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 einfache Zertifikate
a.sign corporate medium

Version: 1.0.1

Datum: 13.04.2004

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.

1.2 Identifikation

Name der Policy: a.trust Certificate Policy für einfache Zertifikate
a.sign corporate medium

Version: 1.0.1/13.04.2004

Object Identifier: **1.2.040.0.17** (a.trust) **.1** (Policy) **.72** (a.sign corporate medium) **.1.0.1** (Version) vorliegende Version

Die vorliegende Policy ist in Übereinstimmung mit den Anforderungen aus RFC 2527 (siehe [RFC2527]).

1.3 Anwendungsbereich

Die a.sign corporate medium Policy gilt für einfache a.sign corporate medium Zertifikate entsprechend der Definition § 2 Abs. 8 [SigG], welche an Organisationen, die Betreiber von Servern zur Durchführung von Signatur- und Geheimhaltungsoperationen sind, ausgestellt werden. Die geheimen Schlüssel der Signatoren befinden sich auf deren Rechner.

Die Besonderheit des Dienstes „medium“ ist dadurch gegeben, dass a.trust dem Signator besondere Pflichten hinsichtlich der Generierung und Aufbewahrung des privaten Schlüssels auferlegt (siehe Kapitel 2.2).

a.sign corporate medium Zertifikate sind auch für die Erstellung von Signaturen im Sinne des § 2 Z 3 lit. a bis d [SigG] geeignet.

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 für a.sign corporate medium Zertifikate Beachtung fanden.

2 Verpflichtungen und Haftungsbestimmungen

2.1 Verpflichtungen von 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 (z. B. Verzeichnisdienst).

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 der Zertifizierungsrichtlinie für a.sign corporate (siehe [CPS]).

2.2 Verpflichtungen des Signators

a.trust bindet den Signator vertraglich an die Einhaltung der nachfolgend angeführten Verpflichtungen. Dem Zertifikatswerber werden die Vertragsbedingungen auf der Homepage zugänglich gemacht und gleichzeitig mit dem Absenden des Bestellformulars bestätigt er deren Kenntnisnahme und Akzeptanz.

Die dem Signator auferlegten Verpflichtungen umfassen:

1. die Angabe vollständiger und korrekter Informationen in Übereinstimmung mit den Anforderungen dieser Policy insbesondere anlässlich des Vorgangs der Registrierung,

2. die Generierung und Aufbewahrung des privaten Schlüssels in einer externen Hardware-Einheit wie einer Smartcard oder einem Hardware Security Modul,

3. die Anwendung entsprechender Vorsicht, um den unbefugten Gebrauch des privaten Schlüssels zu verhindern und die sichere Vernichtung desselben nach Ablauf der Gültigkeitsperiode,

4. die unverzügliche Benachrichtigung von a.trust, wenn vor Ablauf der Gültigkeitsdauer eines a.sign corporate medium Zertifikats, einer der nachfolgenden Fälle eintritt:

   - der private Schlüssel des Signators wurde möglicherweise kompromittiert,
   - die Kontrolle über den privaten Schlüssel ging verloren,
   - der private Schlüssel wurde auf einem anderen Medium als der bei der Bestellung angegebenen Smartcard oder Hardware Security Modul generiert oder abgespeichert,
   - die im Zertifikat beinhalteten Informationen sind inkorrekt oder haben sich geändert.

2.3 Verpflichtungen des Überprüfers von Zertifikaten

Ein Überprüfer, der ein a.sign corporate medium Zertifikat zur Verifizierung einer Signatur oder zur Verschlüsselung 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,
- eventuelle im Zertifikat oder den veröffentlichten Geschäftsbedingungen dargelegte Einschränkungen der Nutzung des Zertifikats beachtet (siehe dazu auch unten und Kapitel 1.3),
- und sämtliche anderweitig vorgeschriebene Vorsichtsmaßnahmen (siehe [CPS]) einhält.

2.4 Haftung

a.trust haftet als Aussteller von a.sign corporate medium Zertifikaten

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

- dafür, dass die im Zertifikat enthaltenen Daten zum Zeitpunkt der Ausstellung korrekt waren und anlässlich der Registrierung 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, Zertifikatsgenerierung, Zertifikatsausgabe, Widerrufsdiensten und Abfragediensten über den Zertifikatsstatus.

3.1 Certification Practice Statement

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

1. a.trust verfügt über eine Darstellung aller Vorgangsweisen und Prozeduren, die nötig sind, um die Anforderungen aus dieser Policy zu erfüllen.

2. Die Zertifizierungsrichtlinie für a.sign corporate benennt die Verpflichtungen von a.trust und aller externen Vertragspartner, die Dienstleistungen für a.trust unter Beachtung der jeweils anwendbaren Policies und Richtlinien erbringen.

3. a.trust macht allen Signatoren und anderen Personen, die auf die Zuverlässigkeit der a.trust Dienste vertrauen, das Certification Practice Statement und jegliche Dokumentation, die die Übereinstimmung mit dieser Policy dokumentiert, zugänglich (siehe Kapitel 3.3.4).

4. Die Geschäftsführung der a.trust stellt das alleinige Entscheidungsgremium dar, das für die Genehmigung der Zertifizierungsrichtlinie für a.sign corporate verantwortlich ist.

5. Die Geschäftsführung von a.trust trägt auch die Verantwortung für die ordnungsgemäße Implementierung der Zertifizierungsrichtlinie für a.sign corporate.

6. a.trust hat einen Revisionsprozess zur Überprüfung der Vorgangsweisen der Zertifizierung aufgesetzt, der auch Maßnahmen zur Wartung der Zertifizierungsrichtlinie für a.sign corporate umfasst.

7. a.trust wird zeitgerecht über Änderungen informieren, die im Certification Practice Statement vorgenommen werden und eine überarbeitete Version der Zertifizierungsrichtlinie für a.sign corporate entsprechend Punkt 3 dieses Absatzes unverzüglich zugänglich machen.

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] und damit in Übereinstimmung mit [SigRL] Annex II (f) und (g):

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

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

3. 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 Bestimmungen aus § 10 [SigV] sicher, dass die privaten Schlüssel geheim gehalten werden und ihre Integrität bewahrt bleibt und beachtet auch für die Erbringung von einfachen Zertifizierungsdiensten die Bestimmungen des § 10 [SigV].

3.2.3 Verteilung der öffentlichen CA Schlüssel

a.trust stellt durch die folgenden Maßnahmen sicher, dass die Integrität und Authentizität der öffentlichen Schlüssel anlässlich der Verteilung gewahrt bleibt:

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

- Ausstellung und Veröffentlichung eines selbstsignierten Root-Zertifikats.

Das Zertifikat des CA Schlüssels zur Signatur von a.sign corporate medium Zertifikaten wird den Signatoren durch Veröffentlichung im Rahmen des Verzeichnis-

dienstes zugänglich gemacht. a.trust gewährleistet die Authentizität dieses Zertifikats.

3.2.4 Schlüsseloffenlegung

Eine Offenlegung der geheimen CA Schlüssel ist nicht vorgesehen.

3.2.5 Verwendungszweck von CA Schlüsseln

Der private Schlüssel der Zertifizierungsstelle wird nur für die Erstellung von a.sign corporate medium Zertifikaten und für die Signatur der zugehörigen Widerrufslisten innerhalb von physisch abgesicherten Räumlichkeiten verwendet.

3.2.6 Ende der Gültigkeitsperiode von CA Schlüsseln

Geheime Schlüssel zur Signatur von a.sign corporate medium Zertifikaten werden verwendet, solange die verwendeten Algorithmen den Sicherheitserwartungen entsprechen. Die Zertifikate über die Schlüssel der Zertifizierungsstelle werden alle drei Jahre erneuert. Wenn die Algorithmen den Sicherheitserwartungen nicht mehr entsprechen, findet keine Erneuerung statt und die Schlüssel werden mit Erreichen des Endes der Gültigkeit gelöscht.

Eine Archivierung der geheimen Schlüssel ist nicht vorgesehen.

3.2.7 Erzeugung der Schlüssel für die Signatoren

Die Generierung des Schlüssels eines Signators wird von diesem selbst in einer speziell dafür vorgesehenen Hardware wie z. B. einer Smartcard oder einem Hardware Security Modul in sicherer Weise vorgenommen.

a.trust erhält keine Kenntnis des privaten Schlüssels.

3.3 Lebenszyklus des Zertifikats

3.3.1 Registrierung des Signators

Die Maßnahmen zur Identifikation und Registrierung des Zertifikatsinhabers stellen sicher, dass der Antrag auf Ausstellung eines a.sign corporate medium Zertifikats korrekt, vollständig und autorisiert ist.

1. Bevor der Vertrag zwischen dem Signator und a.trust abgeschlossen wird, werden dem Signator die Geschäftsbedingungen und allfällige sonstige Bestimmungen zur Nutzung des Zertifikats elektronisch zugänglich gemacht (siehe 3.3.4).

2. Das Antragsformular und die Informationen sind über die Web-Seite von a.trust elektronisch zugänglich.

3. Der Zertifikatsantrag enthält u. a. die folgenden Angaben:

   - den vollständigen Namen, Telefonnummer und E-Mailadresse des Signators, das ist ein technischer Verantwortlicher des Unternehmens wie z. B. Serveradministrator,
   - den vollständigen Namen und Kontaktinformation (Telefonnummer und E-Mailadresse) eines organisatorisch Verantwortlichen mit Zeichnungsberechtigung,
   - Passwort für den Widerruf
   - Firmenbuch- oder EBR-Nummer (wenn vorhanden),
   - Name und Sitz der Organisation,
   - Name der Organisationsuntereinheit,
   - optional E-Mailadresse für das Zertifikat (die E-Mailadresse muss zu einer im Besitz der Organisation befindlichen Domain gehören),
   - die zu zertifizierende öffentliche Schlüsselkomponente,
   - Angaben über die Hardware, welche zur Schlüsselgenerierung und –aufbewahrung verwendet wird.

4. Der mit dem Signator abzuschließende Vertrag beinhaltet insbesondere:

   - die Annahme der Verpflichtungen des Signators,

- 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.

5. 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 aller im Antrag genannten Personen,

   - ggf. Prüfung des Besitzes der Domain,

   - Prüfung, ob eine spezielle Hardware für Schlüsselgenerierung und –aufbewahrung verwendet wird,

   - Prüfung der Rechtmäßigkeit der Zertifikatsbestellung durch telefonische Rücksprache mit dem organisatorisch Verantwortlichen.

6. Der Zertifikatsantrag und alle damit im Zusammenhang stehenden vom Antragsteller zugesandten und in Papierform vorliegenden Daten und Dokumente (Ausweiskopien, ggf. Bestätigungen über das Unternehmen und die Vertretungsbefugnis) werden auf die Dauer von mind. sieben Jahren nach Ablauf der Gültigkeit (elektronisch) archiviert.

7. 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 des Zertifikats und Neuausstellungen

Durch die folgenden Maßnahmen wird sicher gestellt, dass Anträge von Zertifikatswerbern, die bereits anlässlich einer vorhergehenden Zertifikatsaus-stellung registriert wurden, vollständig, korrekt und ordnungsgemäß autorisiert sind. Die Maßnahmen gelten sowohl für die Verlängerung der Gültigkeitsdauer 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 Signator 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 Signators bestätigt.

4. Die Verlängerung der Gültigkeitsdauer von Zertifikaten vor deren Ablauf erfolgt entsprechend § 12 Abs 4 [SigV]. Die sich aus der Verlängerung ergebende neue Gültigkeitsperiode beträgt höchstens drei Jahre. Eine Verlängerung erfolgt nur wenn die kryptografische Sicherheit der verwendeten Verfahren über die gesamte neue Gültigkeitsdauer ausreichend sicher gestellt ist und keine Hinweise auf Kompromittierung des privaten Schlüssel des Antragsteller bestehen.

3.3.3 Erstellung des Zertifikats

Durch die folgenden Maßnahmen wird sicher gestellt, dass Ausstellung, Verlängerung und Neuausstellung von Zertifikaten in sicherer Weise erfolgen und auch den Anforderungen von [SigG] entsprechen.

1. Die a.sign corporate medium Zertifikate werden 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
   - Distinguished Name (subject)
     - Common Name
       Name des zertifizierten Schlüssels, wird aus der Organisation bzw. deren Kurzform, einer Kennung des Schlüssels und einem für die Organisation eindeutigen Ordnungsbegriff gebildet
     - Name der Organisation,
     - Name der Organisationsuntereinheit (Abteilung etc.): optional

- E-Mailadresse: optional
- Land des Sitzes der Organisation (z. B. AT, DE)

- 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

2. Die Zertifikate werden von der Zertifizierungsstelle erzeugt, nachdem der Signator identifiziert und die Rechtmäßigkeit des Antrags durch telefonische Rückfrage bestätigt wurde. Das Verfahren ist für die Ausstellung und Neuausstellung nach einem Widerruf oder Datenänderung identisch.

3. Die eindeutige Zuordnung des Zertifikats zum Signator ist sicher gestellt durch:
   - Erstellung des PKCS#10-Requests durch den Signator als Grundlage für die Zertifizierung.
   - Erzeugung des Zertifikats nach Überprüfung aller Antragsdaten auf ihre Korrektheit durch a.trust.

4. Die in der Registrierungsstelle aufgenommenen Daten werden signiert und verschlüsselt (SSL) an die Zertifizierungsstelle übertragen. Vertraulichkeit und Integrität sämtlicher Daten sind damit sicher gestellt.

5. Alle RA-Mitarbeiter sind mit Signaturkarte ausgestattet. Die Authentizität der übermittelten Registrierungsdaten wird durch Verifizierung der Signatur des RA-Mitarbeiters überprüft.

3.3.4 Bekanntmachung der Vertragsbedingungen

a.trust macht den Signatoren und den Benutzern, die auf die Zuverlässigkeit der a.trust Dienste vertrauen, die Bedingungen, welche die Benutzung des a.sign corporate medium Zertifikats betreffen, durch Veröffentlichung der folgenden Dokumente auf der a.trust Homepage zugänglich:

1. der gegenständlichen Certificate Policy,
2. des Certification Practice Statement (Zertifizierungsrichtlinie für a.sign corporate),
3. der Allgemeinen Geschäftsbestimmungen von a.trust,
4. der sonstigen Mitteilungen.

Änderungen werden dem Signator mittels Bekanntmachung auf der a.trust Homepage und ggf. zusätzlich per E-Mail oder brieflich mitgeteilt. Sie sind von jedermann von der a.trust Homepage abrufbar.

In o. a. Dokumenten ist das Folgende eindeutig festgelegt:

- a.sign corporate medium Zertifikate werden an Organisationen, welche Betreiber von Servern sind, ausgegeben,
- die Verpflichtungen des Signators gem. Kapitel 2.2.
- die Vorgehensweise zur Überprüfung eines Zertifikats inklusive der Notwendigkeit der Überprüfung des Zertifikatsstatus, so dass der Überprüfer mit gutem Grund dem Zertifikat vertrauen kann (siehe Kapitel 2.3),
- wie ggf. ein den Umfang der Haftung einschränkendes Transaktionslimit in a.sign corporate medium Zertifikaten zu erkennen ist,
- die Zeitdauer für die Aufbewahrung von Registrierungsinformationen (siehe Kapitel 3.3.1),
- die Zeitdauer für die Aufbewahrung von Aufzeichnungen wichtiger die Zertifizierungsstelle betreffender Ereignisse (siehe Kapitel 3.4.11),
- die Tatsache, dass der Betrieb als Zertifizierungsdiensteanbieter der Aufsichtsstelle gemäß §6 [SigG] angezeigt wurde,
- Vorgehensweisen zur Behandlung von Beschwerden und Streitfällen,
- die Anwendbarkeit des [SigG] und [SigV].

3.3.5 Veröffentlichung der Zertifikate

Von a.trust ausgestellte Zertifikate werden den Signatoren und den Überpüfern folgendermaßen verfügbar gemacht.

1. Alle a.sign corporate medium Zertifikate werden 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 corporate medium" einfach herstellbar.

4. Der Verzeichnisdienst ist an sieben Tagen pro Woche jeweils 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 eine irreversible vorzeitige Beendigung der Gültigkeit eines Zertifikats.

1. Die Vorgangsweise für das Auslösen des Widerrufs ist in der Zertifizierungsrichtlinie für a.sign corporate 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.

2. Ein Widerruf kann vom Signator innerhalb der Geschäftszeiten beim Widerrufsdienst für a.sign corporate medium Zertifikate telefonisch beantragt werden. Alle Anträge werden mit Einlangen bearbeitet. Zum Nachweis der Berechtigung des Antragstellers muss das bei der Zertifikatsbestellung gewählte Passwort für den Widerruf angegeben werden. Der Name der Organisation, der Name des Anrufers und im Zertifikat enthaltene Daten wie z. B. Common Name müssen dem Mitarbeiter des a.trust Widerrufsdienstes genannt werden. Die Daten des Anrufs werden aufgezeichnet und abgelegt. Wurde das Passwort für den Widerruf vergessen, so kann der Widerruf auch per Einschreiben mit firmenmäßiger Zeichnung beantragt werden.

3. Ein einmal widerrufenes Zertifikat kann nicht wieder Gültigkeit erlangen.

4. 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 von a.trust abrufbar.
   - Jede Widerrufsliste enthält den Zeitpunkt der geplanten Ausgabe der nächsten Liste.
   - Falls erforderlich kann eine neue Widerrufsliste auch vorzeitig (d. h. vor der nächsten geplanten Ausgabe) veröffentlicht werden.
   - Jede Widerrufsliste ist mit dem Zertifizierungsschlüssel signiert.

5. 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
   - Informationen 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.

6. Der Widerrufsdienst für a.sign corporate medium Zertifikate kann zu den Geschäftszeiten kontaktiert werden. Spätestens innerhalb von drei Stunden ab Bekanntwerden des Widerrufsgrundes erfolgt eine Aktualisierung der Widerrufsliste. Die jeweils aktuellen Geschäftszeiten können von der a.trust Homepage in Erfahrung gebracht werden.

7. Widerrufslisten sind täglich 24 Stunden abfragbar. Im Fall von Systemausfällen kommen die in der Zertifizierungsrichtlinie für a.sign corporate genannten Vorkehrungen zum Tragen, um die Auswirkungen möglichst gering zu halten.

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

9. Die Verzeichnisdienste für Widerrufslisten sind öffentlich und international zugänglich.

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 in der Zertifizierungsrichtlinie für a.sign corporate veröffentlicht.

2. Die Geschäftsführung von 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.

3.4.2 Informationsklassifikation und -verwaltung

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

3.4.3 Personelle Sicherheitsmaßnahmen

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

1. a.trust beschäftigt ausschließlich Personal, welches über das benötigte Fachwissen, die Qualifikation und Erfahrung für die jeweilige Position verfügt.

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

3. Für alle Mitarbeiter von 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 Verschlüsselungen und mit der Führung von Personal, das Verantwortung für sicherheitskritische Tätigkeiten trägt, verfügen.

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 in der a.sign corporate Zertifizierungsrichtlinie 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, welche sie für eine vertrauenswürdige Position ungeeignet erscheinen lassen. Eine Beschäftigung erfolgt erst nach einer diesbezüglichen Überprüfung.

3.4.4 Physikalische und organisatorische Sicherheitsmaßnahmen

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

1. Der Zutritt zu den Räumlichkeiten, in denen Zertifizierungs- und Widerrufsdienste erbracht werden, ist auf autorisiertes Personal beschränkt. Die Systeme, welche 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 Daten verarbeitenden 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 Zertifikatsgenerierung und Widerrufsdienste erfolgt durch klar definierte Sicherheitszonen, d. h. durch räumliche Trennung von anderen organisatorischen Einheiten sowie physischen Zutrittsschutz.

6. Die Sicherheitsmaßnahmen beinhalten den Gebäudeschutz, die Computersysteme selbst und alle sonstigen Einrichtungen, die für deren Betrieb unerlässlich sind. Der Schutz der Einrichtungen für die Zertifikatserstellung und Bereitstellung der Widerrufsdienste umfasst physische Zutrittskontrolle, Abwendung von Gefahren durch Naturgewalten, Feuer, Rohrbrüche und Gebäudeeinstürze, Schutz vor Ausfall von Versorgungseinheiten sowie vor 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 worden.

5. Datenträger werden je nach ihrer Sicherheitsstufe 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 ausreichender 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. Betriebliche 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 betrieblichem 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.

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 in der Zertifizierungsrichtlinie für a.sign corporate angeführt. Administrative und den 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 in Zusammenhang 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 befinden sich in einer physisch gesicherten Umgebung, die Konfiguration wird periodisch 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.

10. Änderungen (Löschungen, Hinzufügungen) der Verzeichnis- und Widerrufsdienste müssen durch eine Signatur der Zertifizierungsstelle gesichert sein.

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 folgendes vorgesehen:

1. Der Notfallsplan von a.trust sieht die (tatsächliche oder 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 Signatoren, die auf die Verlässlichkeit 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 ihrer Dienstleistungen sowohl gegenüber Signatoren als auch gegenüber allen auf die Zuverlässigkeit der Dienste vertrauenden Parteien möglichst gering gehalten ist.

1. Vor Beendigung der Dienstleistung werden

   - alle Signatoren, Zertifizierungsdiensteanbieter und sonstige Parteien, mit denen a.trust eine geschäftliche Verbindung unterhält, direkt und andere auf die Zuverlässigkeit der a.trust-Dienste vertrauende Parteien durch Veröffentlichung von der Einstellung unterrichtet,

   - die Verträge mit Subunternehmern (Verzeichnisdienst etc.) 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 und gelöscht.

2. Die Abdeckung der Kosten für o. a. Vorkehrungen sind durch Gesellschaftergarantien abgedeckt.

3. Die Zertifizierungsrichtlinie für a.sign corporate benennt die Vorkehrungen, die bei Einstellung der Tätigkeit getroffen werden, insbesondere jene

   - für die Benachrichtigung der betroffenen Personen und Organisationen,

   - für die Übertragung der Verpflichtungen auf Dritt-Parteien 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 worden, um persönliche Daten vor unautorisierter und ungesetzlicher Verarbeitung sowie vor versehentlicher Zerstörung oder Beschädigung zu schützen.

4. Den Signatoren 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 a.sign corporate medium Zertifikaten

Alle Informationen, die in Zusammenhang mit a.sign corporate medium Zertifikaten stehen, werden aufbewahrt. Insbesondere gilt:

1. Die Vertraulichkeit und Integrität der aktuellen sowie der archivierten Daten wird gewahrt.

2. Alle Daten zu a.sign corporate medium Zertifikaten werden vollständig, vertraulich und in Übereinstimmung mit der veröffentlichten Zertifizierungsrichtlinie archiviert.

3. Aufzeichnungen, welche a.sign corporate medium Zertifikate betreffen, werden für die Beweisführung der ordnungsgemäßen Zertifizierung im Rahmen gerichtlicher Auseinandersetzungen verfügbar gemacht. Zusätzlich hat der Signator zu den Registrierungs- und sonstigen persönlichen Daten, die ihn betreffen, Zugang.

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 a.sign corporate medium Zertifikaten stehen, werden, sofern nicht ausdrücklich ein anderer Zeitraum genannt wird, für mind. sieben Jahre elektronisch aufbewahrt.

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

7. Die spezifischen Ereignisse und Daten, die aufgezeichnet werden, sind in der Zertifizierungsrichtlinie dokumentiert.

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

9. Die Vertraulichkeit der Daten der Signatoren ist gewährleistet.

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

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

12. Alle Anträge auf Widerruf und die damit verbundenen Informationen werden aufgezeichnet.

3.5 Organisatorisches

a.trust ist als Organisation zuverlässig und hält die in den folgenden Kapiteln (siehe 3.5.1 und 3.5.2) angeführten Richtlinien strikt ein.

3.5.1 Allgemeines

1. Alle Richtlinien und Vorgehensweisen sind nicht-diskriminierend.

2. Die Dienstleistungen im Rahmen von a.sign corporate medium stehen Organisationen, welche Server betreiben und sich verpflichten, die von a.trust auferlegten Richtlinien hinsichtlich der Sicherheit der Schlüsselgenerierung einzuhalten, 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. Hinsichtlich der finanziellen Ausstattung befolgt a.trust die Bestimmungen in § 2 [SigV].

6. 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.

7. 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.

8. Die rechtlichen Beziehungen zu Subunternehmern, welche Dienstleistungen für a.trust erbringen, sind vertraglich geregelt und ausführlich dokumentiert.

9. 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 von a.trust unabhängig von anderen Gesellschaften. Die Geschäftsführung und das Personal, welches sicherheitskritische und leitende Funktionen ausübt, ist frei von kommerziellem, finanziellem und sonstigem Druck, der die Zuverlässigkeit ihrer 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

a.sign corporate medium Zertifikat	Ein nicht qualifiziertes Zertifikat, das für einen Server ausgestellt wird und mit dem besondere Verpflichtungen hinsichtlich der Schlüsselgenerierung verbunden sind.
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.
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 geheim zu haltende 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.

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 System	Ein kryptographisches 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 Teil wird von seinem Besitzer sicher bewahrt und kann Daten entschlüsseln oder eine digitale Signatur erstellen.
Qualifiziertes Zertifikat	Zertifikat, welches den Bestimmungen lt. § 5 [SigG] 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.
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.
Signaturerstellungseinheit	Komponenten, die vom Unterzeichner verwendet werden, um eine elektronische Signatur zu erstellen.
SSL	Secure Socket Layer, ein Protokoll zur sicheren Übertragung von Daten über das Internet mit Hilfe eines Public-Key Systems.
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 Zertifikatserweiterungen erstellt werden können
Zertifikats-Widerrufsliste, CRL	Eine digital signierte Datenstruktur, die widerrufene Zertifikate anführt, welche von einem bestimmten Zertifizierungsdiensteanbieter ausgestellt wurden.
Zertifizierungsdienste-anbieter, Certification Authority, CA	Eine Person oder Stelle, die Zertifikate ausstellt oder anderweitige elektronische Signaturdienste öffentlich anbieten darf.
Zertifizierungsrichtlinie	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 (Datenschutzgesetz 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 einfache Zertifikate a.sign corporate
[ETSI]	Policy requirements for certification authorities issuing qualified certificates – ETSI TS 101 456
[RFC2527]	RFC 2527, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, March 1999