), im Vier-Augen-Prinzip in einer physisch abgesicherten Umgebung durchgeführt (siehe 3.4.4).

2. Die Schlüssel werden in einer Signaturerstellungseinheit (Hardware Security Modul) erstellt, die einem Bestätigungsverfahren bei A-SIT unterzogen wurde und zur Erstellung fortgeschrittener Signaturen geeignet ist.

3. Für die Schlüsselgenerierung wird ein Algorithmus verwendet, der auch für qualifizierte Zertifikate als geeignet angesehen würde.

4. Die Schlüssellänge und der Algorithmus wären ebenfalls für qualifizierte Zertifikate geeignet und entsprechen Anhang I [SigV].

3.2.2 Speicherung der CA-Schlüssel

a.trust stellt in Übereinstimmung mit den Regelungen dess § 10 [SigV] sicher, dass die privaten Schlüssel geheim gehalten werden und ihre Integrität bewahrt bleibt und beachten auch für die Erbringung von einfachen Zertifizierungsdiensten die Bestimmungen des § 10 [SigV].

Die Schlüssel sind in einem Hardware Security Modul gespeichert, der von A-SIT als zur Erstellung fortgeschrittener Signaturen geeignet bestätigt wurde.

Es sind Maßnahmen getroffen worden, die garantieren, dass die privaten CA-Schlüssel das Hardware Security Modul nicht verlassen und kein Zugriff von außen darauf möglich ist.

3.2.3 Verteilung der öffentlichen CA-Schlüssel

a.trust stellt durch die folgenden Maßnahmen sicher, dass die Integrität und Authentizität ihres öffentlichen Root-Schlüssels für nicht qualifizierte Zertifikate anlässlich der Verteilung gewahrt bleibt:

- bei der Übergabe zur Veröffentlichung an die Aufsichtsstelle durch Übermittlung eines signierten PKCS#10 Certificate Request und

- durch Ausstellung und Veröffentlichung eines selbstsignierten Root-Zertifikats im Verzeichnis.

Das untergeordnete a.sign Company Root Zertifikat, mit dessen zugehörigem privatem Schlüssel die Zertifikate der Zertifikatsinhaber signiert werden, wird den Anwendern durch Veröffentlichung im a.trust Verzeichnisdienst zugänglich gemacht. a.trust gewährleistet die Authentizität dieses Zertifikats.

3.2.4 Schlüsseloffenlegung

Eine Offenlegung von geheimen CA Schlüsseln ist nicht vorgesehen.

3.2.5 Verwendungszweck von CA-Schlüsseln

Die privaten Schlüssel der Zertifizierungsstellen werden nur für die Ausstellung von Zertifikaten und für die Signatur der zugehörigen Widerrufsliste innerhalb von physisch abgesicherten Räumlichkeiten verwendet.

3.2.6 Ende der Gültigkeitsperiode von CA-Schlüsseln

Geheime CA-Schlüssel werden benutzt, solange die verwendeten Algorithmen den Sicherheitserwartungen entsprechen. Das a.trust Root-Zertifikat und das a.sign Company Root Zertifikat werden für einen Zeitraum von drei Jahren ausgestellt. Die Zertifikate der Zertifikatsinhaber hingegen werden für einen Zeitraum von höchstens zehn Jahren ausgestellt.

Eine Archivierung der geheimen Schlüssel ist nicht vorgesehen.

3.2.7 Verwaltung und Lebenszyklus der Hardware Security Module für die Zertifizierung

Die Sicherheit der zur Zertifikatssignatur durch a.trust verwendeten Hardware Security Module ist über ihren gesamten Lebensweg hindurch wie folgt abgesichert:

1. Die Inbetriebnahme eines Hardware Security Moduls, das gültige Zertifizierungsschlüssel enthält, ist an das Zusammenwirken von zwei autorisierten Mitarbeitern, deren Verantwortlichkeit im Rollenmodell des Sicherheitskonzepts festgelegt ist, gebunden.

2. Die korrekte Funktionsweise des Hardware Security Moduls wird von den autorisierten Mitarbeitern bei Inbetriebnahme überprüft.

3.2.8 Erzeugung der Schlüssel für die Zertifikatsinhaber

Die Generierung des Schlüssels des Inhabers eines von a.sign Company Root ausgestellten Zertifikats erfolgt in dessen Hardware Security Modul und ist im Detail in der Zertifizierungsrichtlinie des Zertifikatsinhabers beschrieben.

a.trust erhält keine Kenntnis des privaten Schlüssels eines Zertifikatsinhabers.

3.3 Lebenszyklus des von a.sign Company Root ausgestellten Zertifikats

3.3.1 Registrierung des Zertifikatswerbers

Zur Antragstellung und Registrierung muss ein berechtigter Vertreter des Unternehmens mit der zuständigen Registrierungsstelle der a.trust (Kontaktinformationen sind auf der a.trust Homepage veröffentlicht) in Kontakt treten.

Dem Zertifikatswerber werden die Geschäftsbedingungen und andere Bestimmungen und Dokumentation (CPS und Certificate Policy) für a.sign Company Root zugänglich gemacht.

Bei der Antragstellung müssen die folgenden Daten bekannt gegeben werden:

- der vollständige Name, Telefonnummer und E-Mailadresse eines technischen Verantwortlichen,
- der vollständige Name und Kontaktinformation eines rechtlich-organisatorischen Verantwortlichen (Zeichnungsberechtigung),
- Passwort für den Widerruf,
- Firmenbuch- oder EBR-Nummer (wenn vorhanden),
- Common Name des Zertifikats
- Name und Sitz der Organisation,
- Optional: Name einer Organisationsuntereinheit
- die zu zertifizierende öffentliche Schlüsselkomponente.

Der mit dem Zertifikatswerber abzuschließende Vertrag beinhaltet insbesondere:

- die Annahme der Verpflichtungen des Zertifikatsinhabers,
- die Zustimmung, dass von a.trust Aufzeichnungen über den Registrierungsvorgang und alle dabei erhaltenen Daten geführt werden und dass diese Aufzeichnungen ggf. bei Beendigung der Zertifizierungsdienste an Dritte übergeben werden können,
- die Bestätigung der Korrektheit des Zertifikatsinhaltes.

Die Registrierungsstelle nimmt die folgenden Überprüfungen des Antrags vor:

- Prüfung der Organisation (lt. Firmenbuch oder anhand von Datenbanken vertrauenswürdiger Dritter),
- Prüfung der Vertretungsbefugnis und der Ausweiskopien der beiden verantwortlichen Personen,
- Prüfung der Eigentümerschaft und der erfolgten Zertifizierung des zur Schlüsselgenerierung benutzten Hardware Security Moduls.

Der Zertifikatsantrag und alle damit im Zusammenhang stehenden vom Antragsteller übermittelten und in Papierform vorliegenden Daten und Dokumente (Ausweiskopien, Firmenbuchauszug, Nachweis der Vertretungsbefugnis sowie Zertifizierungsbescheinigungen des Hardware Security Moduls und Rechnungen) werden auf die Dauer von mind. sieben Jahren nach Ablauf der Gültigkeit (physisch oder elektronisch) archiviert.

Die Beachtung der Bestimmungen des Datenschutzgesetzes ([DSG]) sind durch die seitens a.trust den Registrierungsstellen vorgeschriebenen Prozesse sicher gestellt.

3.3.2 Verlängerung der Gültigkeitsdauer

Durch die folgenden Maßnahmen wird sichergestellt, dass Anträge von Zertifikatswerbern, die bereits anlässlich einer vorhergehenden Zertifikatsausstellung registriert wurden, vollständig, korrekt und ordnungsgemäß autorisiert sind. Die Maßnahmen gelten sowohl für die Verlängerung der Gültigkeitsdauer, falls diese durchgeführt wird, als auch für die Neuausstellung nach Ablauf oder Widerruf eines Zertifikats.

1. Die Registrierungsstelle hat die im Zertifikat enthaltenen Daten hinsichtlich ihrer aktuellen Gültigkeit zu prüfen.
2. Etwaige Änderungen in den Vertragsbedingungen werden dem Antrag stellenden Unternehmen mitgeteilt und seine Zustimmung dazu eingeholt. Die Maßnahmen erfolgen in Übereinstimmung mit Abschnitt 3.3.1.

3. Etwaige Änderungen von Informationsinhalten der Dokumentation zur Antragstellung werden entsprechend 3.3.1 überprüft, festgehalten und seitens des Antragstellers bestätigt.

4. Die sich aus der Verlängerung ergebende neue Gültigkeitsperiode darf nicht länger sein als die der Erstausstellung. Eine Verlängerung darf nur erfolgen, wenn die kryptografische Sicherheit der verwendeten Verfahren über die gesamte neue Gültigkeitsdauer ausreichend sichergestellt ist und keine Hinweise auf Kompromittierung des privaten Schlüssels des Antragstellers bestehen.

3.3.3 Erstellung der Zertifikate

Die Zertifikate werden gem. den Bestimmungen in Anhang 2 [SigV] als X.509 v3 Zertifikate erstellt. Die in den Zertifikaten enthaltenen Angaben sind insb. die folgenden:

- Versionsnummer des Zertifikats: es werden Zertifikate der Version 3 (codiert mit dem Wert 2) ausgestellt
- Seriennummer des Zertifikats
- Bezeichnung des Zertifikatsausstellers
- Beginn und Ende der Gültigkeit des Zertifikats
- Bezeichnung des Zertifikatsinhabers
- öffentlicher Schlüssel (mit Angabe des Algorithmus)
- Angabe des Algorithmus für die Signatur des Zertifikats
- Signatur über das Zertifikat
- Zertifikatserweiterungen, wie z. B.:
    - Informationen über die anzuwendende Policy bzw. CPS
    - Zertifikatsverwendung
    - Information zum Auffinden der CRL.

Das Zertifikat wird von der a.sign Company Root CA erzeugt. Die eindeutige Zuordnung des Zertifikats zum Zertifikatsinhaber ist gesichert durch:

- Erstellung eines PKCS#10-Requests durch den Antragsteller als Grundlage für die Zertifizierung.

- Erzeugung des Zertifikats nach Überprüfung aller Antragsdaten auf ihre Korrektheit durch die Registrierungsstelle der a.trust.

- Bestätigung der Korrektheit der Daten durch den Antragsteller.

Die in der Registrierungsstelle aufgenommenen Daten werden signiert und verschlüsselt (SSL) an die Zertifizierungsstelle übertragen. Vertraulichkeit und Integrität sämtlicher Daten sind damit sicher gestellt. Alle RA-Mitarbeiter sind mit einer Signaturkarte ausgestattet und die Authentizität der übermittelten Registrierungsdaten wird durch Verifizierung der Signatur des RA-Mitarbeiters überprüft.

3.3.4 Bekanntmachung der Vertragsbedingungen

a.trust stellt den Zertifikatsinhabern und Überprüfern von Zertifikaten und Signaturen die Bedingungen betreffend die Benutzung des Zertifikats durch Veröffentlichung der nachfolgenden Dokumente auf der a.trust-Homepage zur Verfügung:

1. der gegenständlichen Certificate Policy,

2. des Certification Practice Statement (Zertifizierungsrichtlinie für a.sign Company Root, siehe [CPS]),

3. der Allgemeinen Geschäftsbestimmungen von a.trust, sowie

4. der sonstigen Mitteilungen.

Änderungen werden dem Zertifikatsinhaber mittels Bekanntmachung auf der a.trust-Homepage und ggf. auch mittels Anschreibens zur Kenntnis gebracht. Sie sind von jedermann von der a.trust-Homepage abrufbar.

In o. a. Dokumenten ist eindeutig festgelegt:

- dass die Zertifikate an Unternehmen ausgegeben werden und die Anwendung des privaten Schlüssels an ein zertifiziertes Hardware Security Modul gebunden ist,

- die Verpflichtungen des Zertifikatsinhabers entsprechend Kapitel 2.2,

- die Vorgehensweise zur Überprüfung eines Zertifikats inklusive der Notwendigkeit der Überprüfung des Zertifikatsstatus, sodass der Überprüfer mit gutem Grund dem Zertifikat vertrauen kann (siehe 2.3),

- die Zeitdauer, für die Registrierungsinformationen aufgehoben werden (siehe Kapitel 3.3.1),

- die Zeitdauer, für die Aufzeichnungen von wichtigen Ereignissen der Zertifizierungsstelle aufgehoben werden (siehe Kapitel 3.4.11),
- Vorgehensweisen zur Behandlung von Beschwerden und Streitfällen,
- die Anwendbarkeit des [SigG] und [SigV].

3.3.5 Veröffentlichung der Zertifikate

Von a.trust ausgestellte a.sign Company Root Zertifikate werden den Zertifikatsinhabern und den Überpüfern des Zertifikats folgendermaßen verfügbar gemacht:

1. Das Zertifikat wird im Verzeichnisdienst von a.trust veröffentlicht.
2. Die Bedingungen für die Benutzung eines Zertifikats werden von a.trust allen Beteiligten zur Kenntnis gebracht (siehe Kapitel 3.3.4).
3. Die Identifikation der anzuwendenden Bestimmungen ist durch die eindeutige Zuordnung zum Produktnamen "a.sign Company Root" einfach herstellbar.
4. Der Verzeichnisdienst ist 7 Tage 24 Stunden verfügbar. Unterbrechungen von mehr als 30 Minuten werden gemäß § 13 Abs 5 [SigV] als Störfälle dokumentiert.
5. Die Verzeichnisdienste sind öffentlich und international zugänglich.

3.3.6 Widerruf

Der Widerruf ist die irreversible vorzeitige Beendigung der Gültigkeit eines Zertifikats.

3.3.6.1 Ablauf des Widerrufs

Die Vorgangsweise für das Auslösen eines Widerrufs ist im Certification Practice Statement (siehe [CPS]) dokumentiert, insbesondere:

- wer berechtigt ist, einen Widerruf zu beantragen,
- wie ein Widerrufsantrag gestellt werden kann,
- die Mechanismen für die Bereitstellung von Statusinformationen und
- die maximale Zeitdauer, die zwischen Einlangen eines Widerrufsantrags und der Veröffentlichung des Widerrufs, verstreichen kann.

Ein Widerruf kann vom Zertifikatsinhaber telefonisch zu den auf der Homepage der a.trust angegebenen Zeiten und unter der Nummer, die ebendort zu finden ist, beim Widerrufsdienst beantragt werden. Alle Anträge werden mit Einlangen bearbeitet. Spätestens innerhalb von drei Stunden ab Bekanntwerden des Widerrufsgrundes erfolgt eine Aktualisierung der Widerrufsliste.

Die Durchführung von Widerrufen beim Widerrufsdienst ist an die Kenntnis eines dafür eigens vorgesehenen Widerrufspassworts gebunden. Dem Mitarbeiter des Widerrufsdienstes muss ein Widerrufsgrund genannt werden.

Widerrufslisten sind öffentlich und international zugänglich und täglich 24 Stunden abfragbar. Im Fall von Systemausfällen kommen die im Certification Practice Statement für a.sign Company Root Zertifikate (siehe [CPS]) genannten Vorkehrungen zum Tragen, um die Auswirkungen möglichst gering zu halten.

Statusinformationen über Zertifikate können auch online mittels OCSP abgefragt werden. Die Integrität und Authentizität der OCSP-Antworten sind durch eine Signatur gesichert.

3.3.6.2 Widerrufsliste

Widerrufene Zertifikate werden in einer Widerrufsliste (CRL) unter Berücksichtigung der nachfolgenden Regelungen veröffentlicht:

- Die aktuelle Update-Frequenz der Widerrufsliste ist im Internet über die Web-Seite der a.trust abrufbar.
- Jede Widerrufsliste enthält den Zeitpunkt der geplanten Ausgabe der nächsten Liste.
- Falls erforderlich kann eine neue Widerrufsliste auch vorzeitig veröffentlicht werden.
- Jede Widerrufsliste ist mit dem Zertifizierungsschlüssel signiert.

Widerrufslisten werden als X.509 Version 2 CRLs ausgegeben. Die wesentlichen Angaben in den CRLs sind die folgenden

- Versionsnummer der CRL: Version 2 (codiert mit dem Wert 1),
- Bezeichnung des Ausstellers,
- Zeitpunkt der CRL-Ausstellung sowie der nächsten geplanten Ausstellung,
- Information über die in der CRL enthaltenen Zertifikate:

- Seriennummer,
- Zeitpunkt der Eintragung in die CRL,
- Eintragungsgrund

- CRL-Erweiterungen:
  - Angabe des Algorithmus für die Signatur über die CRL
  - Signatur über die CRL.

3.4 a.trust Verwaltung

3.4.1 Sicherheitsmanagement

Es gelten die folgenden Bestimmungen:

1. a.trust ist für alle Prozesse im Rahmen der Zertifizierungsdienste verantwortlich, dies gilt auch für die an Vertragspartner ausgelagerten Dienste. Die Verantwortlichkeiten der Vertragspartner sind klar geregelt und Kontrollen zur Überprüfung der ordnungsgemäßen Tätigkeit eingerichtet. Die für die Sicherheit relevanten Vorgehensweisen sind im Certification Practice Statement für a.sign Company Root Zertifikate (siehe [CPS]) veröffentlicht.

2. Die Geschäftsführung der a.trust ist unmittelbar verantwortlich für die Definition der Sicherheitsrichtlinien und deren Kommunikation an die mit sicherheitsrelevanten Vorgängen befassten Mitarbeiter.

3. Die Sicherheitsinfrastruktur von a.trust wird ständig überprüft und an sich ändernde Anforderungen angepasst. Jegliche Änderungen, die einen Einfluss auf das Ausmaß der erreichten Sicherheit haben, sind von der Geschäftsführung der a.trust zu genehmigen.

4. Alle Sicherheitsmaßnahmen und sicherheitsrelevanten Funktionen zur Bereitstellung der Zertifizierungsdienste werden von a.trust dokumentiert und entsprechend der Dokumentation implementiert und gewartet.

5. Der Betrieb des Rechenzentrums der a.trust ist an SBS Siemens Business Services Ges.m.b.H. ausgelagert. SBS ist an die Wahrung der Informationssicherheit vertraglich gebunden.

6. Die Ausstellung von Endbenutzerzertifikaten ist an den Inhaber des von a.sign Company Root ausgestellten Zertifikats ausgelagert. Dieser ist vertraglich an die Wahrung der Informationssicherheit gebunden und muss a.trust ein Sicherheits- und ein Betriebskonzept übergeben.

3.4.2 Informationsklassifikation und -verwaltung

a.trust stellt sicher, dass alle Daten und Informationen in geeigneter Weise abgesichert sind.

In der Risiko- und Bedrohungsanalyse sind alle Informationsbestände verzeichnet und gem. ihrer Schutzwürdigkeit klassifiziert.

3.4.3 Personelle Sicherheitsmaßnahmen

Das Personal der a.trust und deren Beschäftigungsmodalitäten sind geeignet, das Vertrauen in die Abwicklung der Zertifizierungsdienste zu stärken. Insbesondere wird auf die folgenden Erfordernisse Wert gelegt:

1. a.trust beschäftigt ausschließlich Personal, welches über das gem. § 10 Abs 5 [SigV] benötigte Fachwissen, die Qualifikation und Erfahrung für die jeweilige Position verfügt.

2. Sicherheitsrelevante Funktionen und Verantwortlichkeiten werden in den jeweiligen Stellenbeschreibungen dokumentiert. Funktionen, von denen die Sicherheit der Zertifizierungsdienste abhängt, sind eindeutig identifiziert.

3. Für alle Mitarbeiter der a.trust (unabhängig ob in einem temporären oder ständigen Beschäftigungsverhältnis angestellt) sind klare Stellenbeschreibungen ausgearbeitet, in denen die Pflichten, Zugriffsrechte und Minimalkompetenzen dargelegt sind.

4. Die Ausübung sowohl der administrativen als auch der Managementfunktionen steht im Einklang mit den Sicherheitsrichtlinien.

5. Alle Leitungsfunktionen sind mit Personen besetzt, die über Erfahrung mit der Technologie digitaler Signaturen und mit der Führung von Personal verfügen, das Verantwortung für sicherheitskritische Tätigkeiten trägt.

6. Alle Mitarbeiter, denen vertrauenswürdige Positionen zugeordnet sind, werden von Interessenskonflikten, die einer unvoreingenommenen Erfüllung der Aufgaben entgegenstehen könnten, frei gehalten.

7. Alle vertrauenswürdigen Positionen sind im Certification Practice Statement (siehe [CPS]) im Detail beschrieben.

8. Die Zuweisung der Positionen erfolgt mit formeller Ernennung durch die Geschäftsführung.

9. Entsprechend § 10 Abs 4 [SigV] beschäftigt a.trust keine Personen, die strafbare Handlungen begangen haben, die sie für eine vertrauenswürdige Position ungeeignet erscheinen lassen. Eine Beschäftigung erfolgt erst nach einer diesbezüglichen Überprüfung. Dies gilt in gleicher Weise für die Mitarbeiter der Unternehmen, die für a.trust Dienste erbringen.

3.4.4 Physikalische und organisatorische Sicherheitsmaßnahmen

Es ist sichergestellt, dass der Zutritt zu Räumlichkeiten, in denen sicherheitskritische Funktionen ausgeübt werden, abgesichert ist und Risken einer physischen Beschädigung der Vermögenswerte minimiert sind. Insbesondere gilt:

1. Der Zutritt zu den Räumlichkeiten, in denen Zertifizierungs- und Widerrufsdienste erbracht werden, ist auf autorisiertes Personal beschränkt. Die Systeme, die die Zertifikate ausstellen, sind vor Gefährdung durch Umweltkatastrophen geschützt.

2. Es werden Maßnahmen ergriffen, um den Verlust, die Beschädigung oder die Kompromittierung von Anlagen und die Unterbrechung des Betriebes zu verhindern.

3. Weitere Maßnahmen gewährleisten, dass eine Kompromittierung oder ein Diebstahl von Daten und datenverarbeitenden Anlagen nicht möglich ist.

4. Die Systeme für die Zertifikatsgenerierung und die Widerrufsdienste werden in einer gesicherten Umgebung betrieben, sodass eine Kompromittierung durch unautorisierte Zugriffe nicht möglich ist.

5. Die Abgrenzung der Systeme für die Zertifikatsgenerierung und Widerrufsdienste erfolgt durch klar definierte Sicherheitszonen d. h. durch räumliche Trennung von anderen organisatorischen Einheiten und physischen Zutrittsschutz.

6. Die Sicherheitsmaßnahmen inkludieren den Gebäudeschutz, die Computersysteme selbst und alle sonstigen Einrichtungen, die für deren Betrieb unerlässlich sind. Der Schutz der Einrichtungen für die Zertifikatserstellung und die Bereitstellung der Widerrufsdienste umfasst physische Zutrittskontrolle, Ab-

wendung von Gefahren durch Naturgewalten, Feuer, Rohrbrüche und Gebäudeeinstürze, Schutz vor Ausfall von Versorgungseinheiten, Diebstahl, Einbruch und Systemausfällen.

7. Die unautorisierte Entnahme von Informationen, Datenträgern, Software und Einrichtungsgegenständen, welche zu den Zertifizierungsdiensten gehören, wird durch Kontrollmaßnahmen verhindert.

3.4.5 Betriebsmanagement

a.trust stellt sicher, dass das Zertifizierungssystem sicher und korrekt betrieben und das Risiko des Versagens minimiert wird. Insbesondere gilt:

1. Die Integrität der Computersysteme und Informationen ist gegen Viren und böswillige oder unautorisierte Software geschützt.

2. Schaden durch sicherheitskritische Zwischenfälle und Fehlfunktionen wird durch entsprechende Aufzeichnungen und Fehlerbehebungsprozeduren verhindert.

3. Datenträger werden vor Beschädigung, Diebstahl und unautorisiertem Zugriff geschützt.

4. Für die Ausführung von sicherheitskritischen und administrativen Aufgaben, die sich auf die Erbringung der Zertifizierungsdienste auswirken, sind Verfahrensweisen definiert und in Kraft gesetzt.

5. Datenträger werden je nach ihrer Sicherheitsstufe (siehe Kapitel 3.4.2) behandelt und aufbewahrt. Nicht mehr benötigte Datenträger, die vertrauliche Daten beinhalten, werden in sicherer Weise vernichtet.

6. Kapazitätserfordernisse werden beobachtet und künftige Entwicklungen prognostiziert, sodass stets die angemessene Prozessorleistung und Speicherplatz zur Verfügung stehen.

7. Auf Zwischenfälle wird so rasch wie möglich reagiert, um sicherheitskritische Vorkommnisse auf ein Minimum zu begrenzen. Alle Zwischenfälle werden baldmöglichst aufgezeichnet.

Die sicherheitskritischen Funktionen im Rahmen der Zertifizierungs- und Widerrufsdienste werden von den gewöhnlichen Funktionen strikt getrennt.

Sicherheitskritische Funktionen inkludieren:

1. Operationale Funktionen und Verantwortungen

2. Planung und Abnahme von Sicherheitssystemen
3. Schutz vor böswilliger Software
4. Allgemeine Wartungstätigkeiten
5. Netzwerkadministration
6. Aktive Überprüfung von Log-Files und Prüfberichten, Analyse von Zwischenfällen
7. Datenträgerverwaltung und –sicherheit
8. Daten- und Softwareaustausch

Diese Aufgaben werden von Sicherheitsbeauftragten geregelt, können aber von operativem Personal (unter Beaufsichtigung) gem. Sicherheitskonzept und Stellenbeschreibungen durchgeführt werden.

3.4.6 Zugriffsverwaltung

a.trust stellt durch die nachfolgenden Maßnahmen sicher, dass der Zugriff auf das Zertifizierungssystem ausschließlich auf ordnungsgemäß autorisierte Personen beschränkt ist.

1. Sicherungsmaßnahmen wie z. B. Firewalls bewahren das interne Netzwerk vor Zugriffen durch Dritte.
2. Vertrauliche Daten werden geschützt, wenn sie über unsichere Netzwerke ausgetauscht werden, wie z. B. die Registrierungsdaten.
3. Eine Benutzerverwaltung, die den verschiedenen Funktionen unterschiedliche Zugriffsrechte einräumt, ist eingerichtet; insbesondere werden sicherheitsrelevante von nicht sicherheitskritischen Funktionen sorgfältig getrennt. Änderungen in den Zugriffsrechten werden im System sofort nachgezogen. Die Kontrolle der Benutzerverwaltung ist Teil des internen Audits.
4. Zugriff auf Informationen und Anwendungen ist auf Grund der vergebenen Zugriffsrechte eingeschränkt. Die dafür geltenden Definitionen sind im Certification Practice Statement für a.sign Company Root Zertifikate (siehe [CPS]) angeführt. Administrative und den laufenden Betrieb betreffende Funktionen sind streng getrennt. Die Verwendung von System-Utility-Programmen ist besonders eingeschränkt.

5. Das Personal muss sich vor jedem kritischen Zugriff auf Applikationen, die im Bezug mit dem Zertifikatsmanagement stehen, authentifizieren.

6. Die Zugriffe werden in Log-Dateien aufgezeichnet. Das Personal wird für die ausgeführten Tätigkeiten zur Verantwortung gezogen.

7. Eine Wiederverwendung von Datenspeichern führt nicht zur Offenlegung von vertraulichen Daten an nicht autorisierte Personen.

8. Komponenten des lokalen Netzwerks sind in einer physisch gesicherten Umgebung und ihre Konfiguration wird regelmäßig überprüft.

9. Die Entdeckung von unautorisierten und/oder außergewöhnlichen Zugriffsversuchen auf die eigentliche Zertifizierungsstelle und die Widerrufsdienste wird durch geeignete Maßnahmen gesichert, sodass ggf. sofort Gegenmaßnahmen ergriffen werden können. Dies geschieht durch die Führung und Auswertung von CA-Logfiles und Firewall-Logfiles.

10. Ändernde Zugriffe (Löschungen, Hinzufügungen) auf die Verzeichnis- und Widerrufsdienste werden durch Passworteingabe abgesichert.

11. Versuche des unautorisierten Zugriffs auf Verzeichnis- und Widerrufsdienste werden aufgezeichnet.

3.4.7 Entwicklung und Wartung vertrauenswürdiger Systeme

a.trust verwendet vertrauenswürdige Systeme und Produkte, die gegen Veränderung geschützt sind:

1. Eine Analyse der Sicherheitsanforderungen muss im Stadium der Design- und Anforderungsspezifikation im Rahmen jedes Entwicklungsprojekts erfolgen, das von a.trust oder von Dritten im Auftrag von a.trust durchgeführt wird.

2. Änderungskontrollprozeduren existieren für die Erstellung von geplanten Programmversionen, sonstigen Änderungen und Fehlerbehebungen.

3.4.8 Erhaltung des ungestörten Betriebes und Behandlung von Zwischenfällen

a.trust wird sich bemühen, nach Katastrophenfällen, inklusive der Kompromittierung eines Zertifizierungsschlüssels, den Betrieb so rasch wie möglich wieder aufzunehmen. Insbesondere ist vorgesehen:

1. Der Notfallsplan sieht die (vermutete) Kompromittierung des privaten Zertifizierungsschlüssels als Katastrophenfall vor.

2. Sollte dieser Fall eintreten, so hat a.trust die Aufsichtsstelle (siehe § 6 Abs 5 [SigG]), die Zertifikatsinhaber, die auf die Sicherheit der Zertifizierungsdienste vertrauenden Personen und ggf. andere Zertifizierungsdiensteanbieter, mit denen Vereinbarungen bestehen, davon zu unterrichten und mitzuteilen, dass die Widerrufs- und Zertifikatsinformationen nicht mehr als zuverlässig anzusehen sind.

3. Zertifikate und Widerrufslisten werden als nicht mehr gültig gekennzeichnet.

3.4.9 Einstellung der Tätigkeit

Gem. § 12 [SigG] wird a.trust die Einstellung der Tätigkeit unverzüglich der Aufsichtsstelle anzeigen und sicher stellen, dass eine eventuelle Beeinträchtigung der Dienstleistung gegenüber Zertifikatsinhabern und vertrauenden Parteien möglichst gering gehalten wird.

Vor Beendigung der Dienstleistung werden

- alle Zertifikatsinhaber, Zertifizierungsdiensteanbieter und sonstige Parteien, mit denen a.trust eine geschäftliche Verbindung unterhält, direkt, sowie jene Parteien, die auf die Zuverlässigkeit der Zertifizierungsdienste vertrauen, durch Veröffentlichung von der Einstellung unterrichtet,

- die Verträge mit Subunternehmern zur Erbringung von Zertifizierungsdiensten beendet,

- Vorkehrungen zur Übernahme der Verzeichnis- und Widerrufsdienste sowie der Aufzeichnungen gemäß Kapitel 3.4.11 durch einen anderen Zertifizierungsdiensteanbieter getroffen,

- die privaten Schlüssel von a.trust von der Nutzung zurückgezogen.

Das Certification Practice Statement für a.sign Copmpany Root Zertifikate (siehe [CPS]) benennt die Vorkehrungen, die bei Einstellung der Tätigkeit getroffen werden, insbesondere jene Vorkehrungen

- für die Benachrichtigung der betroffenen Personen und Organisationen,
- für die Übertragung der Verpflichtungen auf Drittparteien und
- wie der Widerrufsstatus von nicht abgelaufenen Zertifikaten gehandhabt wird.

3.4.10 Übereinstimmung mit gesetzlichen Regelungen

a.trust handelt grundsätzlich in Übereinstimmung mit den gesetzlichen Regelungen und Auflagen gemäß [SigG]; insbesondere sind nachfolgende Punkte sicher gestellt:

1. Wichtige Aufzeichnungen werden vor Verlust, Zerstörung und Verfälschung bewahrt.
2. Die Anforderungen des Datenschutzgesetzes werden befolgt.
3. Nötige technische und organisatorische Maßnahmen sind ergriffen, um persönliche Daten vor unautorisierter und ungesetzlicher Verarbeitung sowie vor versehentlicher Zerstörung oder Beschädigung zu schützen.
4. Den Zertifikatsinhabern wird versichert, dass die an a.trust übermittelten Informationen nur mit ihrem Einverständnis, mit gerichtlichem Beschluss oder auf Basis gesetzlicher Regelungen offen gelegt werden.

3.4.11 Aufbewahrung der Informationen zu Zertifikaten

Alle Informationen, die in Zusammenhang mit Zertifikaten stehen, werden aufbewahrt. Insbesondere gilt:

1. Die Vertraulichkeit und Integrität der aktuellen sowie der archivierten Daten ist gewahrt.
2. Die Daten zu den Zertifikaten werden vollständig und vertraulich in Übereinstimmung mit der veröffentlichten Zertifizierungsrichtlinie (siehe [CPS]) archiviert.
3. Aufzeichnungen, die Zertifikate betreffen, werden für die Beweisführung der ordnungsgemäßen Zertifizierung im Rahmen gerichtlicher Auseinandersetzun-

gen verfügbar gemacht. Zusätzlich hat der Zertifikatsinhaber Zugang zu den Registrierungs- und sonstigen persönlichen Daten, die ihn betreffen.

4. Die Aufzeichnungen umfassen auch den genauen Zeitpunkt des Eintretens wichtiger Ereignisse, die in Zusammenhang mit der Systemumgebung, dem Schlüssel- und dem Zertifikats-Management stehen.

5. Alle Daten, die in Zusammenhang mit Zertifikaten stehen, werden für die Dauer von mindestens sieben Jahren aufbewahrt. Der Antrag wird für mindestens drei Jahre in der betreffenden Registrierungsstelle aufbewahrt.

6. Alle Aufzeichnungen erfolgen derart, dass sie innerhalb der Aufbewahrungsfrist nicht unbemerkt oder unabsichtlich gelöscht oder zerstört werden können.

7. Die spezifischen Ereignisse und Daten die aufgezeichnet werden, sind in der Zertifizierungsrichtlinie (siehe [CPS]) dokumentiert.

8. Insbesondere werden alle Registrierungsinformationen, inkl. jener, die im Zusammenhang mit der Verlängerung der Gültigkeitsdauer von Zertifikaten (Erneuerung von Zertifikaten) stehen, elektronisch aufbewahrt.

9. Die archivierten Registrierungsinformationen beinhalten insbesondere:

   - die Identifikationsdokumente, die anlässlich der Registrierung vorgelegt wurden,
   - die Akzeptanz der vertraglichen Vereinbarungen durch den Zertifikatsinhaber,
   - vom Zertifikatsinhaber gewählte und akzeptierte Zertifikatsinhalte,
   - Angabe der Registrierungsstelle und des zuständigen RA-Mitarbeiters.

10. Die Vertraulichkeit der Daten der Zertifikatsinhaber ist gewährleistet.

11. Es werden alle Ereignisse, die den Lebenszyklus der CA-Schlüssel von a.trust betreffen, aufgezeichnet.

12. Es werden alle Ereignisse, die den Lebenszyklus der Zertifikate betreffen, aufgezeichnet.

13. Alle Anträge auf Widerruf und die damit verbundenen Informationen werden festgehalten.

3.5 Organisatorisches

a.trust ist als Organisation zuverlässig und hält die folgenden Richtlinien strikt ein:

3.5.1 Allgemeines

1. Alle Richtlinien und Vorgehensweisen sind nicht-diskriminierend.
2. Die Dienstleistungen der a.trust im Rahmen von a.sign Company Root stehen Unternehmen zur Verfügung.
3. a.trust ist eine juristische Person (Gesellschaft mit beschränkter Haftung).
4. a.trust verfügt über Systeme zur Qualitätssicherung und Gewährleistung der Informationssicherheit, die den angebotenen Zertifizierungsdiensten angemessen sind.
5. Die Haftung, insbesondere diejenige zur Schadenswiedergutmachung, entspricht den Bestimmungen des [SigG] (siehe Kapitel 2.4).
6. Hinsichtlich der finanziellen Ausstattung befolgt a.trust die Bestimmungen in § 2 [SigV].
7. Das von a.trust beschäftigte Personal verfügt entsprechend den Bestimmungen des [SigG] (siehe auch Kapitel 3.4.3) über die nötige Schulung, Training, technisches Wissen und Erfahrung und ist in ausreichender Zahl vorhanden, um den geplanten Umfang der Zertifizierungsdienste bewerkstelligen zu können.
8. Es sind Richtlinien und Vorgehensweisen für die Behandlung von Beschwerden und Streitfällen vorhanden, die von Kunden oder anderen Parteien an a.trust herangetragen werden und die Erbringung ihrer Dienstleistungen betreffen.
9. Die rechtlichen Beziehungen zu Subunternehmern, welche Dienstleistungen für a.trust erbringen, sind vertraglich geregelt und präzise dokumentiert.
10. Es gibt keine aktenkundigen Gesetzesverletzungen seitens a.trust.

3.5.2 Zertifikatserstellungs- und Widerrufsdienste

Die für die Erbringung von Zertifizierungs- und Widerrufsdiensten vorgesehenen organisatorischen Einheiten sind hinsichtlich ihrer Entscheidungen über die Erbringung, Aufrechterhaltung und Beendigung der Dienstleistungen unabhängig von anderen Gesellschaften. Die Geschäftsführung und das Personal, das sicherheitsrelevante und leitende Funktionen ausübt, sind frei von kommerziellem, finanziellem und sonstigem Druck, der das Vertrauen in ihre Tätigkeit negativ beeinflussen könnte.

Die für die Zertifizierungs- und Widerrufsdienste bestimmten Einheiten verfügen über eine dokumentierte Struktur, die die Unvoreingenommenheit der Aufgabenausführung gewährleistet.

4 Anhang

A Begriffe und Abkürzungen

Certificate Policy, Policy	Ein Regelwerk, das den Einsatzbereich eines Zertifikates für eine bestimmte Benutzergruppe und/oder Anwendungsklasse festhält.
CPS, Certification Practice Statement	Aussagen über die bei der Ausstellung von Zertifikaten von einem Zertifizierungsdiensteanbieter eingehaltenen Vorgehensweise
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.
Hardware Security Modul	Elektronisches System zur sicheren Generierung und 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.
Kompromittierung	Eine unautorisierte Offenlegung von oder der Verlust der Kontrolle über sicherheitskritische Informationen und geheimzuhaltende Daten.
OCSP	Online Certificate Status Protocol
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

Privater Schlüssel, geheimer Schlüssel	Geheimer Teil eines Schlüsselpaares, der zum digitalen Signieren sowie zum Entschlüsseln von Nachrichten/Dokumenten erforderlich ist und geheimgehalten werden muss.
Public-Key System	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.
Registrierungsstelle, Registration Authority, RA	Eine vertrauenswürdige Einrichtung, welche die Überprüfung der Identität der Zertifikatsbewerber im Namen des Zertifizierungsdiensteanbieters unter Berücksichtigung der Zertifizierungsrichtlinie (CPS) durchführt und selbst keine Zertifikate ausstellt.
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 dazugehörigen privaten Schlüssel erstellt wurde, verifizieren bzw. mit dem privaten Schlüssel Daten entschlüsseln, welche mit dem zugehörigen öffentlichen Schlüssel verschlüsselt wurden.
Signaturerstellungseinheit	Komponenten, die vom Unterzeichner verwendet werden, um eine elektronische Signatur zu erstellen.
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.
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 Zertifikatserwieterungen erstellt werden können.
Zertifikats-Widerrufsliste, CRL	Eine digital signierte Datenstruktur, die widerrufene Zertifikate anführt, welche von einem bestimmten Zertifizierungsdiensteanbieter ausgestellt wurden.

Zertifizierungsdienstean-bieter, Certification Authority, CA	Eine Person oder Stelle, die Zertifikate ausstellt oder anderweitige elektronische Signaturdienste öffentlich anbieten darf.
Zertifizierungsrichtlinie	Gleichbedeutend mit Certification Practice Statement, siehe CPS

B Referenzdokumente

[SigG]	Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG). BGBl. I Nr. 190/1999 (NR: GP XX RV 1999 AB 2065 S. 180. BR: AB 6065 S. 657.)
[SigV]	Verordnung zum Signaturgesetz, BGBl II 2000/30, 02. 02. 2000
[SigRL]	Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, 13. 12. 1999
[DSG]	Bundesgesetz über den Schutz personenbezogener Daten (Daten-schutzgesetz 2000 - DSG 2000). BGBl. I Nr. 165/1999 (NR: GP XX RV 1613 AB 2028 S. 179. BR: 5992 AB 6034 S. 657.)
[CPS]	a.trust Certification Practice Statement für a.sign Company Root Zertifikate
[ETSI]	Policy requirements for certification authorities issuing qualified certificates – ETSI TS 101 456, V1.2.1 (2002-04)