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

a.trust
Certificate Policy für einfache Zertifikate a.sign GRZ-IT

Version: 1.0.3
Datum: 07.10.2009

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 GRZ-IT 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 GRZ-IT
Version:	1.0.3/ 07.10.2009
Object Identifier:	1.2.040.0.17 (a.trust) .1 (Policy) .15 (a.sign company root) .2 (a.sign GRZ-IT) .1.0.3 (Version) vorliegende Version

Die vorliegende Policy ist in Übereinstimmung mit den Anforderungen aus [RFC3647].

1.3 Anwendungsbereich

Die a.sign GRZ-IT Policy gilt für einfache a.sign GRZ-IT Zertifikate entsprechend der Definition § 2 Abs. 8 [SigG], welche zur Durchführung von Signatur- und Geheimhaltungsoperationen ausgestellt werden.

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].

Ausgestellt werden diese Zertifikate an die Benutzer aller Kunden der GRZ IT Center Linz GmbH.

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 GRZ-IT 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 Sorge zu tragen; 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.

2.2 Verpflichtungen des Zertifikatsinhabers

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,
- 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 der Zertifikatsausgebenden Stelle, 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 ging verloren,
  - die im Zertifikat beinhalteten Informationen sind inkorrekt oder haben sich geändert.

2.3 Verpflichtungen des Überprüfers von Zertifikaten

Ein Überprüfer, der ein a.trust 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 und a.trust bereitgestellten Abfragemöglichkeiten vornimmt (siehe dazu Kapitel 3.3.7),
- 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 einhält.

2.4 Haftung

GRZ-IT haftet als Aussteller von a.sign GRZ-IT Company Root Zertifikaten für die Einhaltung der in dieser Policy festgelegten Richtlinien, insbesondere für die Maßnahmen zur prompten Veröffentlichung von Widerrufslisten und die Einhaltung der genannten Standards (ITU X.509).

GRZ-IT 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

GRZ-IT gibt für den Zertifizierungsdienst von a.sign GRZ-IT Zertifikaten keine Zertifizierungsrichtlinie heraus. Alle Maßnahmen zur sicheren und verlässlich Erbringung des Zertizierungsdienstes werden in dieser Policy beschrieben.

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 CA Schlüssel zur Ausstellung von qualifizierte Zertifikate als geeignet angesehen werden würde.
3. Die Schlüssellänge und der Algorithmus wären ebenfalls zu Ausstellung von qualifizierte Zertifikate geeignet und entsprechen Anhang I [SigV].

Für die von GRZ-IT erzeugten CA Schlüssel gilt folgendes: In der aktuellen Version sind dies 2048 Bit lange Schlüssel welche mit sha1RSA signiert werden. Die dazu erforderlichen Zufallszahlen werden mithilfe des OpenBSD - Zufallsgenerator erzeugt. Die Schlüssel werden in einer LDAP - Datenbank gespeichert. Der Zugang zu dieser Datenbank erfolgt im Normalfall ausschliesslich geräteintern für die Entschlüsselung / Signatur der zu verarbeitenden Mails. Konsolenzugriff bzw. Zugriff über eine ssh-Shell sollte vom Kunden den Anforderungen entsprechend unterbunden werden.

3.2.2 Speicherung der CA Schlüssel

a.trust stellt sicher, dass die von a.trust generierten privaten Schlüssel geheim gehalten werden und ihre Integrität bewahrt bleibt.

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:

- Ausstellung und Veröffentlichung eines selbst signierten Root-Zertifikats,
- Ausstellung und Veröffentlichung eines durch die Aufsichtsstelle und das Root-Zertifikat signierten Zwischeninstanz-Zertifikats und durch
- Ausstellung und Veröffentlichung eines durch das Zwischeninstanz-Zertifikat signierten Ausstellerzertifikates.

Das Zertifikat des CA Schlüssels zur Signatur von a.sign GRZ-IT Zertifikaten 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 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 GRZ-IT Zertifikaten und für die Signatur der zugehörigen Widerrufslisten oder Antworten von OCSP Anfragen innerhalb von physisch abgesicherten Räumlichkeiten verwendet.

3.2.6 Ende der Gültigkeitsperiode von CA Schlüsseln

Geheime Schlüssel zur Signatur von a.sign GRZ-IT Zertifikaten werden verwendet, solange die verwendeten Algorithmen den Sicherheitserwartungen entsprechen. Die Zertifikate über die Schlüssel der a.trust Zertifizierungsstelle werden spätestens alle zehn Jahre erneuert. Eine Archivierung der geheimen Schlüssel ist nicht vorgesehen.

3.2.7 Erzeugung der Schlüssel für die Zertifikatsinhaber

Die Schlüssel für die Benutzer werden von der SEPPmail Appliance mit einem Algorithmus und einer Schlüssellänge generiert, die auch für CA Schlüssel zur Ausstellungvon qualifizierter Zertikate als geeignet angesehen werden würde. In der aktuellen Version sind dies 2048 Bit lange Schlüssel welche mit sha1RSA signiert werden. Die dazu erforderlichen Zufallszahlen werden mithilfe des OpenBSD - Zufallsgenerator erzeugt. Die Schlüssel werden in einer LDAP - Datenbank gespeichert. Der Zugang zu dieser Datenbank erfolgt im Normalfall ausschliesslich geräteintern für die Entschlüsselung / Signatur der zu verarbeitenden Mails. Konsolenzugriff bzw. Zugriff über eine ssh-Shell sollte vom Kunden den Anforderungen entsprechend unterbunden werden.

3.2.8 Sicherheit der a.sign GRZ-IT Schlüssel

Die Sicherheit der privaten Schlüsselkomponente ist in Kapitel 3.2.7 beschrieben.

3.3 Lebenszyklus des Zertifikats

3.3.1 Registrierung des Zertifikatsinhabers

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

Ein persönliches Erscheinen des Zertifikatsinhabers in der Registrierungsstelle ist für die Ausstellung eines a.sign GRZ-IT Zertifikats nicht erforderlich.

Der Registrierungsstelle sind zumindest folgende Daten des Zertifikatswerbers bekanntzugeben:

- den vollständigen Namen,
- eine Kontaktadresse,
- die E-Mail-Adresse und
- eine Telefonnummer.

Das Zertifkat beinhaltet den Namen der Organisation für die der Zertifkatswerber tätig ist sowie eine E-Mail-Adresse.

Anmerkung: die Identität mit einer bestimmten Person wird dabei nicht garantiert.

3.3.2 Verlängerung der Gültigkeitsdauer des Zertifikats und Neuausstellungen

Eine Verlängerung der Gültigkeitsdauer von a.sign GRZ-IT Zertifikaten ist nicht vorgesehen. Es wird stets ein neues Zertifikat ausgestellt.

3.3.3 Erneuerung des Zertifikates

Ein Zertikatsänderung ist gemäß[RFC3647] möglich und kann im Anlassfall automatisch durch die Registrierungsstelle durchgeführt werden. Ein modiziertes Zertikat ist durch eine abgeänderte Zertikatsseriennummer eindeutig von dem urspünglichen zu unterscheiden und enthält den selben öffentlichen Schlüssel. Eine Modikation darf nur dann durchgeführt werden, wenn keine Kompromittierung des privaten Schlüssel vorliegt.

3.3.4 Erstellung des Zertifikats

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

1. Die a.sign GRZ-IT 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 des Zertifikatsinhabers:
     - Common Name: Vor- und Zuname des SignatorsOder Bezeichnung der rechtsfähigen Einrichtung (juristische Person).
     - Name der Organisation (optional),
     - Name der Organisationsuntereinheit (optional)
     - E-Mailadresse (optional)
     - Nationalität des Zertifizierungsdiensteanbieters (AT)
   - öffentlicher Schlüssel (mit Angabe des Algorithmus)
   - Angabe des Algorithmus für die Signatur des Zertifikats
   - Signatur über das Zertifikat
   - nicht als kritisch gekennzeichnete Zertifikatserweiterungen (optional)

2. Das Zertifikat wird erzeugt, nachdem der Antragsteller die Korrektheit der angezeigten Daten bestätigt hat.

3. Das Schlüsselpaar des a.sign GRZ-IT Zertifikats wird unmittelbar vor Ausstellung des Zertifikats generiert. Die eindeutige Zuordnung zum Zertifikatsinhaber ist durch die Unmittelbarkeit der Abfolge der einzelnen Schritte sicher gestellt.

3.3.5 Bekanntmachung der Vertragsbedingungen

a.trust macht den Zertifikatsinhabern und den Benutzern, die auf die Zuverlässigkeit der a.trust Dienste vertrauen, die Bedingungen, welche die Benutzung des a.sign GRZ-IT Zertifikats betreffen, durch Veröffentlichung der folgenden Dokumente auf der a.trust Homepage (https://www.a-trust.at/docs) zugänglich:

1. der gegenständlichen Certificate Policy,

2. der Allgemeinen Geschäftsbestimmungen von a.trust,

3. sonstigen Mitteilungen.

Änderungen werden dem Zertifikatsinhaber 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.

3.3.6 Veröffentlichung der Zertifikate

Eine Veröffentlichung der Zertifikate in einem öffentlichen Verzeichnis ist nicht vorgesehen.

3.3.7 Widerruf

Der Widerruf ist eine irreversible vorzeitige Beendigung der Gültigkeit eines Zertifikats. Der Widerruf von a.sign GRZ-IT Zertifikaten kann durch den Zertifikatsinhaber beantragt werden und wird nach Bekanntgabe ehebaldigst durchgeführt. Der Zertifikatsinhaber muss durch den Widerrufsdienst eindeutig indentifiziert werden, wobei diese Identifikation keiner besonderen Form bedarf.

Es wird für a.sign GRZ-IT CA-Zertifkate eine eigene Widerrufsliste durch a.trust veröffentlicht. Die Widerrufslisten der a.trust 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.

3.3.8 Sperre

Eine Sperre von a.sign GRZ-IT Zertifikaten ist nicht vorgesehen.

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.
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 ausgelagert. Der Dienstleister 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 Sicherheitsvorkehrungen

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

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 technische Einrichtungen Zertifizierungs- und Widerrufsdienste erbringen, 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 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.
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. Das Personal muss sich vor jedem kritischen Zugriff auf Applikationen, die in Zusammenhang mit dem Zertifikatsmanagement stehen, authentifizieren.
5. Die Zugriffe werden in Log-Dateien aufgezeichnet. Das Personal wird für die ausgeführten Tätigkeiten zur Verantwortung gezogen.
6. Eine Wiederverwendung von Datenspeichern führt nicht zur Offenlegung von vertraulichen Daten an nicht autorisierte Personen.
7. Komponenten des lokalen Netzwerks befinden sich in einer physisch gesicherten Umgebung, die Konfiguration wird periodisch überprüft.
8. 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.
9. Sicherheitskritische Objekte der Verzeichnis- und Widerrufsdienste sind durch eine Signatur der Zertifizierungsstelle gesichert.
10. 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 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,
   - 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. Bei der Einstellung der Tätigkeit werden insbesondere folgende Vorkehrungen getroffen

   - 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 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 GRZ-IT Zertifikaten

Alle Informationen, die in Zusammenhang mit a.sign GRZ-IT 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 GRZ-IT Zertifikaten werden vollständig und vertraulich archiviert.

3. Aufzeichnungen, welche a.sign GRZ-IT Zertifikate betreffen, werden für die Beweisführung der ordnungsgemäßen Zertifizierung im Rahmen gerichtlicher Auseinandersetzungen verfügbar gemacht. Zusätzlich hat der Zertifikatsinhaber 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 GRZ-IT 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 diesem Dokument festgehalten.

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 Zertifikatsinhaber 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 bzw. Sperre 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. a.trust ist eine juristische Person (Gesellschaft mit beschränkter Haftung).

3. a.trust verfügt über Systeme zur Qualitätssicherung und Gewährleistung der Informationssicherheit, die den angebotenen Zertifizierungsdiensten angemessen sind.

4. Hinsichtlich der finanziellen Ausstattung befolgt a.trust die Bestimmungen in § 2 [SigV].

5. 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.

6. 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.

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

8. 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.

A Anhang

A.1 Begriffe und Abkürzungen

a.sign GRZ-IT Zertifikat	Ein nicht qualifiziertes Zertifikat
Certificate Policy, Policy	Ein Regelwerk, das den Einsatzbereich eines Zertifikates für eine bestimmte Benutzergruppe und/oder Anwendungsklasse festhält.
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.
Zertifizierungsdiensteanbieter, Certification Authority, CA	Eine Person oder Stelle, die Zertifikate ausstellt oder anderweitige elektronische Signaturdienste öffentlich anbieten darf.

A.2 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 und BGBl. II Nr. 527/2004 vom 30.12.2004

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

[ETSI] Policy requirements for certification authorities issuing qualified certificates - ETSI TS 101 456

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