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 government user

Version: 1.0

Datum: 11.12.2003

Inhaltsverzeichnis

1 Einführung

1.1 Überblick

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

Die a.sign government user Certificate Policy gilt für einfache Zertifikate entsprechend den Definitionen der EU-Richtlinie [SigRL] und dem Österreichischen Bundesgesetz über elektronische Signaturen, welche an Endbenutzer ausgestellt werden, keine sicheren Signaturerstellungseinheiten voraussetzen und für die Erstellung einfacher digitaler Signaturen geeignet sind.

1.2 Identifikation

Name der Policy:	a.trust Certificate Policy für einfache Zertifikate a.sign government user
Version:	1.0/11.12.2003
Object Identifier:	**1.2.040.0.17** (a.trust)**.1** (Policy)**.14.2** (a.sign government user) **.1.0** (Version) vorliegende Version

Die vorliegende Policy ist in Übereinstimmung mit den Anforderungen aus RFC 2527.

1.3 Anwendungsbereich

Die a.sign government user Certificate Policy gilt für einfache Zertifikate entsprechend der Definition § 2 Abs. 8 [SigG], die ausschließlich an Endbenutzer, welche in der öffentlichen Verwaltung beschäftigt sind, ausgestellt werden. Die geheimen Schlüssel der Zertifikatsinhaber befinden sich auf deren PC und sind durch Software-Verschlüsselung gesichert.

Signaturen, die in Übereinstimmung mit dieser Policy hergestellt werden, sind einfache Signaturen im Sinne des [SigG] und entsprechen Artikel 5.2 der EU-Richtlinie [SigRL].

Auch einfache digitale Signaturen können somit lt. Signaturgesetz Rechtwirksamkeit entfalten: „Die rechtliche Wirksamkeit einer elektronischen Signatur und deren Verwendung als Beweismittel können nicht allein deshalb ausgeschlossen werden, weil die elektronische Signatur nur in elektronischer Form vorliegt, weil sie nicht auf einem qualifizierten Zertifikat oder nicht auf einem von einem akkreditierten Zertifizierungsdiensteanbieter ausgestellten qualifizierten Zertifikat beruht oder weil sie nicht unter Verwendung von technischen Komponenten und Verfahren im Sinne des § 18 erstellt wurde.“ (siehe § 3 (1) [SigG]).

Ausgestellt werden diese Zertifikate mit einem Behördenkennzeichen in den Zertifikatserweiterungen ausschließlich an Angehörige von österreichischen Behörden (Organisationseinheiten der öffentlichen Verwaltung). Ein definierter Organisationsverantwortlicher der jeweiligen Behörde stellt sicher, dass die beantragende Person ein Recht auf die Ausstellung eines Behördenzertifikats hat. Die beantragende Person muss außerdem über eine E-Mailadresse mit dem Aufbau antragsteller@organisation.gv.at verfügen.

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 government user 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 (Registrierungsstellen, Widerrufsdienste).

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 government.

2.2 Verpflichtungen des Zertifikatsinhabers

a.trust bindet den Zertifikatsinhaber vertraglich an die Einhaltung der nachfolgend angeführten Verpflichtungen. Im Rahmen der Registrierung wird der Zertifikatsinhaber auf die Vertragsbedingungen der a.trust Homepage hingewiesen.

Die dem Zertifikatsinhaber auferlegten Verpflichtungen umfassen:

- die Angabe vollständiger und korrekter Informationen in Übereinstimmung mit den Anforderungen dieser Policy,
- die ausschließliche Verwendung des privaten Schlüssels für die im Zertifikat eingetragenen Zwecke unter Beachtung der dem Anwender mitgeteilten Beschränkungen,
- die Anwendung entsprechender Vorsicht, um den unbefugten Gebrauch seines privaten Schlüssels zu verhindern und die sichere Vernichtung desselben nach Ablauf der Gültigkeitsperiode,
- die unverzügliche Benachrichtigung von a.trust, wenn vor Ablauf der Gültigkeitsdauer des Zertifikats, einer der nachfolgenden Fälle eintritt:

- der private Schlüssel des Zertifikatsinhabers wurde verloren, gestohlen oder möglicherweise kompromittiert,
- die Kontrolle über den privaten Schlüssel durch Kompromittierung der Aktivierungsdaten (PIN) oder durch andere Umstände ging verloren,
- die im Zertifikat beinhalteten Informationen haben sich geändert.

2.3 Verpflichtungen des Überprüfers von Zertifikaten

Ein Zertifikatsnutzer der ein a.trust Zertifikat zur Verifizierung einer Signatur 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 Kapitel 1.3),
- und sämtliche anderweitig vorgeschriebene Vorsichtsmaßnahmen (siehe [CPS]) einhält.

2.4 Haftung

a.trust haftet als Aussteller von a.sign government user 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 enthaltene E-Mailadresse zum Zeitpunkt der Ausstellung korrekt war und dass die Übereinstimmung der Zertifikatsdaten mit dem Antrag überprüft wurde,
- dafür, dass die mit dem Behördenkennzeichen gekennzeichneten Zertifikate nur an jene Personen, deren Daten von einem definierten organisatorischen Verantwortlichen genehmigt wurden und welche über eine E-Mailadresse der

Domain gv.at in der Form antragsteller@organisation.gv.at verfügen, ausgestellt werden.

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, die Bereitstellung von Schlüsselpaaren, die Zertifikatsgenerierung und Zertifikatsausgabe und die Bereitstellung von Widerrufsdiensten und Abfragediensten über den Zertifikatsstatus.

3.1 Certification Practice Statement

a.trust hat die nachfolgend aufgelisteten 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 government 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 Zertifikatsinhabern und Überprüfern von Zertifikaten 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 verantwortlich ist.

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

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

7. a.trust wird zeitgerecht über beabsichtigte Änderungen informieren, die im Certification Practice Statement vorgenommen werden sollen und eine überarbeitete Version der Zertifizierungsrichtlinie für a.sign government 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) mindestens 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] und den Empfehlungen der Expertengruppe der European Electronic Signature Standardisation Initiative.

3.2.2 Speicherung der CA-Schlüssel

a.trust stellt 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].

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, die garantieren, dass die privaten Schlüssel von a.trust das Hardware Security Modul nicht verlassen und kein Zugriff von außen darauf möglich ist.

Es werden keine Sicherungskopien der Schlüssel hergestellt; die entsprechende Funktion wird während der Initialisierung der Hardware Security Module still gelegt.

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 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 a.trust-Schlüssels wird den Zertifikatsinhabern durch Veröffentlichung im Rahmen des Verzeichnisdienstes zugänglich gemacht. a.trust gewährleistet die Authentizität dieses Zertifikats.

3.2.4 Schlüsseloffenlegung

Eine Offenlegung der privaten Schlüssel der Zertifizierungsstelle ist nicht vorgesehen und auf Grund der Speicherung in gesicherten Signaturerstellungseinheiten auch nicht möglich.

3.2.5 Verwendungszweck von a.trust-Schlüsseln

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

3.2.6 Ende der Gültigkeitsperiode von a.trust-Schlüsseln

Geheime Schlüssel zur Signatur von a.sign government user Zertifikaten werden mit Erreichen des Endes ihrer Gültigkeit deaktiviert.

Eine Archivierung ist nicht vorgesehen und auf Grund der Speicherung in gesicherten Signaturerstellungseinheiten auch nicht möglich.

Eine Verwendung über die Gültigkeitsperiode hinaus ist damit ausgeschlossen.

3.2.7 Verwaltung und Lebenszyklus der Hardware Security Module für die Zertifizierung

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

1. Die Sicherheit des Hardware Security Moduls wird während des Transports und der Lagerung durch Verschweißung in spezieller Folie erreicht.

2. Die Nutzung eines Hardware Security Modul, das gültige Zertifizierungsschlüssel enthält, ist an das Zusammenwirken von zwei autorisierten a.trust-Mitarbeitern gebunden.

3. Die korrekte Funktionsweise des Hardware Security Moduls wird von a.trust bei Inbetriebnahme überprüft.

4. Geheime Schlüssel zur Signatur von a.sign government user Zertifikaten werden deaktiviert, bevor ein Hardware Security Modul außer Betrieb genommen wird.

3.2.8 Erzeugung der Schlüssel für die Zertifikatsinhaber

Die Generierung der Schlüssel der Zertifikatsinhaber erfolgt entweder in der Software der Registrierungsstelle oder im Browser des Antragstellers. Die Art der Generierung des Schlüssels wird vom Organisationsverantwortlichen festgelegt.

Die Sicherheit und Geheimhaltung der privaten Schlüssel sind durch die folgenden Maßnahmen gewährleistet:

- Der verwendete Algorithmus ist für digitale Signaturen geeignet.

- Die verwendete Schlüssellänge und der Algorithmus wären auch für sichere digitale Signaturen geeignet und entsprechen Anhang I [SigV] und den Empfehlungen der Expertengruppe der European Electronic Signature Standardisation Initiative.

- Bei Generierung der Schlüssel durch die Registrierungsstelle erfolgt die Übergabe des a.sign government user Zertifikats und des Schlüsselpaares an den Zertifikatsinhaber in verschlüsselter und gegen Veränderung gesicherter Form. Die benötigte PIN wird dem Zertifikatsinhaber per Telefon durchgesagt.

- Bei Generierung der Schlüssel im Browser des Zertifikatsinhabers erhält der Zertifikatsinhaber von der CA eine E-Mail mit Passwort zur Abholung des Zertifikats.

3.2.9 Sicherheit der a.sign government user Schlüssel

Für die Sicherheit der privaten Schlüsselkomponente ist der Zertifikatsinhaber verantwortlich.

Die Speicherung des Schlüssels erfolgt auf einem Speichermedium in seiner Einflusssphäre in verschlüsselter Form.

3.3 Lebenszyklus des Zertifikats

3.3.1 Registrierung des Zertifikatsinhabers

Ein persönliches Erscheinen des Zertifikatsinhabers in der Registrierungsstelle ist für die Ausstellung eines a.sign government user Zertifikats nicht erforderlich.

Der Zertifikatswerber erstellt einen Antrag auf Ausstellung eines Zertifikats aus, der an an a.trust übermittelt wird.

Der Antrag enthält die folgenden Anaben:

- den vollständigen Namen des Zertifikatswerbers,
- Organisationszugehörigtkeit
- Dienstanschrift, Diensttelefonnummer
- die E-Mailadresse (Domain gv.at) des Zertifikatswerbers
- E-Mailadresse, Kontaktdaten des Organisationsverantwortlichen
- ggf. Verwaltungsbezeichner

Der Name des Zertifikatsinhabers und seine E-Mailadresse (Zertifikatserweiterung) sind zwingende Inhalte des Zertifikats.

Die Generierung des Schlüsselpaars übernimmt entweder die Registrierungsstelle oder der Antragsteller selbst in seinem Browser (Anstoß über eine von a.trust bekannt gegebene Web-Applikation).

Der Zertifikatsantrag und alle damit im Zusammenhang stehenden relevanten Aufzeichnungen werden archiviert.

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

3.3.2 Neuausstellung des Zertifikats

Nach Ablauf der Gültigkeitsdauer oder Widerruf wird ein neues Zertifikat ausgestellt.

Bei Neuausfolgung eines a.sign government user Zertifikats nach Ablauf oder Widerruf eines Zertifikats hat die Registrierungsstelle die Daten zur Identifikation des Antragstellers hinsichtlich ihrer aktuellen Gültigkeit erneut zu prüfen.

Etwaige Änderungen in den Vertragsbedingungen werden dem Antragsteller mitgeteilt.

3.3.3 Erstellung des Zertifikats

Durch die folgenden Maßnahmen wird sicher gestellt, dass die Ausstellung von Zertifikaten in sicherer Weise erfolgt.

1. Die a.sign government user 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
   - 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
- Der für alle Behördenzertifikate verpflichtende Ausdruck der Behördeneigenschaft (Behördenkennzeichen) : Object Identifier, der die Behördeneigenschaft ausdrückt
  ggf. kann auch ein Verwaltungsbezeichner angegeben werden
- E-Mailadresse
- Zertifikatsverwendung
- Information zum Auffinden der CRL.

2. Das Schlüsselpaar des a.sign government user Zertifikats wird unmittelbar vor Ausstellung des Zertifikats in der Registrierungsstelle oder unmittelbar vor dem Absenden des öffentlichen Schlüssels an a.trust im Browser des Antragstellers generiert. Die eindeutige Zuordnung zum Zertifikatsinhaber ist durch die Unmittelbarkeit der Abfolge der einzelnen Schritte sicher gestellt.

3. Jedem Antragsteller wird eine innerhalb von a.trust einmalig vergebene und eindeutige Identifikationsnummer zugeordnet. Um die Eindeutigkeit des hervorgehobenen Namens des Zertifikatsinhabers zu erreichen, werden die Namensangaben im Zertifikatsinhaber-Attribut (subject) um diese Nummer ergänzt.

3.3.4 Bekanntmachung der Vertragsbedingungen

a.trust macht den Zertifikatsinhabern und Überprüfern die Bedingungen betreffend die Benutzung von a.sign government user Zertifikaten durch Veröffentlichung der nachfolgenden Dokumente auf der a.trust-Homepage zugänglich:

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

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

In o. a. Dokumenten ist eindeutig festgelegt:

- a.sign government user Zertifikate werden ausschließlich an Angehörige österreichischer Behörden ausgegeben, deren Antrag von einem Organisationsverantwortlichen genehmigt wurde,
- die Verpflichtungen des Zertifikatsinhabers entsprechend 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),
- die Zeitdauer für die Aufbewahrung der 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,
- die Anwendbarkeit des [SigG] und [SigV].

3.3.5 Veröffentlichung der Zertifikate

Von a.trust ausgestellte Zertifikate werden den Zertifikatsinhabern und den Überprüfern folgendermaßen verfügbar gemacht.

1. Das Zertifikat wird (bei Generierung durch die RA, zusammen mit dem Schlüsselpaar) gesichert an den Zertifikatsinhaber übermittelt.
2. Das Zertifikat wird im Verzeichnisdienst von a.trust veröffentlicht.
3. Die Bedingungen für die Benutzung eines Zertifikats werden von a.trust allen Beteiligten zur Kenntnis gebracht (siehe Kapitel 3.3.4).
4. Die Identifikation der anzuwendenden Bestimmungen ist durch die eindeutige Zuordnung zum Produktnamen „a.sign government user“ einfach herstellbar.
5. 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.
6. Die Verzeichnisdienste sind öffentlich und international zugänglich.

3.3.6 Widerruf

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

Die Vorgangsweise für das Auslösen eines Widerrufs ist in der Zertifizierungsrichtlinie für a.sign government 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.
- Der Widerruf kann telefonisch mit Angabe des Widerrufspassworts beantragt werden. Alle Anträge werden mit Einlangen bearbeitet.
- Ein einmal widerrufenes Zertifikat kann nicht wieder Gültigkeit erlangen.
- 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 veröffentlicht werden.
- Jede Widerrufsliste ist mit dem Zertifizierungsschlüssel signiert.
- Die Widerrufsdienste können zu den auf der Homepage angegebenen Zeiten kontaktiert werden. Spätestens innerhalb von drei Stunden ab Bekanntwerden des Widerrufsgrundes erfolgt eine Aktualisierung der Widerrufsliste.
- Beim Antrag auf Widerruf eines Zertifikats muss der Grund für den Widerruf angegeben werden.
- Widerrufslisten sind täglich 24 Stunden abfragbar. Im Fall von Systemausfällen kommen die in der Zertifizierungsrichtlinie für a.sign government user geannten 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.
- Die Verzeichnisdienste für Widerrufslisten sind öffentlich und international zugänglich.

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.

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 Registrierungs- und Widerrufsdienste. 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 government 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, entsprechend der Dokumentation implementiert und gewartet.

5. Der Betrieb des Rechenzentrums, der Registrierungsstelle und des Widerrufsdienstes der a.trust sind an Vertragspartner ausgelagert. Die Vertragspartner sind 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 Einstellungsmodalitäten sind geeignet, das Vertrauen in die Abwicklung der Zertifizierungsdienste zu stärken. Insbesondere wird auf die folgenden Maßnahmen Wert gelegt:

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

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

- 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.

- Die Ausübung der administrativen und Management-Funktionen steht im Einklang mit den Sicherheitsrichtlinien.
- Alle Leitungsfunktionen sind mit Personen besetzt, die über Erfahrung mit der Technologie digitaler Signaturen und mit der Führung von Personal, das Verantwortung für sicherheitskritische Tätigkeiten trägt, verfügen.
- Alle Mitarbeiter, denen vertrauenswürdige Positionen zugeordnet sind, werden von Interessenskonflikten, die einer unvoreingenommenen Erfüllung der Aufgaben entgegenstehen könnten, frei gehalten.
- Alle vertrauenswürdigen Positionen sind in der a.sign government Zertifizierungsrichtlinie im Detail beschrieben (siehe [CPS]).
- Die Zuweisung der Positionen erfolgt mit formeller Ernennung durch die Geschäftsführung.
- Entsprechend § 10 (4) [SigV] beschäftigt a.trust keine Personen, die strafbare Handlungen begangen haben, welche sie für eine vertrauenswürdige Position ungeeignet erscheinen lassen. Eine Einstellung 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 der Vermögenswerte minimiert sind. Insbesondere gilt:

- Der Zutritt zu den Räumlichkeiten, in denen Zertifizierungs- und Widerrufsdienste erbracht werden, ist auf autorisiertes Personal beschränkt. Die Systeme, welche die Zertifikate ausstellen, sind vor Gefährdung durch Umweltkatastrophen geschützt.
- Es werden Maßnahmen ergriffen, um den Verlust, die Beschädigung oder die Kompromittierung von Anlagen und die Unterbrechung des Betriebes zu verhindern.
- Weitere Maßnahmen gewährleisten, dass eine Kompromittierung oder ein Diebstahl von Daten und Daten verarbeitenden Anlagen nicht möglich ist.
- Die Systeme für die Zertifikatsgenerierung und die Widerrufsdienste werden in einer gesicherten Umgebung betrieben, sodass eine Kompromittierung durch unautorisierte Zugriffe nicht möglich ist.

- 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.

- 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 Betrieb 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.

- 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:

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

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

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

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

- Datenträger werden je nach ihrer Sicherheitsstufe behandelt und aufbewahrt. Nicht mehr benötigte Datenträger, die vertrauliche Daten beinhalten, werden in sicherer Weise vernichtet.

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

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

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

Sicherheitskritische Funktionen inkludieren:

- Betriebliche Funktionen und Verantwortungen
- Planung und Abnahme von Sicherheitssystemen
- Schutz vor böswilliger Software
- Allgemeine Wartungstätigkeiten
- Netzwerkadministration
- Aktive Überprüfung von Log-Files und Prüfberichten, Analyse von Zwischenfällen
- Datenträgerverwaltung und –sicherheit
- Daten- und Softwareaustausch

Diese Aufgaben werden von a.trust-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, wie z. B. die Registrierungsdaten.

3. Eine Benutzerverwaltung, die den verschiedenen Funktionen unterschiedliche Zugriffsrechte einräumt, ist eingerichtet; insbesondere werden sicherheitsrelevante Funktionen von unkritischen exakt getrennt. Änderungen in den Zugriffs-

rechten 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 government 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 (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 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 Zertifikatsinhabern als auch gegenüber allen auf die Zuverlässigkeit der a.trust-Dienste vertrauenden Parteien möglichst gering gehalten ist.

1. Vor Beendigung der Dienstleistung werden

   - alle Zertifikatsinhaber, 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 (Registrierungsstellen 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 in Entsprechung zu Kapitel 3.2.6 deaktiviert.

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

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

   - 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:

- Wichtige Aufzeichnungen werden vor Verlust, Zerstörung und Verfälschung bewahrt.
- Die Anforderungen des Datenschutzgesetzes werden befolgt.
- Nötige technische und organisatorische Maßnahmen sind ergriffen worden, um persönliche Daten vor unautorisierter und ungesetzlicher Verarbeitung sowie vor versehentlicher Zerstörung oder Beschädigung zu schützen.
- 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 a.sign government user Zertifikaten

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

- Die Vertraulichkeit und Integrität der aktuellen sowie der archivierten Datensätze ist gewahrt.

- Die Daten zu a.sign government user Zertifikaten werden vollständig, vertraulich und in Übereinstimmung mit der veröffentlichten Zertifizierungsrichtlinie archiviert.
- Alle Daten, die in Zusammenhang mit den Zertifikaten stehen, werden, sofern nicht explizit ein anderer Zeitraum genannt wird, für mind. sieben Jahre aufbewahrt.
- Alle Aufzeichnung erfolgen derart, dass sie innerhalb der Aufbewahrungsfrist nicht unbemerkt versehentlich oder absichtlich gelöscht oder zerstört werden können.
- Die spezifischen Ereignisse und Daten, die aufgezeichnet werden, sind in den Zertifizierungsrichtlinien dokumentiert.
- Insbesondere werden alle Registrierungsinformationen, inkl. jener, die im Zusammenhang mit der Neuausstellung von Zertifikaten stehen, aufbewahrt.
- Die Vertraulichkeit der Daten der Zertifikatsinhaber ist gewährleistet.
- Es werden alle Ereignisse, die den Lebenszyklus der Schlüssel der a.trust und den Lebenszyklus der Zertifikate betreffen, aufgezeichnet.
- Wesentliche Ereignisse, die im Zusammenhang mit der Generierung der Schlüssel der Zertifikatsinhaber stehen, werden aufgezeichnet.
- 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 government user stehen ausschließlich Angehörigen österreichischer Behörden mit einer E-Mailadresse des Formats antragsteller@organisation.gv.at 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 von 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 das Vertrauen in ihre Tätigkeit negativ beeinflussen könnte.

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

4 Anhang

A Begriffe und Abkürzungen

a.sign government user	Produktname für a.sign Software Zertifikate, die an Behördenmitarbeiter mit einer E-Mailadresse der Domain gv.at ausgestellt werden.
Certificate Policy, Policy	Ein Regelwerk, das den Einsatzbereich eines Zertifikates für eine bestimmte Benutzergruppe und/oder Anwendungsklasse festhält.
Certification Practice Statement, CPS, Zertifizierungsrichtlinie	Aussagen über die bei der Ausstellung von Zertifikaten von einem Zertifizierungsdiensteanbieter eingehaltenen Vorgehensweise
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 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 Teil eines Schlüsselpaares, der zum digitalen Signieren sowie zum Entschlüsseln von Nachrichten/Dokumenten erforderlich ist und geheimgehalten 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 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 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.

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 government