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

a.trust

Certificate Policy für qualifizierte a.sign Premium Zertifikate für sichere Signaturen

Version: 1.2.1

Datum: 09.12.2004

Inhaltsverzeichnis

1 Einführung

1.1 Überblick

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

Die a.sign Premium Qualified Certificate Policy für sichere 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 sicherer digitaler Signaturen geeignet sind.

1.2 Identifikation

Name der Policy:	a.trust Certificate Policy für qualifizierte a.sign Premium Zertifikate für sichere Signaturen
Version:	1.2.1/09.12.2004
Object Identifier:	**1.2.040.0.17** (a.trust)**.1** (Policy)**.11** (a.sign Premium)**.1.2.1** (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 Qualified Certificate Policy gilt für qualifizierte Zertifikate gem. § 5 [SigG], welche ausschließlich an Endbenutzer ausgestellt werden. Die geheimen Schlüssel der Signatoren befinden sich auf sicheren Signaturerstellungseinheiten, den a.sign Premium Karten, die von a.trust an zwei Signatorengruppen ausgestellt werden:

1. an Mitarbeiter und Studierende der Wirtschaftsuniversität Wien („WU-Karte“) und

2. andere Signatoren (a.sign Premium Standardkarten), wobei es eine bei a.trust bestellte reine Signaturkarte oder eine signaturfähige Karte mit zusätzlichen Funktionen (z. B. Maestrokarte, Mitgliedsausweis etc.) sein kann. Aufgrund des verwendeten Betriebssystems der Smartcard sind zwei Ausprägungen möglich, die wie folgt unterschieden werden:

   - a.sign Premium „Standardkarten Variante 1“
     diese Karten sind dadurch erkennbar und von den anderen unterscheidbar, dass sie durch die a.sign Client Software ((diese Software ist Produktbestandteil) als „a sign premium a“ angezeigt werden und ggf. auf der Kartenoberfläche einen Bindestrich „-“ zwischen CIN und CSN aufweisen,

   - a.sign Premium „Standardkarten Variante 2“.

Sichere elektronische Signaturen, die auf Basis eines qualifizierten a.sign Premium Zertifikats für sichere 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 sicheren digitalen 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], [Zert-ACOS] und [A-SIT-CardOS]) basiert, und unter Verwendung von bescheinigten Komponenten und Verfahren kann eine sichere Signatur erstellt werden. Die sichere Überprüfung einer sicheren Signatur bedingt ebenfalls die Verwendung von dafür bescheinigten Komponenten und Verfahren.

Für alle dieser empfohlenen Komponenten und Verfahren ist die Durchführung eines Evaluierungsprozesses durch eine Bestätigungsstelle (z. B. A-SIT) notwendig.

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 sichere Signaturen Beachtung fanden.

2 Verpflichtungen und Haftungsbestimmungen

2.1 Verpflichtungen der a.trust

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

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

a.trust hat die Pflicht, eine Liste der für eine sichere Signaturerzeugung und -prüfung zu verwendenden Komponenten und Verfahren zur erstellen und aktuell zu halten und diese den Signatoren und Überprüfern von Zertifikaten zugänglich zu machen.

a.trust ist verpflichtet, die Signatoren über die erfolgte freiwillige Akkreditierung bei der Aufsichtsstelle gem. § 17 [SigG] zu informieren.

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

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

2.2 Verpflichtungen des Signators

a.trust bindet den Signator vertraglich an die Einhaltung der nachfolgend angeführten Verpflichtungen anlässlich der Registrierung (siehe Kapitel 3.3.1). Dazu hat der Signator die ihm zugesandten Vertragsbedingungen mit eigenhändiger Unterschrift zu akzeptieren und der Registrierungsstelle auszuhändigen.

Die dem Signator auferlegten Verpflichtungen umfassen die folgenden Punkte:

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

2. die ausschließliche Verwendung des Signaturschlüssels für die Erstellung digitaler Signaturen unter Beachtung der dem Signator mitgeteilten Beschränkungen,

3. die Anwendung entsprechender Vorsicht, um den unbefugten Gebrauch seines privaten Schlüssels zu verhindern und die sichere Vernichtung desselben nach Ablauf der Gültigkeitsperiode sowie die sichere Vernichtung der a.sign Premium Karte (z. B. mittels Durchschneiden oder Durchstanzen des Chips), sofern sie nicht weiterhin für andere Zwecke wie z. B. Maestroanwendungen oder Studentenausweis verwendet werden soll,

4. den Einsatz der von a.trust empfohlenen technischen Komponenten und Verfahren für die Erstellung der sicheren elektronischen Signatur,

5. dafür Sorge zu tragen, dass auf dem PC-Arbeitsplatz, an welchem die sichere digitale Signatur erstellt wird, kein unbefugt eingebrachter Programmcode zur Anwendung kommt:

   - Der Signator muss alle notwendigen technischen und organisatorischen Maßnahmen ergreifen, um unbefugten Zugriff auf seinen PC-Arbeitsplatz und die darauf befindlichen Daten 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.

6. die unverzügliche Benachrichtigung von a.trust, wenn vor Ablauf der Gültigkeitsdauer des Zertifikats, einer der nachfolgenden Fälle eintritt:

   - der private Schlüssel des Signators wurde verloren, gestohlen oder möglicherweise kompromittiert,

   - die Kontrolle über den privaten Schlüssel durch Kompromittierung der Aktivierungsdaten (PIN) oder durch andere Umstände ging verloren,

   - die im Zertifikat beinhalteten Informationen sind ungenau oder haben sich geändert.

Verwendet der Signator andere als die von a.trust empfohlenen technischen Komponenten und Verfahren, so haftet a.trust ausschließlich für den Inhalt des von ihr ausgestellten qualifizierten Zertifikates, zum Zeitpunkt der Ausstellung, und für die Sicherheit der a.sign Premium Karte hinsichtlich ihrer Funktionalität als sichere Signaturerstellungseinheit.

2.3 Verpflichtungen des Überprüfers von Zertifikaten

Ein Überprüfer (§18 Abs 4 [SigG]), der ein a.trust Zertifikat zur Verifizierung einer Signatur verwendet, kann diesem nur dann vertrauen, wenn er

- eine Überprüfung der Gültigkeitsperiode und des Sperr- oder Widerrufsstatus des Zertifikats unter Verwendung der von a.trust bereitgestellten Abfragemöglichkeiten vornimmt,
- eventuelle im Zertifikat oder den veröffentlichten Geschäftsbedingungen dargelegte Einschränkungen der Nutzung des Zertifikats beachtet (siehe dazu auch unten und Kapitel 1.3, letzter Absatz),
- und sämtliche anderweitig vorgeschriebene Vorsichtsmaßnahmen (siehe [CPS]) einhält.

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

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

2.4 Haftung

a.trust haftet als Aussteller 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 Certification Practice Statement

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

1. a.trust 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 Qualified Certificate Policy zu erfüllen, in ihrem Sicherheitskonzept dargestellt.

3. Das Certification Practice Statement 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 das Certification Practice Statement und jegliche Dokumentation, die die Übereinstimmung mit dieser Policy dokumentiert, zugänglich (siehe Kapitel 3.3.4).

5. Die Geschäftsführung der a.trust stellt das alleinige Entscheidungsgremium dar, das für die Genehmigung des Certification Practice Statements 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 im Certification Practice Statement vorgenommen werden sollen, und wird nach Genehmigung derselben entsprechend Punkt 5 dieses Absatzes eine überarbeitete Version des Certification Practice Statements 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 bleiben:

- bei der Übergabe zur Veröffentlichung an die Aufsichtsstelle durch Übermittlung eines signierten PKCS#10 Certificate Request und
- durch Herausgabe eines selbstsignierten Zertifikats und Veröffentlichung desselben im Verzeichnisdienst der a.trust und Veröffentlichung eines Fingerabdrucks des öffentlichen Schlüssels in gedruckter Form.

Das Zertifikat des CA-Schlüssels wird den Signatoren durch Speicherung auf der a.sign Premium Karte zugänglich gemacht. a.trust gewährleistet die Authentizität dieses Zertifikats.

3.2.4 Schlüsseloffenlegung

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

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 innerhalb von physisch abgesicherten Räumlichkeiten verwendet.

3.2.6 Ende der Gültigkeitsperiode von CA-Schlüsseln

Eine Archivierung ist nicht vorgesehen und eine Verwendung über die Gültigkeitsperiode hinaus ist damit ausgeschlossen.

3.2.7 Verwaltung und Lebenszyklus der Hardware Security Module für die Zertifizierung

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

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

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

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

3.2.8 Erzeugung der Schlüssel für die Signatoren

Die Generierung der Schlüssel der Signatoren entspricht den Bestimmungen von § 3 Abs 2 und Anhang 1 [SigV]. Sicherheit und Geheimhaltung der privaten Schlüssel sind gewährleistet:

1. Der verwendete Algorithmus ist für sichere digitale Signaturen geeignet und als solcher bestätigt.

2. Bei der a.sign Premium Karte handelt es sich um eine von einer Bestätigungsstelle (wie z. B. A-SIT) nach §18(5) [SigG] bescheinigte Smartcard, welche eine sichere Signaturerstellungseinheit darstellt und die Erzeugung und Speicherung der Signaturerstellungsdaten und die Erstellung sicherer elektronischer Signaturen ermöglicht (siehe [A-SIT-Starcos], [Zert-ACOS] und [A-SIT-CardOS]).

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

4. Der geheime Schlüssel wird in der a.sign Premium Karte während der Initialisierung generiert und kann nicht ausgelesen werden.

5. Nur der Signator hat Zugriff auf seinen privaten Schlüssel. Dies wird dadurch gewährleistet, dass:

- die a.sign Premium Karte mit dem Signaturschlüsselpaar nur gegen Ausweisleistung an den Signator übergeben wird oder
- der Signator die a.sign Premium Karte mit dem Signaturschlüsselpaar zwar schon in seinem Besitz hat, aber die zur Auslösung der Signatur notwendige PIN unmittelbar in der Registrierungsstelle nach seiner ordnungsgemäßen Identifizierung vergeben muss.

3.2.9 Sicherheit der a.sign Premium Karte

a.trust ergreift alle nötigen Maßnahmen, dass die a.sign Premium Karte vor Verfälschung und missbräuchlicher Verwendung geschützt wird.

Im Chip der a.sign Premium Karten ist verfügbarer Speicherplatz für zusätzliche Daten vorhanden. Zusätzliche Daten dürfen ausschließlich mit Genehmigung und Freigabe durch a.trust in die a.sign Premium Karte eingebracht werden.

3.2.9.1 a.sign Premium Karte für Studenten und Mitarbeiter der Wirtschaftsuniversität Wien

Die Initialisierung der a.sign Premium Karte für WU-Studenten und -Mitarbeiter erfolgt in abgeschlossenen streng kontrollierten Räumlichkeiten im Rechenzentrum der Telekom Austria. Danach wird sie an die Registrierungsstelle versandt.

Die Verwendung der Signaturfunktion der WU-Karte ist durch eine PIN geschützt. Der Signator gibt eine selbst gewählte 8-stellige PIN anlässlich des Registrierungsvorgangs in der RA ein.

Die Möglichkeiten von PIN-Fehleingaben sind begrenzt. Nach drei Fehleingaben ist die Signaturfunktion der a.sign Premium Karte gesperrt.

3.2.9.2 a.sign Premium Standardkarte Variante 1

Die Produktion der Karte beim Kartenhersteller erfolgt in abgeschlossenen streng kontrollierten Räumlichkeiten.

Die Verwendung der Signaturfunktion der Karte ist durch eine PIN geschützt. Der Signator muss die sechs-stellige Signatur-PIN selbst unmittelbar bei der Abholung der Karte in der Registrierungsstelle wählen.

Die Möglichkeiten von PIN-Fehleingaben sind begrenzt. Nach zehn Fehleingaben ist die Signaturfunktion der Karte gesperrt.

3.2.9.3 a.sign Premium Standardkarte Variante 2

Die Produktion der a.sign Premium Karte beim Kartenhersteller erfolgt in abgeschlossenen streng kontrollierten Räumlichkeiten.

Die Verwendung der Signaturfunktion der a.sign Premium Karte ist durch eine PIN geschützt. Der Signator erhält eine Initial-PIN von a.trust per Post in einem Kuvert zugesandt, die vom Signator bei der Abholung der Karte in der Registrierungsstelle in einen selbst gewählten Wert geändert werden muss. Die Initial-PIN ist nicht geeignet die Signaturfunktion auszulösen.

Die Möglichkeiten von PIN-Fehleingaben sind begrenzt. Nach zehn Fehleingaben ist die Signaturfunktion der a.sign Premium Karte gesperrt.

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 im Auftrag der a.trust handelnden Registrierungsstellen haben den Antragsteller auf ein qualifiziertes Zertifikat an Hand eines amtlichen Lichtbildausweises zu identifizieren. Dafür ist die physische Anwesenheit des Antragstellers unabdingbar.

Der Zertifikatsantrag enthält in Entsprechung von § 11 Abs 2 [SigV] u. a. die folgenden Daten:

- den vollständigen Namen und die Meldeadresse des Zertifikatswerbers,
- Datum und Ort der Geburt des Zertifikatswerbers,
- Datum der Ausstellung und Nummer des vorgelegten Lichtbildausweises sowie die Behörde, die diesen ausstellte.

Der Signaturvertrag (Antrag auf Ausstellung eines qualifizierten Zertifikats) ist vom Antragsteller hinsichtlich Korrektheit der Daten zu überprüfen und unterschrieben der

Registrierungsstelle auszuhändigen. Er beinhaltet insbesondere die Akzeptanz der folgenden Vereinbarungen:

- die Annahme der Verpflichtungen des Signators,
- die Bestätigung der Aushändigung der a.sign Premium Karte,
- die Zustimmung dass von a.trust Aufzeichnungen über den Registrierungsvorgang und alle dabei erhaltenen Daten geführt werden, und dass diese Aufzeichnungen ggf. bei Beendigung der Zertifizierungsdienste an Dritte übergeben werden können,
- die Zustimmung zur Veröffentlichung des Zertifikats oder die Ablehnung derselben, und
- die Bestätigung der Korrektheit des Zertifikatsinhalts.

Der Signator kann im Zertifikat statt seines Namens mit einem Pseudonym bezeichnet werden. Die Einhaltung der Anforderungen von § 8 Abs 4 [SigG]) werden dabei von der Registrierungsstelle überprüft.

Der Zertifikatsantrag und alle damit im Zusammenhang stehenden relevanten Dokumente (das vom Antragsteller vorgelegte Ausweispapier) werden entsprechend § 16 Abs 1 [SigV] auf die Dauer von 33 Jahren elektronisch archiviert.

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

3.3.1.1 Registrierung für WU-Karten

Die Geschäftsbedingungen und allfällige sonstige Bestimmungen zur Nutzung des Zertifikats werden dem Signator über die a.trust Homepage zugänglich gemacht (siehe 3.3.4).

Der Antrag auf Ausstellung eines qualifizierten Zertifikats inklusive Signaturvertrag und ein Merkblatt für die Registrierung werden dem Signator ausgehändigt.

3.3.1.2 Registrierung für Standardkarten Variante 1

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

Wenn die Karte über die Homepage oder die RA bestellt wurde, wird der Antrag auf Ausstellung eines qualifizierten Zertifikats inklusive Signaturvertrag dem Signator zu-

gesandt. In jedem Fall werden dem Signator der Antrag auf Ausstellung eines qualifizierten Zertifikats inklusive Signaturvertrag und ein Merkblatt bei der Registrierung ausgehändigt.

3.3.1.3 Registrierung für Standardkarten Variante 2

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

Der Antrag auf Ausstellung eines qualifizierten Zertifikats inklusive Signaturvertrag, ein Merkblatt für die Registrierung und das PIN-Kuvert werden dem Signator zugesandt.

3.3.2 Verlängerung der Gültigkeitsdauer der Signaturprüfdaten und Neuausstellungen eines Zertifikats

Durch die nachfolgend angeführten Maßnahmen wird sicher gestellt, dass Anträge von Zertifikatswerbern, die bereits anlässlich einer vorhergehenden Zertifikatsausstellung registriert wurden, vollständig, korrekt und ordnungsgemäss autorisiert sind. Die Maßnahmen gelten sowohl für die Verlängerung der Gültigkeitsdauer der Signaturprüfdaten als auch für die Neuausstellung nach Ablauf oder Widerruf eines Zertifikats.

1. Die Registrierungsstelle hat die Daten zur Identifikation des Antragstellers hinsichtlich ihrer aktuellen Gültigkeit zu prüfen.

2. Etwaige Änderungen in den Vertragsbedingungen werden dem Antragsteller mitgeteilt und seine Zustimmung dazu eingeholt. Die Maßnahmen erfolgen in Übereinstimmung mit Abschnitt 3.3.1.

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

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

5. Bei WU-Karten ist eine Verlängerung der Gültigkeitsdauer nicht möglich, sondern nur bei a.sign Premium Standardkarten.

3.3.3 Erstellung des Zertifikats

Durch die folgenden Maßnahmen wird sicher gestellt, dass Ausstellung, Verlängerung und Neuausstellung von Zertifikaten in sicherer Weise erfolgen und 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. Die eindeutige Zuordnung des Schlüsselpaars zum Signator ist bei der a.sign Premium WU Karte durch die folgenden Maßnahmen gegeben:

   - Auslesen der Kartennummer und des öffentlichen Schlüssels aus der a.sign Premium Karte und Vergleich der ausgelesenen Daten mit denen in der Datenbank.

   - Weiterleitung der Kartennummer und des öffentlichen Schlüssels gemeinsam mit den Signatordaten an die Zertifizierungsstelle und Ausstellung des a.sign Premium Zertifikats nach Verknüpfung mit den Signatordaten.

5. Die eindeutige Zuordnung des Schlüsselpaars zum Signator wird bei der a.sign Premium Standard Karte Variante 1 wie folgt sicher gestellt:

   - Wenn bereits bei der Bestellung eine Identifikationsnummer (CIN) vergeben und bei der Personalisierung durch den Kartenproduzenten auf die Kartenoberfläche gedruckt wurde, erfolgt eine Überprüfung der sichtbaren Kartendaten mit den Antragstellerdaten, insbesondere der CIN.

   - Wenn bereits bei der Personalisierung durch den Kartenproduzenten der Name auf der Kartenoberfläche aufgebracht wurde, vergleicht der RO diesen mit dem im Ausweis gespeicherten Namen.

   - Die Karte mit dem vorgenerierten privaten Schlüssel wird dem Signator erst zum Registrierungszeitpunkt zugeordnet (d. h. der Kartenproduzent bringt keine signatorspezifischen Daten auf den Chip oder die Kartenoberfläche auf), somit ist die Zuordnung eindeutig gewährleistet.

6. Die eindeutige Zuordnung des Schlüsselpaars zum Signator ist bei der a.sign Premium Standard Karte Variante 2 durch folgende Vorkehrungen sicher gestellt:

   - Einstellung des öffentlichen Schlüssels in ein Transport-Zertifikat der a.sign Premium Karte während der Kartenproduktion.

   - Überprüfung der sichtbaren Kartendaten mit den Antragstellerdaten, insbesondere der Identifikationsnummer.

- Auslesen des Transport-Zertifikats aus der a.sign Premium Karte und Verifizieren dieses Zertifikats im Rahmen der Registrierung.

- Weiterleitung dieses Zertifikats gemeinsam mit den Signatordaten an die Zertifizierungsstelle von a.trust und Ausstellung des a.sign Premium Zertifikats nach Verknüpfung mit den Signatordaten.

7. 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:

1. der gegenständlichen Certificate Policy,

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

3. der Allgemeinen Geschäftsbestimmungen von a.trust,

4. der Belehrungen für den Signator,

5. der sonstigen Mitteilungen.

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

In o. a. Dokumenten ist eindeutig festgelegt:

- dass die qualifizierten Zertifikate an die Öffentlichkeit ausgegeben werden (kein eingeschränkter Benutzerkreis) und ihre Anwendung an eine sichere Signaturerstellungseinheit (a.sign Premium Karte) gebunden ist,
- dass nur dann eine sichere Signatur erstellt wird, wenn die von a.trust empfohlenen Komponenten und Verfahren verwendet werden, andernfalls handelt es sich um eine einfache Signatur,
- die Verpflichtungen des Signators in Entsprechung zu Kapitel 2.2.
- die Vorgehensweise zur Überprüfung eines Zertifikats inklusive der Notwendigkeit der Überprüfung des Zertifikatsstatus, so dass der Überprüfer mit gutem Grund dem Zertifikat vertrauen kann (siehe 2.3),
- wie ein ggf. den Umfang der Haftung einschränkendes Transaktionslimit in a.sign Premium Zertifikaten zu erkennen ist,
- die Zeitdauer für die Registrierungsinformationen aufgehoben werden (siehe Kapitel 3.3.1),
- die Zeitdauer für die Aufzeichnungen von wichtigen Ereignissen der Zertifizierungsstelle aufgehoben werden (siehe Kapitel 3.4.11),
- Vorgehensweisen zur Behandlung von Beschwerden und Streitfällen,
- die Anwendbarkeit des [SigG] und [SigV].

3.3.5 Veröffentlichung der Zertifikate

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

1. Anlässlich der Erstellung eines Zertifikats wird dieses am Ende des Registrierungsvorgangs auf die a.sign Premium Karte des Signators gespeichert.
2. Wenn der Signator damit einverstanden ist, wird das Zertifikat im Verzeichnisdienst von a.trust veröffentlicht.
3. Die Bedingungen für die Benutzung eines Zertifikats werden von a.trust allen Beteiligten zur Kenntnis gebracht (siehe Kapitel 3.3.4).
4. Die Identifikation der anzuwendenden Bestimmungen ist durch die eindeutige Zuordnung zum Produktnamen "a.sign Premium" einfach herstellbar.

5. Der Verzeichnisdienst ist 7 Tage 24 Stunden verfügbar. Unterbrechungen von mehr als 30 Minuten werden gemäß § 13 Abs 5 [SigV] als Störfälle dokumentiert.

6. Die Verzeichnisdienste sind öffentlich und international zugänglich.

3.3.6 Sperre und Widerruf

Eine Sperre ist ein zeitlich begrenztes Aussetzen der Gültigkeit eines Zertifikats. Der Widerruf ist eine irreversible vorzeitige Beendigung der Gültigkeit eines Zertifikats.

1. Die Vorgangsweisen für das Auslösen von Sperre und Widerruf sind im Certification Practice Statement 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.

2. Ein Widerruf kann jederzeit vom Signator beim Widerrufsdienst von a.trust telefonisch oder per Fax beantragt werden. Die Sperre und Sperraufhebung kann der Signator ausschließlich telefonisch beim Widerrufsdienst beantragen. Alle Anträge werden mit Einlangen bearbeitet.

3. Die Durchführung von Sperren und Widerrufen beim Widerrufsdienst ist an die Kenntnis eines dafür eigens vorgesehenen Sperr- und Widerrufspassworts gebunden. In Ausnahmefällen und bei Dringlichkeit können auch andere mit dem Signator verknüpfte Informationen zur Identifikation der Rechtmäßigkeit herangezogen werden. In diesem Fall ist allerdings nur die Durchführung einer Sperre möglich.

4. Wenn eine Sperre beantragt wird, muss der Signator dem Mitarbeiter des Widerrufsdienstes ein mindestens vier-stelliges Passwort mitteilen, mit dem er innerhalb der Sperrfrist die Sperre wieder aufheben lassen kann. Dieses Passwort darf nicht mit dem Passwort für Sperre und Widerruf identisch sein und muss anlässlich jeder Sperre neu gewählt werden.

5. Bei der Aufhebung der Sperre muss der Signator dann zwingend das gewählte Sperraufhebungspasswort angeben, da sonst keine Sperraufhebung durchgeführt wird und die Sperre bestehen bleibt, bis sie nach Ende der Frist in einen Widerruf umgewandelt wird.

6. Für die Durchführung eines Widerrufs muss dem Mitarbeiter des Widerrufsdienstes ein Widerrufsgrund genannt werden.

7. Die Sperre gilt, sofern sie nicht vorher aufgehoben wird, vom Zeitpunkt der Aufgabe bis 22:00 Uhr des zweiten auf den Tag der Beantragung folgenden Werktags, an dem sie in einen Widerruf übergeführt wird.

8. Von der Durchführung eines Widerrufs oder einer Sperre wird der Signator von a.trust schriftlich verständigt.

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

10. Anlässlich der Durchführung eines Widerrufs kann der Signator bei dem Mitarbeiter des Widerrufsdienstes die Ersatzbestellung seiner a.sign Premium Standardkarte veranlassen.

11. 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.

12. 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.

13. 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.

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

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

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

3.4 a.trust Verwaltung

3.4.1 Sicherheitsmanagement

Es gelten die folgenden Bestimmungen:

1. a.trust ist für alle Prozesse im Rahmen der Zertifizierungsdienste verantwortlich, dies gilt auch für die an Vertragspartner ausgelagerten Registrierungs- und Widerrufsdienste sowie die für die Signatur relevanten Bereiche der Kartenproduktion. Die Verantwortlichkeiten der Vertragspartner sind klar geregelt und Kontrollen zur Überprüfung der ordnungsgemäßen Tätigkeit eingerichtet. Die für die Sicherheit relevanten Vorgehensweisen sind im Certification Practice Statement für a.sign Premium (siehe [CPS]) veröffentlicht.

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

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

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

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

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:

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

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

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

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

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

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

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

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

9. Entsprechend § 10 Abs 4 [SigV] beschäftigt a.trust keine Personen, die strafbare Handlungen begangen haben, die sie für eine vertrauenswürdige Position ungeeignet erscheinen lassen. Eine Beschäftigung erfolgt erst nach einer diesbezüglichen Überprüfung.

3.4.4 Physikalische und organisatorische Sicherheitsmaßnahmen

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

1. Der Zutritt zu den Räumlichkeiten, in denen Zertifizierungs- und Widerrufsdienste erbracht 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.

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

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

4. Die Systeme für Zertifikatsgenerierung, die Kartenbereitstellung 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, Kartenbereitstellung und Widerrufsdienste erfolgt durch klar definierte Sicherheitszonen d. h. durch

räumliche Trennung von anderen organisatorischen Einheiten und physischen Zutrittsschutz.

6. Die Sicherheitsmaßnahmen inkludieren den Gebäudeschutz, die Computersysteme selbst und alle sonstigen Einrichtungen, die für deren Betrieb unerlässlich sind. Der Schutz der Einrichtungen für die Zertifikatserstellung, 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.

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

3.4.5 Betriebsmanagement

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

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

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

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

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

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

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

7. Auf Zwischenfälle wird so rasch wie möglich reagiert, um 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:

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

Diese Aufgaben werden von 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.

1. Sicherungsmaßnahmen wie z. B. Firewalls bewahren das interne Netzwerk vor Zugriffen durch Dritte.
2. Vertrauliche Daten werden geschützt, wenn sie über unsichere Netzwerke ausgetauscht werden, wie z. B. die Registrierungsdaten.
3. Eine Benutzerverwaltung, die den verschiedenen Funktionen unterschiedliche Zugriffsrechte einräumt, ist eingerichtet; insbesondere werden sicherheitsrelevante von nicht sicherheitskritischen Funktionen sorgfältig getrennt. Änderungen in den Zugriffsrechten werden im System sofort nachgezogen. Die Kontrolle der Benutzerverwaltung ist Teil des internen Audits.
4. Zugriff auf Informationen und Anwendungen ist auf Grund der vergebenen Zugriffsrechte eingeschränkt. Die dafür geltenden Definitionen sind im

Certification Practice Statement für a.sign Premium (siehe [CPS]) angeführt. Administrative und den laufenden Betrieb betreffende Funktionen sind streng getrennt. Die Verwendung von System-Utility-Programmen ist besonders eingeschränkt.

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

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

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

8. Komponenten des lokalen Netzwerks befinden sich in einer physisch gesicherten Umgebung und die Konfiguration wird periodisch überprüft.

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

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

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

3.4.7 Entwicklung und Wartung vertrauenswürdiger Systeme

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

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

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

3.4.8 Erhaltung des ungestörten Betriebes und Behandlung von Zwischenfällen

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

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

2. Sollte dieser Fall eintreten, so hat a.trust die Aufsichtsstelle (siehe § 6 Abs 5 [SigG]), die 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.

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

3.4.9 Einstellung der Tätigkeit

Gem. § 12 [SigG] wird a.trust die Einstellung der Tätigkeit unverzüglich der Aufsichtsstelle anzeigen und sicher stellen, dass eine eventuelle Beeinträchtigung der Dienstleistung gegenüber 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 Certification Practice Statement 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:

1. Wichtige Aufzeichnungen werden vor Verlust, Zerstörung und Verfälschung bewahrt.

2. Die Anforderungen des Datenschutzgesetzes werden befolgt.

3. Nötige technische und organisatorische Maßnahmen wurden ergriffen, um persönliche Daten vor unautorisierter und ungesetzlicher Verarbeitung sowie vor versehentlicher Zerstörung oder Beschädigung zu schützen.

4. Den Signatoren wird versichert, dass die an a.trust übermittelten Informationen nur mit ihrem Einverständnis, mit gerichtlichem Beschluss oder auf Basis gesetzlicher Regelungen offen gelegt werden.

3.4.11 Aufbewahrung der Informationen zu 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 Zertifikats-Management stehen.

5. Alle Datensätze, die in Zusammenhang mit qualifizierten Zertifikaten stehen, werden entsprechend § 16 (1) [SigV] für 33 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, insbesondere dessen eindeutige Nummer,
   - die Aufbewahrungsstelle der elektronischen Kopien der Antragsdokumente inklusive der Ausweispapiere,
   - 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

1. Alle Richtlinien und Vorgehensweisen sind nicht-diskriminierend.

2. Die Dienstleistungen von a.trust stehen allen Personen zur Verfügung, die über einen

   - österreichischen Personalausweis bzw. eine Identitätskarte oder
   - einen österreichischen Führerschein oder
   - einen international gültigen Reisepass in deutscher und/oder englischer Sprache verfügen.

3. a.trust ist eine juristische Person (Gesellschaft mit beschränkter Haftung).

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

5. Die Haftung, insbesondere diejenige zur Schadenswiedergutmachung, entspricht den Bestimmungen des [SigG] (siehe Kapitel 2.4).

6. Hinsichtlich der finanziellen Ausstattung befolgt a.trust die Bestimmungen in § 2 [SigG].

7. Das von a.trust beschäftigte Personal verfügt entsprechend den Bestimmungen des [SigG] (siehe auch Kapitel 3.4.3) über die nötige Schulung, Training, technisches Wissen und Erfahrung und ist in ausreichender Zahl vorhanden, um den geplanten Umfang der Zertifizierungsdienste bewerkstelligen zu können.

8. Es sind Richtlinien und Vorgehensweisen für die Behandlung von Beschwerden und Streitfällen vorhanden, die von Kunden oder anderen Parteien an die a.trust herangetragen werden und die Erbringung ihrer Dienstleistungen betreffen.

9. Die rechtlichen Beziehungen zu Subunternehmern, die Dienstleistungen für a.trust erbringen, sind vertraglich geregelt und ordnungsgemäß dokumentiert.

10. Es gibt keine aktenkundigen Gesetzesverletzungen seitens a.trust.

3.5.2 Zertifikatserstellungs- und Widerrufsdienste

Die für die Erbringung von Zertifizierungs- und Widerrufsdiensten vorgesehenen organisatorischen Einheiten sind hinsichtlich ihrer Entscheidungen über die Erbringung, Aufrechterhaltung und Beendigung der Dienstleistungen 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.

4 Anhang

A Begriffe und Abkürzungen

a.sign Premium Karte	Eine Prozessorchipkarte, die geheime Schlüssel des Karteninhabers enthält und zur Erstellung und Verifizierung digitaler Signaturen dient.
Certificate Policy, Policy	Ein Regelwerk, das den Einsatzbereich eines Zertifikates für eine bestimmte Benutzergruppe und/oder Anwendungsklasse festhält.
CPS, Certification Practice Statement	Aussagen über die bei der Ausstellung von Zertifikaten von einem Zertifizierungsdiensteanbieter eingehaltenen Vorgehensweise
Digitale Signatur	Elektronische Signatur, die mit Hilfe von Verfahren der asymmetrischen Kryptographie erzeugt wird.
E-Mail	Electronic Mail; Nachrichten, die in digitaler Form über computerbasierte Kommunikationswege versandt oder empfangen werden.
Elektronische Signatur	Eine Signatur in digitaler Form, die in Daten enthalten ist, Daten beigefügt wird oder logisch mit ihnen verknüpft ist und von einem Unterzeichner verwendet wird, um zu bestätigen, dass er den Inhalt dieser Daten billigt. Sie ist so mit den Daten verknüpft, dass eine nachträgliche Veränderung der Daten offenkundig wird.
Hardware Security Modul	Elektronisches System zur sicheren Speicherung von Schlüsseln und zur Berechnung und Verifizierung von Signaturen.
Integrität (von Daten)	Ein Zustand, in dem Daten weder von Unbefugten verändert noch zerstört wurden.
Kompromittierung	Eine unautorisierte Offenlegung von oder der Verlust der Kontrolle über sicherheitskritische Informationen und geheimzuhaltende Daten.
OCSP	Online Certificate Status Protocol
Öffentlicher Schlüssel	Öffentlicher Teil eines Schlüsselpaares. Er ist Bestandteil eines Zertifikates und wird zur Überprüfung von Digitalen Signaturen bzw. zur Verschlüsselung von Nachrichten/Daten verwendet.
PIN	Personal Identification Number

Privater Schlüssel, geheimer Schlüssel	Geheimer Teil eines Schlüsselpaares, der zum digitalen Signieren sowie zum Entschlüsseln von Nachrichten/Dokumenten erforderlich ist und geheimgehalten werden muss.
Public-Key System	Ein 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 (private) 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 Zertifizierungsrichtlinie (CPS) durchführt und selbst keine Zertifikate ausstellt.
Schlüsselpaar	Ein privater Schlüssel und der dazugehörige öffentliche Schlüssel. Abhängig vom verwendeten Algorithmus kann man mit Hilfe des öffentlichen Schlüssels eine digitale Unterschrift, die mit dem dazugehörigen privaten Schlüssel erstellt wurde, verifizieren bzw. mit dem privaten Schlüssel Daten entschlüsseln, welche mit dem zugehörigen öffentlichen Schlüssel verschlüsselt wurden.
Signator	Eine Person, die eine elektronische Signatur erstellt.
Signaturerstellungseinheit	Komponenten, die vom Unterzeichner verwendet werden, um eine elektronische Signatur zu erstellen.
Signaturprüfdaten	Daten wie Codes oder öffentliche Signaturschlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden (§ 2(6) [SigG]).
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 Zertifikatserwiete-rungen erstellt werden können
Zertifikats-Widerrufsliste, CRL	Eine digital signierte Datenstruktur, die widerrufene Zertifikate anführt, welche von einem bestimmten Zertifizierungsdiensteanbieter ausgestellt wurden.
Zertifizierungsdienstean-bieter, Certification Authority, CA	Eine Person oder Stelle, die Zertifikate ausstellt oder anderweitige elektronische Signaturdienste öffentlich anbieten darf.
Zertifizierungsrichtlinie	Gleichbedeutend mit Certification Practice Statement, siehe CPS

B Referenzdokumente

[SigG]	Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG). BGBl. I Nr. 190/1999 (NR: GP XX RV 1999 AB 2065 S. 180. BR: AB 6065 S. 657.)
[SigV]	Verordnung zum Signaturgesetz, BGBl II 2000/30, 02. 02. 2000
[SigRL]	Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, 13. 12. 1999
[DSG]	Bundesgesetz über den Schutz personenbezogener Daten (Daten-schutzgesetz 2000 - DSG 2000). BGBl. I Nr. 165/1999 (NR: GP XX RV 1613 AB 2028 S. 179. BR: 5992 AB 6034 S. 657.)
[CPS]	a.trust Certification Practice Statement für qualifizierte a.sign Premium Zertifikate für sichere Signaturen
[BWG99]	Bundesgesetz über das Bankwesen (Bankwesengesetz - BWG). BGBl. I Nr. 123/1999 (NR: GP XX RV 1793 AB 1894 S. 175. BR: 5966 AB 5978 S. 656.)
[ETSI]	Policy requirements for certification authorities issuing qualified certificates – ETSI TS 101 456, V1.2.1 (2002-04)
[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, 20.08.2004
[A-SIT-CardOS]	A-SIT Bescheinigung nach §18(5) SigG: Prozessorchipkarte mit Smart Card IC SLE 66CX320P und Betriebssystem CardOS/M4.01 (Version C803) und Applikation für digitale Signatur Version 0.20, 18.11.2004
[Zert-ACOS]	BSI Zertifizierungsbestätigung BSI-DSZ-CC-0220-2004 und BSI-DSZ-CC-0221-2004 vom 19.10.2004 und Stellungnahme von A-SIT über die in Bescheinigung befindliche ACOS-Karte