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
https://www.a-trust.at

a.trust Anwendungsvorgabe (Certificate Policy) für qualifizierte Zertifikate a.sign premium

Version: 1.3.0
Datum: 28.12.2007

Inhaltsverzeichnis

1 Einführung

1.1 Überblick

Die Anwendungsvorgaben (Certificate Policy) enthalten ein Regelwerk, das den Einsatzbereich eines Zertifikats für eine bestimmte Benutzergruppe und/oder Anwendungsklasse mit gemeinsamen Sicherheitsanforderungen definieren.

Die a.sign Premium Qualified Certificate Policy für qualifizierte Signaturen gilt für qualifizierte Zertifikate entsprechend den Definitionen der EU-Richtlinie [SigRL] und dem österreichischen Bundesgesetz über elektronische Signaturen [SigG], die an Endbenutzer ausgestellt werden, auf sicheren Signaturerstellungseinheiten basieren und für die Erstellung qualifizierten Signaturen geeignet sind.

1.2 Dokumentidentifikation

Name der Richtlinie:	a.trust Anwendungsvorgaben (Certificate Policy) für qualifizierte Zertifikate a.sign premium für qualifizierte Signaturen
Version:	1.3.0 / 28.12.2007
Object Identifier:	1.2.040.0.17 (a.trust) .1 (CP) .11 (a.sign premium) .1.3.0 (Version) vorliegende Version

Der a.trust OID 1.2.040.0.17 ist bei ÖNORM registriert.

Die vorliegende Policy ist in Übereinstimmung mit ETSI TS 101 456 Klasse "QCP public with SSCD" [Object Identifier: 0.4.0.1456.1.1] (siehe [ETSI]) und mit [RFC3647].

1.3 Anwendungsbereich

Die a.sign Premium Anwendungsvorgaben gelten für qualifizierte Zertifikate gem. § 5 [SigG], welche ausschließlich an Endbenutzer ausgestellt werden. Der zertifizierte Signaturschlüssel des Signators darf ausschließlich für das Erstellen von Signaturen genutzt werden.

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

Ausgestellt werden a.sign Premium Zertifikate auf folgende geeignete Chipkarten:

- a.sign Premium e-card

- a.sign Premium Standardkarten, wobei es eine bei a.trust bestellte reine Signaturkarte oder eine signaturfähige Karte mit zusätzlichen Funktionen (z. B. Maestrokarte, Mastercard, Mitgliedsausweis etc.) sein kann.

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

Die Erstellung einer qualifizierten Signatur setzt die Verwendung der von a.trust empfohlenen Komponenten und Verfahren voraus.

Zu diesen empfohlenen Komponenten und Verfahren gehören:

- ein von a.trust empfohlenes Hash-Verfahren,
- die sichere Eingabe der Signatur-PIN auf einem von a.trust empfohlenen Kartenlesegerät mit integriertem numerischem Tastenblock,
- die sichere Anzeige der zu signierenden Daten mittels eines von a.trust empfohlenen Viewers, der gewährleistet, dass ausschließlich die dem Signator dargestellten Daten signiert werden.

Nur mit einem qualifizierten Zertifikat, welches auf der von einer Bestätigungsstelle (z.B. A-SIT) bescheinigten sicheren Signaturerstellungseinheit (a.sign Premium Karte, siehe [A-SIT-Starcos], [A-SIT-ACOS] und [A-SIT-Starcos e-card] basiert, und unter Verwendung von empfohlenen Komponenten und Verfahren kann eine qualifizierte Signatur erstellt werden. Die sichere Überprüfung einer qualifizierten Signatur bedingt ebenfalls die Verwendung von dafür empfohlenen Komponenten und Verfahren.

Dem Signator steht es frei andere technische Komponenten und Verfahren einzusetzen, jedoch muss dies für alle Zertifikatsnutzer zwingend aus den signierten Daten unmittelbar erkennbar hervorgehen.

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 qualifizierte Zertifikate für qualifizierte Signaturen Beachtung fanden.

2 Verpflichtungen und Haftung

2.1 Verpflichtungen des Zertifizierungsdiensteanbieters

a.trust verpflichtet sich das alle Anforderungen dieser Anwendungsvorgabe und der Zertifizierungsrichtlinie erfüllt sind, die sich insbesondere auf die folgenden Aspekte erstrecken:

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

2.2 Verpflichtungen der Zertifikatsinhaber

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

- Die Signatoren verpflichten sich die Allgemeinen Geschäftsbedingungen zusammen mit der a.sign Premium Anwendungsvorgabe (Policy), der Zertifizierungsrichtlinie und den Entgeltbestimmungen von a.trust als Grundlage für den abgeschlossenen Vertrag anzuerkennen.
- Der Signator ist für die Richtigkeit der Angaben verantwortlich, die er bei der Registrierung macht und wirkt gemäß den in der Zertifizierungsrichtlinie angegebenen Verfahren zur Identitätsfeststellung und Authentifikation mit.
- Der Signator ist verpflichtet, seinen privaten Schlüssel angemessen zu schützen. Dies umfasst insbesondere keinen Zugriff durch unautorisierte Personen auf die a.sign Premium Karte zuzulassen und die Aktivierungsdaten (PIN) des privaten Schlüssels geheim zu halten.
- Falls nötig initiiert der Signator unverzüglich die Sperre oder den Widerruf seines Zertifikats. Wird die Sperre nicht nach einem vorgegebenen Zeitraum aufgehoben, so erfolgt automatisch ein Widerruf des Zertifikats.
- Der Signator setzt sein Zertifikat nur zu dem im Zertifikat angegebenen Zweck ein. Maßgeblich hierfür sind die zum Zeitpunkt der Ausstellung des Zertifikats gültige Zertifizierungsrichtlinie und die zugehörigen Anwendungsvorgaben (Policy).
- Der Signator ist grundsätzlich verpflichtet, empfohlene technische Komponenten und Verfahren für die Erstellung der qualifizierten Signatur einzusetzen. Dem Signator steht es frei andere technische Komponenten und Verfahren einzusetzen, jedoch muss dies für alle Zertifikatsnutzer zwingend aus den signierten Daten unmittelbar erkennbar hervorgehen.
- Er muss weiters dafür Sorge tragen, dass auf dem PC-Arbeitsplatz, an welchem die qualifizierte Signatur erstellt wird, kein unbefugt eingebrachter Programmcode zur Anwendung kommt. Dazu soll er die folgenden Vorgaben von a.trust einhalten:
  - Der Signator muss alle notwendigen technischen und organisatorischen Maßnahmen ergreifen, um unbefugten Zugriff auf seinen PC-Arbeitsplatz und die darauf befindlichen Programmcodes zu verhindern.
  - a.trust verpflichtet den Signator sich an die Empfehlungen des Herstellers des von ihm verwendeten Betriebssystems sowie an die Empfehlungen der Hersteller der anderen Software-Produkte, die er installiert hat, zu halten.
- er Signator ist verpflichtet die jeweiligen nationalen Ausfuhrbestimmungen sowie etwaige nationale Nutzungsbeschränkungen bei einer Verwendung im Ausland zu beachten.

2.3 Verpflichtungen der Zertifikatsnutzer

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

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

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

2.4 Haftung

a.trust haftet als Aussteller von qualifizierten Zertifikaten gem. den Bestimmungen in § 23 [SigG].

3 Anforderung an die Erbringung von Zertifizierungsdiensten

Diese Policy ist auf die Erbringung von qualifizierten Zertifizierungsdiensten ausgerichtet. Dies umfasst die Bereitstellung von Registrierungsdiensten, Zertifikatsgenerierung, Zertifikatsausgabe, Sperr- und Widerrufsdiensten und Abfragediensten über den Zertifikatsstatus.

3.1 Zertifizierungsrichtlinie (CPS)

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

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

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

3. Die Zertifizierungsrichtlinie für a.sign Premium (siehe [CPS]) benennt die Verpflichtungen aller externen Vertragspartner, die Dienstleistungen für a.trust unter Beachtung der jeweils anwendbaren Policies und Richtlinien erbringen.

4. a.trust macht allen Signatoren und Überprüfern von elektronischen Signaturen die Zertifizierungsrichtlinie und jegliche Dokumentation, die die Übereinstimmung mit dieser Anwendungsvorgabe dokumentiert, zugänglich (siehe Kapitel 3.3.4).

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

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

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

8. a.trust wird zeitgerecht über beabsichtigte Änderungen informieren, die in der Zertifizierungsrichtlinie vorgenommen werden sollen, und wird nach Genehmigung derselben entsprechend Punkt 5 dieses Absatzes eine überarbeitete Version der Zertifizierungsrichtlinie für a.sign Premium entsprechend Kapitel 3.3.4 unverzüglich zugänglich machen.

3.2 Verwaltung der Schlüssel zur Erbringung von Zertifizierungsdiensten

3.2.1 Erzeugung der a.trust 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 (g) und Annex II (f):

1. Die Erzeugung der Schlüssel wird von dazu autorisiertem Personal (siehe Rollenmodell in 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 für qualifizierte Zertifikate als geeignet angesehen wird.
4. Die Schlüssellänge und der Algorithmus sind 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 in Übereinstimmung mit den Bestimmungen aus § 10 [SigV] sicher, dass die privaten Schlüssel geheim gehalten werden und ihre Integrität bewahrt bleibt.

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

Es sind Maßnahmen getroffen worden, die garantieren, dass die privaten 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:

- Ausstellung und Veröffentlichung eines durch die Aufsichtsstelle signierten Zertifikates und durch

- Ausstellung und Veröffentlichung eines selbstsignierten Root-Zertifikates.

Das Zertifikat des CA Schlüssels zur Signatur von a.sign Premium 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 premium 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 premium 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 Signatoren

Die Schlüssel werden im Hochsicherheitsbereich des Kartenherstellers in den a.sign Premium Karten erzeugt, auf welche anschließend die persönlichen Daten des Signators aufgebracht werden. Ein Zertikat für das Signaturschlüsselpaar wird noch nicht erstellt. Dies geschieht erst im Zuge des Registrierungsprozesses, indem der Signator zuverlässig identiziert und authentiziert wird.

3.2.8 Sicherheit der a.sign Premium Karte

Die Schlüssel der Signatoren werden auf einer den Anforderungen entsprechenden Chipkarte, der a.sign Premium Karte, gespeichert. Es handelt sich bei der a.sign Premium Karte um eine von einer Bestätigungsstelle (wie z.B. ASIT) nach § 18(5) [SigG] bescheinigte Smartcard, welche eine sichere Signaturerstellungseinheit darstellt und die Erzeugung und Speicherung der Signaturerstellungsdaten ermöglicht ([A-SIT-Starcos], [A-SIT-Starcos e-card], [A-SIT-ACOS]). Auf den von a.trust als a.sign Premium Karten

eingesetzten Smartcards mit zertifiziertem Chip ist sicher gestellt, dass es durch andere auf der Karte befindliche Applikationen zu keiner Beeinflussung der Signaturfunktion kommen kann.

3.3 Lebenszyklus des Zertifikats

3.3.1 Registrierung des Signators

Die Maßnahmen zur Identifikation und Registrierung des Signators entsprechen den Anforderungen gem. § 11 [SigV] und stellen sicher, dass der Antrag auf Ausstellung eines qualifizierten Zertifikats korrekt, vollständig und autorisiert ist. Die Maßnahmen entsprechen damit auch [SigRL] Annex II (d).

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

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

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

- ein in Österreich ausgestellter amtlicher Lichtbildausweis (eine Liste der in Österreich gültigen amtlichen Lichtbildausweise, die von a.trust akzeptiert werden, ist auf der Homepage der a.trust zu finden) oder
- ein international gültiger Reisepass in deutscher und/oder englischer Sprache.

Weiters steht die Möglichkeit zur Verfügung, dass mittels eines RSa Briefs (SigV §§11) ein für die Ausstellung der Zertifikate notwendiger Aktivierungscode an die Meldeadresse des Kartenbesitzers versendet wird. Im Rahmen der Zustellung des RSa Briefs ist es notwendig, dass der Antragssteller seine Identität durch das Vorlegen eines gültigen, amtlichen Lichtbildausweises beweist.

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

3.3.2 Erneute Registrierung/Rezertifizierung

Der Signator kann nach einem Widerruf eine Ersatzkarte bestellen bzw. Zertifikate zu einer Karte aktivieren oder auch eine zusätzliche Karte bestellen bzw. aktivieren. Der Vorgang verläuft analog zur Erstregistrierung. Dabei sind allfällige Änderungen in den personenbezogenen Daten anzugeben.

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

3.3.3 Ausstellung von Zertifikaten

Die mit den Schlüsseln versehene a.sign Premium Karte wird entweder an die zuständige Registrierungsstelle weitergeleitet und der Signator nimmt sie dort entgegen oder der Signator ist bereits im Besitz einer signaturfähigen Karte.

Persönliche Ausstellung:

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

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

Online-Austellung:

Im Zuge der Online-Austellung ist es für den Signator notwendig die Identität mittels des Aktivierungscodes (mittels RSa Brief an den Signator übermittelt) und des beim Antrag selbstgewählten Widerrufspassworts zu bestätigen. Die Webanwendung unterbindet die Eingabe von Personendaten. Es wird ausschließlich auf bereits verifizierte Personendaten zur Ausstellung des Zertifikats zurück gegriffen, die von der Karten ausgebenden Stelle an die a.trust zur Verwendung frei gegeben und übermittelt werden.

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

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

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

1. Die Zertifikate werden gem. den Bestimmungen in Anhang 2 [SigV] als X.509 v3 Zertifikate unter Beachtung der Anforderungen von Annex I [SigRL] 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.:
     - Bezeichnung als qualifiziertes Zertifikat
     - Informationen über die anzuwendende Policy bzw. CPS
     - Zertifikatsverwendung
     - Information zum Auffinden der CRL
     - Geburtsdatum des Zertifikatsinhabers (optional)
     - Optionales Behördenkennzeichen und ggf. ein optionaler Verwaltungsbezeichner.

2. Das Zertifikat wird bei der Registrierung auf Veranlassung der Registrierungsstelle erzeugt, nachdem der Antragsteller identifiziert und die Korrektheit aller Daten durch ihn bestätigt wurde. Das Verfahren ist für Verlängerung und Neuausstellung identisch.

3. Das Signatur-Schlüsselpaar der a.sign Premium Karte wurde anlässlich der Initialisierung der Karte erstellt.

4. Für alle a.sign Premium Karten gilt:

   - Jedem Signator wird eine innerhalb der a.trust einmalig vergebene und eindeutige Identifikationsnummer (CIN) zugeordnet. Diese Identifikationsnummer ist Teil des hervorgehobenen Namens und stellt damit seine Eindeutigkeit sicher.
   - Die in der Registrierungsstelle aufgenommenen Daten werden signiert und verschlüsselt (SSL) an die Zertifizierungsstelle übertragen. Vertraulichkeit und Integrität sämtlicher Daten ist damit sicher gestellt.
   - 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 Überprüfern von Signaturen die Bedingungen betreffend die Benutzung des qualifizierten Zertifikats durch Veröffentlichung der nachfolgenden Dokumente auf der a.trust-Homepage zugänglich:

- der gegenständlichen Anwendungsvorgabe (Certificate Policy),
- des Zertifizierungsrichtlinie für a.sign Premium, siehe [CPS],
- der Allgemeinen Geschäftsbestimmungen von a.trust,
- der Belehrungen für den Signator,
- der sonstigen Mitteilungen.

Änderungen werden dem Signator mittels Bekanntmachung auf der a.trust-Homepage und gegebenenfalls per Mail oder Brief mittgeteilt.

3.3.5 Veröffentlichung der Zertifikate

Von a.trust ausgestellte Zertifikate werden den Signatoren und, je nach Vereinbarung mit dem Signator, den Überpüfern folgendermaßen verfügbar gemacht.

- Anlässlich der Erstellung eines Zertifikats wird dieses am Ende des Registrierungsvorgangs auf die a.sign Premium Karte des Signators gespeichert.
- Wenn der Signator damit einverstanden ist, wird das Zertifikat im Verzeichnisdienst von a.trust veröffentlicht.
- Die Bedingungen für die Benutzung eines Zertifikats werden von a.trust allen Beteiligten zur Kenntnis gebracht (siehe Kapitel 3.3.4).
- Die Identifikation der anzuwendenden Bestimmungen ist durch die eindeutige Zuordnung zum Produktnamen "a.sign Premium" einfach herstellbar.
- Der Verzeichnisdienst ist 7 Tage 24 Stunden verfügbar. Unterbrechungen von mehr als 30 Minuten werden gemäß § 13 Abs 5 [SigV] als Störfälle dokumentiert.
- Die Verzeichnisdienste sind öffentlich und international zugänglich.

3.3.6 Sperre und Widerruf

a.sign Premium Zertifikate können vorübergehend gesperrt werden. Diese Sperre kann auch in einen endgültigen Widerruf umgewandelt werden. Ebenso ist ein sofortiger und permanenter Widerruf des Zertifikats möglich. Der Signator wird von einer erfolgten Sperre oder einem Widerruf informiert, sofern a.trust Kontaktinformationen (Adresse, email, ...) bekanntgeben wurden.

Die Vorgangsweisen für das Auslösen von Sperre und Widerruf sind in der Zertifizierungsrichtlinie für a.sign Premium (siehe [CPS]) dokumentiert, insbesondere:

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

Eine Sperre oder ein Widerruf kann durch den Signator vorgenommen werden. Dies kann wie folgt geschehen:

- Der Signator wendet sich per Telefon an den Widerrufsdienst.
- Der Signator bzw. der Vertretungsbefugte veranlasst den Widerruf per Fax.

- Bei Vergessen des Passworts für den Widerruf kann der Signator keinen Widerruf, sondern nur eine Sperre beantragen.

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

- Telefonat: Der Signator kann rund um die Uhr einen Widerruf per Telefon vornehmen. Die Authentikation erfolgt nur über das Sperr- und Widerruf-Passwort, welches der Antragsteller bei der Bestellung bzw. Registrierung selbst festgelegt hat.
  Die für einen Widerruf benötigten Informationen lassen sich wie folgt zusammenfassen:
  - Persönliche Daten (vollständiger Name, Geburtstag und -ort),
  - Passwort für den Widerruf,
  - Identifikationsnummer des Signators (CIN), Kartennummer oder Seriennummer des Zertifikats.
- Fax: Der Signator kann von 0 bis 24 Uhr einen Widerruf per Fax vornehmen. Das Fax muss das Sperr- und Widerrufs-Passwort sowie die vollständige Seriennummer oder die Kartennummer des zu widerrufenden Zertifikats beinhalten.
- Fax: Der Vertretungsbefugte bzw. eine bevollmächtigte Person kann von 0 bis 24 Uhr einen Widerruf per Fax vornehmen. Das Fax muss einen Hinweis auf seine Vertretungsbefugnis sowie die vollständige Seriennummer oder die Kartennummer des zu widerrufenden Zertifikats beinhalten.
- Besuch in einer Registrierungsstelle: Der Signator benötigt dazu einen gültigen, amtlichen Lichtbildausweis. Der RO teilt dem Signator die Zertifikatsnummer und das Passwort für den Widerruf mit, womit der Signator anschließend den Widerruf beim Widerrufsdienst veranlassen kann.

Gesperrte und widerrufene Zertifikate werden in einer Widerrufsliste (CRL) unter Berücksichtigung der nachfolgenden Regelungen veröffentlicht:

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

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

- Versionsnummer der CRL: Version 2 (codiert mit dem Wert 1)
- Bezeichnung des Ausstellers
- Zeitpunkt der CRL-Ausstellung sowie der nächsten geplanten Ausstellung
- Information über die in der CRL enthaltenen Zertifikate:
  - Seriennummer,
  - Zeitpunkt der Eintragung in die CRL,
  - Eintragungsgrund
- CRL-Erweiterungen
- Angabe des Algorithmus für die Signatur über die CRL
- Signatur über die CRL.

Die Widerrufsdienste sind entsprechend § 13 Abs 5 [SigV] täglich 24 Stunden verfügbar. Spätestens innerhalb von drei Stunden ab Bekanntwerden des Widerrufsgrundes erfolgt eine Aktualisierung der Widerrufsliste. Widerrufslisten sind täglich 24 Stunden abfragbar. Im Fall von Systemausfällen kommen die in der Zertifizierungsrichtlinie für a.sign Premium (siehe [CPS]) genannten Vorkehrungen zum Tragen, um die Auswirkungen möglichst gering zu halten. Statusinformationen über Zertifikate können auch online mittels OCSP abgefragt werden. Die Integrität und Authentizität der OCSP-Antworten sind durch eine Signatur gesichert.

3.4 a.trust Verwaltung

3.4.1 Sicherheitsmanagement

Es gelten folgenden Bestimmungen:

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

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

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

3.4.3 Personelle Sicherheitsmaßnahmen

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

- a.trust beschäftigt ausschließlich Personal, welches über das gem. § 10 Abs 5 [SigV] 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 sowohl der administrativen als auch der Managementfunktionen 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 verfügen, das Verantwortung für sicherheitskritische Tätigkeiten trägt.

- Alle Mitarbeiter, denen vertrauenswürdige Positionen zugeordnet sind, werden von Interessenskonflikten, die einer unvoreingenommenen Erfüllung der Aufgaben entgegenstehen könnten, frei gehalten.
- Alle vertrauenswürdigen Positionen sind im Zertifizierungsrichtlinie (siehe [CPS]) im Detail beschrieben.
- Die Zuweisung der Positionen erfolgt mit formeller Ernennung durch die Geschäftsführung.
- Entsprechend § 10 Abs 4 [SigV] beschäftigt a.trust keine Personen, die strafbare Handlungen begangen haben, die sie für eine vertrauenswürdige Position ungeeignet erscheinen lassen. Eine Beschäftigung erfolgt erst nach einer diesbezüglichen Überprüfung.

3.4.4 Physikalische und organisatorische Sicherheitsmaßnahmen

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

- Der Zutritt zu den Räumlichkeiten, in denen Zertifizierungs- und Widerrufsdienste erbracht und in denen die a.sign Premium Karten initialisiert werden, ist auf autorisiertes Personal beschränkt. Die Systeme, die 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 datenverarbeitenden Anlagen nicht möglich ist.
- Die Systeme für Zertifikatsgenerierung, die Kartenbereitstellung und die Widerrufsdienste werden in einer gesicherten Umgebung betrieben, sodass eine Kompromittierung durch unautorisierte Zugriffe nicht möglich ist.
- Die Abgrenzung der Systeme für Zertifikatsgenerierung, Kartenbereitstellung und Widerrufsdienste erfolgt durch klar definierte Sicherheitszonen d.h. durch räumliche Trennung von anderen organisatorischen Einheiten und 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, Kartenproduktion und Bereitstellung der Widerrufsdienste umfasst physische Zutrittskontrolle, Abwendung von Gefahren durch Naturgewalten, Feuer, Rohrbrüche und Gebäudeeinstürze, Schutz vor Ausfall von Versorgungseinheiten, 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.
- Datenträger werden je nach ihrer Sicherheitsstufe (siehe Kapitel 3.4.2) behandelt und aufbewahrt. Nicht mehr benötigte Datenträger, die vertrauliche Daten beinhalten, werden in sicherer Weise vernichtet.
- Kapazitätserfordernisse werden beobachtet und künftige Entwicklungen prognostiziert, sodass stets die angemessene Prozessorleistung und Speicherplatz zur Verfügung stehen.
- Auf Zwischenfälle wird so rasch wie möglich reagiert, um die sicherheitskritischen 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:

- Operationale 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 operativem Personal (unter Beaufsichtigung) gem. Sicherheitskonzept und Stellenbeschreibungen durchgeführt werden.

3.4.6 Zugriffsverwaltung

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

- Sicherungsmaßnahmen wie z.B. Firewalls bewahren das interne Netzwerk vor Zugriffen durch Dritte.
- Vertrauliche Daten werden geschützt, wenn sie über unsichere Netzwerke ausgetauscht werden, wie z.B. die Registrierungsdaten.
- 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.
- Zugriff auf Informationen und Anwendungen ist auf Grund der vergebenen Zugriffsrechte eingeschränkt. Die dafür geltenden Definitionen sind im Zertifizierungsrichtlinie für a.sign Premium (siehe [CPS]) angeführt. Administrative und den laufenden Betrieb betreffende Funktionen sind streng getrennt. Die Verwendung von System-Utility-Programmen ist besonders eingeschränkt.
- Das Personal muss sich vor jedem kritischen Zugriff auf Applikationen, die in Zusammenhang mit dem Zertifikatsmanagement stehen, authentifizieren.
- Die Zugriffe werden in Log-Dateien aufgezeichnet. Das Personal wird für die ausgeführten Tätigkeiten zur Verantwortung gezogen.
- Eine Wiederverwendung von Datenspeichern führt nicht zur Offenlegung von vertraulichen Daten an nicht autorisierte Personen.
- Komponenten des lokalen Netzwerks befinden sich in einer physisch gesicherten Umgebung und die Konfiguration wird periodisch überprüft.

- Die Entdeckung von unautorisierten und/oder außergewöhnlichen Zugriffsversuchen auf die eigentliche Zertifizierungsstelle und die Widerrufsdienste wird durch geeignete Maßnahmen gesichert, sodass ggf. sofort Gegenmaßnahmen ergriffen werden können. Dies geschieht durch die Führung und Auswertung von CA-Logfiles und Firewall-Logfiles.
- Ändernde Zugriffe (Löschungen, Hinzufügungen) auf die Verzeichnis- und Widerrufsdienste werden durch Passworteingabe abgesichert.
- 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.

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

3.4.8 Erhaltung des ungestörten Betriebes und Behandlung von Zwischenfällen

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

- Der Notfallsplan von a.trust sieht die (vermutete) Kompromittierung des privaten Zertifizierungsschlüssels als Katastrophenfall vor.
- Sollte dieser Fall eintreten, so hat a.trust die Aufsichtsstelle (siehe § 6 Abs 5 [SigG]), die Signatoren, die auf die Sicherheit der Zertifizierungsdienste vertrauenden Personen und ggf. andere Zertifizierungsdiensteanbieter, mit denen Vereinbarungen bestehen, davon zu unterrichten und mitzuteilen, dass die Widerrufs- und Zertifikatsinformationen nicht mehr als zuverlässig anzusehen sind.
- 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 Auf-sichtsstelle anzeigen und sicher stellen, dass eine eventuelle Beeinträchtigung der Dienstleistung gegenüber Signatoren und vertrauenden Parteien möglichst gering gehalten wird.

1. Vor Beendigung der Dienstleistung werden
   - alle Signatoren, Zertifizierungsdiensteanbieter und sonstige Parteien, mit denen a.trust eine geschäftliche Verbindung unterhält, direkt, sowie jene Parteien, die auf die Zuverlässigkeit der Zertifizierungsdienste vertrauen, durch Veröffentlichung von der Einstellung unterrichtet,
   - die Verträge mit Subunternehmern (Registrierungsstellen, Kartenhersteller 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 Abschnitt 3.2.6 zerstört.
2. Die Abdeckung der Kosten für o.a. Vorkehrungen sind durch Gesellschaftergarantien abgedeckt.
3. Das Zertifizierungsrichtlinie von a.trust (siehe [CPS]) benennt die Vorkehrungen, die bei Einstellung der Tätigkeit getroffen werden, insbesondere jene Vorkehrungen
   - für die Benachrichtigung der betroffenen Personen und Organisationen,
   - für die Übertragung der Verpflichtungen auf Drittparteien und
   - wie der Widerrufsstatus von nicht abgelaufenen Zertifikaten gehandhabt wird.

3.4.10 Übereinstimmung mit gesetzlichen Regelungen

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

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

- 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 qualifizierten Zertifikaten

Alle Informationen, die in Zusammenhang mit qualifizierten Zertifikaten stehen, werden entsprechend [SigV] aufbewahrt. Insbesondere gilt:

1. Die Vertraulichkeit und Integrität der aktuellen sowie der archivierten Datensätze ist gewahrt.
2. Die Datensätze zu qualifizierten Zertifikaten werden vollständig und vertraulich in Übereinstimmung mit der veröffentlichten Zertifizierungsrichtlinie (siehe [CPS]) archiviert.
3. Aufzeichnungen bezüglich qualifizierter Zertifikate 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 Zertifikatsmanagement stehen.
5. Alle Datensätze, die in Zusammenhang mit qualifizierten Zertifikaten stehen, werden entsprechend § 16 (2) [SigV] für 35 Jahre elektronisch aufbewahrt. Das Antragsformular (Signaturvertrag) wird für drei Jahre in der betreffenden Registrierungsstelle im Original aufbewahrt.
6. Alle Aufzeichnung erfolgen derart, dass sie innerhalb der Aufbewahrungsfrist nicht leicht gelöscht oder zerstört werden können.
7. Die spezifischen Ereignisse und Daten die aufgezeichnet werden, sind in der Zertifizierungsrichtlinie (siehe [CPS]) dokumentiert.
8. Insbesondere werden alle Registrierungsinformationen, inkl. jener, die im Zusammenhang mit der Verlängerung der Gültigkeitsdauer von Zertifikaten stehen, elektronisch aufbewahrt.
9. Die aufzuzeichnenden Registrierungsinformationen beinhalten insbesondere:
   - die Art des Identifikationsdokuments, das anlässlich der Registrierung vorgelegt wurde,
   - die Daten des Identifikationsdokuments,

- die Aufbewahrungsstelle der elektronischen Kopien der Antragsdokumente inklusive der Archivierung der Ausweisdaten,
- die Akzeptanz der vertraglichen Vereinbarungen
- vom Signator gewählte und akzeptierte Zertifikatsinhalte,
- Angabe der Registrierungsstelle und des zuständigen Mitarbeiters.

10. Die Vertraulichkeit der Daten der Signatoren ist gewährleistet.
11. Es werden alle Ereignisse, die den Lebenszyklus der CA-Schlüssel von a.trust betreffen, aufgezeichnet.
12. Es werden alle Ereignisse, die den Lebenszyklus der Zertifikate betreffen, aufgezeichnet.
13. Es werden alle Ereignisse, die im Zusammenhang mit der Generierung der Schlüssel der Signatoren stehen, aufgezeichnet.
14. Es werden alle Ereignisse, die im Zusammenhang mit der Initialisierung und Personalisierung der a.sign Premium Karte stehen aufgezeichnet.
15. Alle Anträge auf Sperren, Sperraufhebung und Widerruf und die damit verbundenen Informationen werden aufgezeichnet. Dies inkludiert die Bandaufzeichnung der Telefonate und die Archivierung von Anträgen per Fax (siehe Kapitel 3.3.6).

3.5 Organisatorisches

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

3.5.1 Allgemeines

- Alle Richtlinien und Vorgehensweisen sind nicht-diskriminierend.
- Die Dienstleistungen von a.trust stehen allen Personen zur Verfügung, die über einen in Österreich ausgestellten amtlichen Lichtbildausweis (die zulässigen Lichtbildausweise sind auf der a.trust Homepage aufgezählt) oder einen international gültigen Reisepass in deutscher und/oder englischer Sprache verfügen.
- a.trust ist eine juristische Person (Gesellschaft mit beschränkter Haftung).
- a.trust verfügt über Systeme zur Qualitätssicherung und Gewährleistung der Informationssicherheit, die den angebotenen Zertifizierungsdiensten angemessen sind.
- Die Haftung, insbesondere diejenige zur Schadenswiedergutmachung, entspricht den Bestimmungen des [SigG] (siehe Kapitel 2.4).

- Hinsichtlich der finanziellen Ausstattung befolgt a.trust die Bestimmungen in § 2 [SigG].
- 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.
- Es sind Richtlinien und Vorgehensweisen für die Behandlung von Beschwerden und Streitfällen vorhanden, die von Kunden oder anderen Parteien an die a.trust herangetragen werden und die Erbringung ihrer Dienstleistungen betreffen.
- Die rechtlichen Beziehungen zu Subunternehmern, die Dienstleistungen für a.trust erbringen, sind vertraglich geregelt und ordnungsgemäß dokumentiert.
- 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 der a.trust unabhängig von anderen Gesellschaften. Die Geschäftsführung und das Personal, das vertrauliche und leitende Funktionen ausübt, sind frei von kommerziellem, finanziellem und sonstigem Druck, der das Vertrauen in ihre Tätigkeit negativ beeinflussen könnte.

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

A Anhang

A.1 Begriffe und Abkürzungen

a.sign Premium Karte	Eine Prozessorchipkarte, die geheime Schlüssel des Karteninhabers enthält und zur Erstellung und Verifizierung digitaler Signaturen dient.
Aktivierungsdaten	Daten, die zur Aktivierung der Schlüssel benötigt werden (PIN).
Anwender	Person, die die Dienstleistungen der Zertifizierungsstelle der a.trust nutzt. Anwender sind sowohl Zertifikatsinhaber als auch Zertifikatsnutzer.
Audit	Von externen Personen durchgeführte Sicherheitsüberprüfung.
CA (Certification Authority), Zertifizierungsdiensteanbieter	Eine Person oder Stelle, die Zertifikate ausstellt oder anderweitige elektronische Signaturdienste öffentlich anbieten darf.
CA-Schlüssel	Schlüssel der CA, die zur Ausstellung von Zertifikaten und dem Unterschreiben von Widerrufslisten (Zertifizierung) verwendet werden.
CA-Zertifikat, Zertifizierungsstellenzertifikat	Zertifikat der Zertifizierungsstelle, das zur Signatur der Zertifikate der Signatoren und der zugehörigen CRLs dient
Certification Policy, Policy	Ein Regelwerk, das den Einsatzbereich eines Zertifikates für eine bestimmte Benutzergruppe und/oder Anwendungsklasse festhält.
Certification Practice Statement, CPS, Zertifizierungsrichtlinie	Aussagen über die bei der Ausstellung von Zertifikaten von einem Zertifizierungsdiensteanbieter eingehaltenen Vorgehensweise
Dienste (CA-Dienste)	Überbegriff für angebotene Dienstleistungen wie Verzeichnisdienst, Statusauskunft und Zeitstempeldienst
Dienste-Schlüssel	Schlüssel eines Dienstes (z. B. Signaturschlüssel zur Signatur von Statusauskünften)
Digitale Signatur	Elektronische Signatur, die mit Hilfe von Verfahren der asymmetrischen Kryptographie erzeugt wird.
E-Mail	Electronic Mail; Nachrichten, die in digitaler Form über computerbasierte Kommunikationswege versandt oder empfangen werden.

Elektronische Signatur	Eine Signatur in digitaler Form, die in Daten enthalten ist, Daten beigefügt wird oder logisch mit ihnen verknüpft ist und von einem Unterzeichner verwendet wird, um zu bestätigen, dass er den Inhalt dieser Daten billigt. Sie ist so mit den Daten verknüpft, dass eine nachträgliche Veränderung der Daten offenkundig wird.
Gültigkeitsmodell	Modell, nach dem die Prüfung der Gültigkeit von Zertifikaten und Signaturen vorgenommen wird.
Hardware Security Modul, HSM	Elektronisches System zur sicheren Speicherung von Schlüsseln und zur Berechnung und Verifizierung von Signaturen.
Integrität (von Daten)	Ein Zustand, in dem Daten weder von Unbefugten verändert noch zerstört wurden.
Kettenmodell	Gültigkeitsmodell, nach dem eine gültige Anwendung des Schlüssels dann erfolgt, wenn zum Zeitpunkt der Anwendung das Zertifikat gültig ist und das übergeordnete Zertifikat zum Zeitpunkt der Erstellung des eingesetzten Zertifikats gültig war.
Kompromittierung	Eine unautorisierte Offenlegung von oder der Verlust der Kontrolle über sicherheitskritische Informationen und geheim zuhaltende Daten.
LDAP	Lightweight Directory Access Protocol ist ein Standard protokoll für Verzeichnisdienste (LDAP Server) im Internet.
OCSP	Online Certificate Status Protocol, Protokoll für die Statusauskunft
OID	Object Identifier, eine Ganzzahl, durch die ein Objekt (z.B. Policy) eindeutig identifiziert wird.
Öffentlicher Schlüssel	Öffentlicher Teil eines Schlüsselpaares. Er ist Bestandteil eines Zertifikates und wird zur Überprüfung von Digitalen Signaturen bzw. zur Verschlüsselung von Nachrichten/Daten verwendet.
PIN	Personal Identification Number (Aktivierungsdaten)
Privater Schlüssel, geheimer Schlüssel	Geheimer Teil eines Schlüsselpaares, der zum digitalen Signieren sowie zum Entschlüsseln von Nachrichten/Dokumenten erforderlich ist und geheim gehalten werden muss.

Public-Key Infrastructure, PKI	Ein kryptografisches System, das ein Paar von durch einen mathematischen Algorithmus verbundenen Schlüsseln benutzt. Der öffentliche Teil dieses Schlüsselpaars kann jedermann zugänglich gemacht werden, der Informationen verschlüsseln oder eine digitale Signatur prüfen will, der geheime (private) Teil wird von seinem Besitzer sicher bewahrt und kann Daten entschlüsseln oder eine digitale Signatur erstellen.
Qualifiziertes Zertifikat	Zertifikat, welches den Bestimmungen des § 5 des Österr. Signaturgesetzes entspricht.
Registrierungsstelle, Registration Authority, RA	Eine vertrauenswürdige Einrichtung, welche die Überprüfung der Identität der Zertifikatsbewerber im Namen des Zertifizierungsdiensteanbieters unter Berücksichtigung der Zertifizierungsrichtlinien durchführt und selbst keine Zertifikate ausstellt.
RFC	Request for Comments, Artikel über Standards und Protokolle im Internet. Neue Standards werden zunächst vorgeschlagen und zur Diskussion gestellt (daher "mit der Bitte um Stellungnahme"). Erst nachdem sie ausdiskutiert und für gut befunden worden sind, werden sie unter einer RFC-Nummer veröffentlicht.
Root-CA, Root-Zertifizierungsstelle	Die Root-CA ist die oberste CA in der Zertifizierungshierarchie der a.trust. Sie stellt die Zertifikate für die nachgeordneten CAs aus.
Root-Zertifikat, Stammzertifikat, Root-CA Zertifikat	Zertifikat des Root-Keys, der zur Signatur der Zertifikate der Zertifizierungsstellen und der zugehörigen CRLs dient
RSA	Signatur- und Verschlüsselungsverfahren; benannt nach Rivest, Shamir und Adleman
Schlüsselpaar	Ein privater Schlüssel und der dazugehörige öffentliche Schlüssel. Abhängig vom verwendeten Algorithmus kann man mit Hilfe des öffentlichen Schlüssels eine digitale Unterschrift, die mit dem dazu gehörigen privaten Schlüssel erstellt wurde, verifizieren bzw. mit dem privaten Schlüssel Daten entschlüsseln, welche mit dem zugehörigen öffentlichen Schlüssel verschlüsselt wurden.
Signator	Eine Person, die eine elektronische Signatur erstellt, Zertifikatsinhaber
Signaturerstellungsdaten	Signaturerstellungsdaten sind einmalige Daten wie Codes oder private Signaturschlüssel, die von dem Signator zur Erstellung einer elektronischen Signatur verwendet werden.

Signaturprüfdaten	Signaturprüfdaten sind Daten wie Codes oder öffentliche Signaturschlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden.
Sperre	Eine Sperre ist ein zeitlich begrenztes vorübergehendes Aussetzen der Gültigkeit eines Zertifikats der a.sign Premium Karte.
Statusauskunft	Dienst, bei dem die Anwender Auskunft über den aktuellen Status (gültig oder gesperrt) eines Zertifikates abrufen können.
URI	Uniform Resource Identifier, spezifiziert eine bestimmte Datei auf einem bestimmten Server, Oberbegriff für URL (Uniform Resource Locator) und URN (Universal Resource Name).
Verifizierung (einer digitalen Signatur)	Feststellung, dass eine digitale Signatur mit dem privaten Schlüssel, der zu dem in einem gültigen Zertifikat beinhalteten öffentlichen Schlüssel gehört, erstellt wurde und die Nachricht sich nach der Signatur nicht verändert hat.
Verzeichnis (-dienst)	Dienst, bei dem die Anwender Zertifikate der CA oder anderer Anwender sowie CRLs abrufen können. Der Zugriff wird über LDAP realisiert.
Widerruf	Der irreversible Vorgang der vorzeitigen Beendigung der Gültigkeit eines Zertifikats ab einem bestimmten Zeitpunkt.
X.509	Der ITU-Standard für Zertifikate. X.509 v3 beschreibt Zertifikate, die mit verschiedenen Zertifikatserweiterungen erstellt werden können
Zeitstempel	Digitale Signatur von digitalen Daten und einem Zeitpunkt. Mit Hilfe eines Zeitstempels kann nachgewiesen werden, dass digitale Dokumente zu einem bestimmten Zeitpunkt existiert haben. Um Manipulationen zu verhindern, soll der Zeitstempel nur von einer vertrauenswürdigen Instanz (z.B. Zertifizierungsstelle) ausgestellt werden.
Zertifikatsinhaber	Anwender, dessen Schlüssel und persönliche Daten im Zertifikat der a.trust festgehalten sind, auch Signator genannt.
Zertifikatsnutzer, Signaturempfänger	Anwender, der Zertifikate über die Schlüssel und Daten anderer nutzt, um Signaturen zu prüfen.
Zertifikats-Widerrufsliste, CRL	Eine digital signierte Datenstruktur, die widerrufene und gesperrte Zertifikate anführt, welche von einem bestimmten Zertifizierungsdiensteanbieter ausgestellt wurden.

A.2 Referenzdokumente

[CPS] a.trust Zertifizierungsrichtlinie für qualifizierte a.sign Premium Zertifikate für sichere Signaturen, in der jeweils aktuellen Version.

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

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

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

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

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

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

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

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

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

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

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

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

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

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