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 fortgeschrittene Zertifikate
a.sign token

Version: 1.0.4

Datum: 14.10.2011

Inhaltsverzeichnis

1 Einführung

1.1 Überblick

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

Die a.sign token Certificate Policy gilt für fortgeschrittene Signaturzertifikate entsprechend den Definitionen der EU-Richtlinie [SigRL] und dem österreichischen Bundesgesetz über elektronische Signaturen [SigG], welche an Endbenutzer ausgestellt werden, auf Signaturerstellungseinheiten (a.sign token Karten) basieren und für die Erstellung fortgeschrittener digitaler Signaturen geeignet sind.

Weiters gilt sie für Verschlüsselungszertifikate, welche ebenfalls an Endbenutzer ausgestellt werden und auf a.sign token bzw. a.sign Premium Karten basieren und für Authentifizierung, Verschlüsselung und die Erstellung fortgeschrittener Signaturen verwendet werden können.

1.2 Identifikation

Name der Policy: a.trust Certificate Policy für fortgeschrittene Zertifikate a.sign token

Version: 1.0.4

Object Identifier: **1.2.040.0.17** (a.trust) **.1** (Policy) **.12** (a.sign token)
.1.0.4 (Version) vorliegende Version

Der A-Trust OID 1.2.040.0.17 ist bei ÖNORM registriert.

Die vorliegende Policy ist in Übereinstimmung mit [ETSI] Klasse „QCP public with SSCD“ und [RFC3647].

1.3 Anwendungsbereich

Die a.sign token Policy gilt für fortgeschrittene Zertifikate entsprechend der Definition § 2 Abs. 8 [SigG], welche ausschließlich an Endbenutzer ausgestellt werden. Die ge-

heimen Schlüssel der Zertifikatsinhaber befinden sich auf Signaturerstellungseinheiten, den a.sign token Karten.

a.sign token Zertifikate werden sowohl für Signatur- als auch für Entschlüsselungsschlüssel, welche sich auf a.sign token Karten befinden, ausgestellt.

Weiters werden a.sign token Zertifikate für jene Entschlüsselungsschlüssel, die sich auf a.sign Premium Karten befinden, ausgestellt.

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

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

1.4 Übereinstimmung mit der Policy

a.trust verwendet den Object Identifier aus Kapitel 1.2 nur für die Erstellung von Zertifikaten, anlässlich deren Ausgabe die Regelungen der gegenständlichen Policy für a.sign token Zertifikate Beachtung fanden.

2 Verpflichtungen und Haftungsbestimmungen

2.1 Verpflichtungen von a.trust

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

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

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

a.trust erbringt die Zertifizierungsdienste in Übereinstimmung mit der Zertifizierungsrichtlinie für a.sign token.

2.2 Verpflichtungen des Zertifikatsinhabers

a.trust bindet den Zertifikatsinhaber 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 Zertifikatsinhaber auferlegten Verpflichtungen umfassen:

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

2. die 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 Karte, auf der sich der private Schlüssel befindet.

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

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

2.3 Verpflichtungen des Überprüfers von Zertifikaten

Ein Überprüfer, 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),
- und sämtliche anderweitig vorgeschriebene Vorsichtsmaßnahmen (siehe [CPS]) einhält.

2.4 Haftung

a.trust haftet als Aussteller von a.sign token Zertifikaten

- für die Einhaltung der zugehörigen Zertifizierungsrichtlinie (siehe [CPS]), insbesondere für die darin festgelegten Maßnahmen zur prompten Veröffentlichung von Widerrufslisten und die Einhaltung der in der Zertifizierungsrichtlinie genannten Standards (ITU X.509)
- dafür, dass die im Zertifikat enthaltenen Daten des Zertifikatsinhabers zum Zeitpunkt der Ausstellung korrekt waren und anlässlich der Registrierung überprüft wurden.

a.trust haftet nicht, falls sie nachweisen kann, dass sie an der Verletzung der oben angeführten Verpflichtungen keine Schuld trifft.

3 Anforderung an die Erbringung von Zertifizierungsdiensten

Diese Policy ist auf die Erbringung von fortgeschrittenen Zertifizierungsdiensten ausgerichtet. Dies umfasst die Bereitstellung von Registrierungsdiensten, Schlüsselgenerierung, Zertifikatserstellung, Zertifikatsausgabe, Widerrufsdiensten und Abfragediensten über den Zertifikatsstatus.

3.1 Certification Practice Statement

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

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

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

3. a.trust macht allen Signatoren und Überprüfern von elektronischen Signaturen das Certification Practice Statement und jegliche Dokumentation, die die Übereinstimmung mit dieser Policy dokumentiert, zugänglich (siehe Kapitel 3.3.4).

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

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

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

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

3.2 Verwaltung der Schlüssel zur Erbringung von Zertifizierungsdiensten

3.2.1 Erzeugung der CA-Schlüssel

Die Generierung der von a.trust zur Erbringung von Zertifizierungsdiensten verwendeten Schlüssel erfolgt in Übereinstimmung mit den Bestimmungen der §§ 6 und 8 [SigV] und damit in Übereinstimmung mit [SigRL] Annex II (f) und (g):

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

2. Die Schlüssel werden in einer Signaturerstellungseinheit (Hardware Security Modul) erstellt, die einem Bestätigungsverfahren bei A-SIT unterzogen wurde und zur Erstellung fortgeschrittener Signaturen geeignet ist.

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

4. Die Schlüssellänge und der Algorithmus wären ebenfalls für qualifizierte Zertifikate geeignet und entsprechen Anhang I [SigV] und den Empfehlungen der Expertengruppe der European Electronic Signature Standardisation Initiative.

3.2.2 Speicherung der CA-Schlüssel

a.trust stellt in Übereinstimmung mit den Bestimmungen aus § 10 [SigV] sicher, dass die privaten Schlüssel geheim gehalten werden und ihre Integrität bewahrt bleibt und beachtet auch für die Erbringung von fortgeschrittenen Zertifizierungsdiensten die Bestimmungen des § 10 [SigV].

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

Es sind Maßnahmen getroffen, die garantieren, dass die privaten Schlüssel von a.trust das Hardware Security Modul nicht verlassen (außer um in einen anderen HSM zum Zweck der Ausfallsicherheit importiert zu werden) und kein Zugriff von außen darauf möglich ist.

3.2.3 Verteilung der öffentlichen CA-Schlüssel

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

- bei der Übergabe zur Veröffentlichung an die Aufsichtsstelle durch Übermittlung eines signierten PKCS#10 Certificate Request und durch
- Ausstellung und Veröffentlichung eines selbstsignierten Root-Zertifikats.

Das Zertifikat des CA-Schlüssels wird den Zertifikatsinhabern durch Speicherung auf der a.sign token Karte und durch Veröffentlichung im Rahmen des Verzeichnisdienstes 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 token Zertifikaten und für die Signatur der zugehörigen Widerrufslisten innerhalb von physisch abgesicherten Räumlichkeiten verwendet.

3.2.6 Ende der Gültigkeitsperiode von CA-Schlüsseln

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

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

Eine Verwendung über die Gültigkeitsperiode hinaus ist damit ausgeschlossen.

3.2.7 Verwaltung und Lebenszyklus der Hardware Security Module für die Zertifizierung

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

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

2. Die Nutzung 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.

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

3.2.8 Erzeugung der Schlüssel für die Zertifikatsinhaber

Die Generierung der Schlüssel der Zertifikatsinhaber entspricht den Bestimmungen von Anhang 1 [SigV]. Die Generierung des Signaturschlüsselpaars des Signators entspricht zudem § 3 Abs. 2 [SigV]. Die Sicherheit und Geheimhaltung der privaten Schlüssel sind durch die folgenden Maßnahmen gewährleistet:

1. Der verwendete Algorithmus wäre auch für sichere digitale Signaturen geeignet und als solcher von A-SIT bestätigt.

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

3. Der geheime Signaturschlüssel wird in der a.sign token Karte während der Personalisierung generiert und kann nicht ausgelesen werden.

4. Der geheime Entschlüsselungsschlüssel wird in einem a.trust Hardware Security Modul erzeugt und in sicherer transportverschlüsselter Weise an den Kartenproduzenten übermittelt und dort auf die Karte aufgebracht. Er kann nicht aus der Karte ausgelesen werden.

5. Die Übergabe der a.sign token Karte mit den beiden Schlüsselpaaren an den Zertifikatsinhaber erfolgt nur gegen Ausweisleistung. Nur der Zertifikatsinhaber hat Zugriff auf seine privaten Schlüssel.

3.2.9 Sicherheit der a.sign token Karte

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

1. Die Produktion beim Kartenhersteller erfolgt in abgeschlossenen streng kontrollierten Räumlichkeiten.

2. Die fertig gestellte Karte wird vom Hersteller an die Registrierungsstelle versandt. In der Registrierungsstelle wird sie dem Signator nach Ausweisleistung übergeben.

3. Die Verwendung der Signaturfunktion der a.sign token 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.

4. Die Verwendung der Entschlüsselungsfunktion der a.sign token Karte ist auch durch eine PIN geschützt. Diese erhält der Zertifikatsinhaber mit demselben Kuvert per Post zugesandt. Die Entschlüsselungs-PIN kann nicht geändert werden.

5. Die Möglichkeiten von PIN-Fehleingaben sind begrenzt. Nach der vierten Fehleingabe der Signatur-PIN ist die Signaturfunktion gesperrt und kann durch Eingabe eines PUK wieder entsperrt werden.

6. Nach der vierten Fehleingabe der Entschlüsselungs-PIN ist die Entschlüsselungsfunktion der Karte gesperrt und kann durch Eingabe eines PUK wieder entsperrt werden.

7. Beide PUK-Werte erhält der Zertifikatsinhaber in einem Kuvert per Post zugesandt.

3.3 Lebenszyklus des Zertifikats

3.3.1 Registrierung des Zertifikatsinhabers

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

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

2. Der Antrag auf Ausstellung eines a.sign token Zertifikats inklusive Signaturvertrag, ein Merkblatt für die Registrierung und das PIN- und PUK-Kuvert werden dem Signator zugesandt; ein Antragsformular und das Merkblatt sind darüber hinaus über die Web-Seite der a.trust elektronisch zugänglich.

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

4. Die vom Antragsteller vorgelegten Ausweispapiere werden elektronisch archiviert.

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

   - 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.

6. Der Antrag auf Ausstellung eines a.sign token Zertifikats ist vom Antragsteller hinsichtlich Korrektheit der Daten zu überprüfen und unterschrieben der Registrierungsstelle auszuhändigen.

7. 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.

8. Eine vom Antragsteller zu nennende Kontaktadresse wird festgehalten.

9. Der mit dem Antragsteller abzuschließende Vertrag beinhaltet insbesondere:

   - die Annahme der Verpflichtungen des Zertifikatsinhabers,
   - die Bestätigung der Aushändigung der a.sign token Karte,
   - die Zustimmung, dass seitens a.trust Aufzeichnungen über den Registrierungsvorgang und allen dabei erhaltenen Daten geführt werden, und dass diese Aufzeichnungen ggf. bei Beendigung der Zertifizierungsdienste an Dritte übergeben werden kann,
   - die Zustimmung zur Veröffentlichung des Zertifikats oder die Ablehnung derselben und
   - die Bestätigung der Korrektheit des Zertifikatsinhaltes

10. Der Zertifikatsantrag und alle damit im Zusammenhang stehenden relevanten Dokumente (Ausweispapier) werden auf die Dauer von mind. sieben Jahren elektronisch archiviert.

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

3.3.2 Verlängerung der Gültigkeitsdauer des Zertifikats und Neuausstellungen

Durch die 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 als auch für die Neuausfolgung einer a.sign token Karte 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 von Zertifikaten vor deren Ablauf erfolgt entsprechend § 12 Abs 4 [SigV]. Die sich aus der Verlängerung ergebende neue Gültigkeitsperiode beträgt höchstens fünf Jahre. Eine Verlängerung erfolgt nur, wenn die kryptografische Sicherheit der verwendeten Verfahren über die gesamte neue Gültigkeitsdauer ausreichend sicher gestellt ist und keine Hinweise auf Kompromittierung des privaten Schlüssel des Antragsteller bestehen.

3.3.3 Erstellung des Zertifikats

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

1. Die a.sign token Zertifikate werden als X.509 v3 Zertifikate erstellt. Die in den Zertifikaten enthaltenen Angaben sind insb. die folgenden:

   - Versionsnummer des Zertifikats: es werden Zertifikate der Version 3 (codiert mit dem Wert 2) ausgestellt
   - Seriennummer des Zertifikats
   - Bezeichnung des Zertifikatsausstellers
   - Beginn und Ende der Gültigkeit des Zertifikats
   - Bezeichnung des Zertifikatsinhabers
   - öffentlicher Schlüssel (mit Angabe des Algorithmus)
   - Angabe des Algorithmus für die Signatur des Zertifikats
   - Signatur über das Zertifikat
   - Zertifikatserweiterungen, wie z. B.:
     - Informationen über die anzuwendende Policy bzw. CPS
     - Zertifikatsverwendung
     - Information zum Auffinden der CRL
     - Geburtsdatum des Zertifikatsinhabers (optional)
     - Optionales Behördenkennzeichen und ggf. ein optionaler Verwaltungsbezeichner.

2. Die Zertifikate werden bei der Abholung der Karte auf Veranlassung der Registrierungsstelle erzeugt, nachdem der Antragsteller identifiziert und die Korrektheit aller Daten durch ihn bestätigt wurde. Das Verfahren ist für Ausstellung, Verlängerung und Neuausstellung identisch.

3. Die eindeutige Zuordnung des Signatur- und Entschlüsselungszertifikats zum Zertifikatsinhaber ist sicher gestellt durch:

   - Einstellung des öffentlichen Schlüssel in ein Transport-Zertifikat der a.sign token (bzw. der a.sign Premium) Karte während der Kartenproduktion.
   - Übergabe der Karte an den Signator anlässlich der Registrierung.
   - Überprüfung der sichtbaren Kartendaten mit den Antragstellerdaten, insbesondere der Identifikationsnummer.
   - Auslesen des Transport-Zertifikats aus der a.sign token (bzw. 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 token Zertifikats nach Verknüpfung mit den Signatordaten.

4. Jedem Antragsteller wird eine innerhalb von a.trust einmalig vergebene und eindeutige Identifikationsnummer zugeordnet. Diese Identifikationsnummer ist Teil des hervorgehobenen Namens und stellt damit seine Eindeutigkeit sicher.

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

6. 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 und Zertifikaten die Bedingungen betreffend die Benutzung des a.sign token 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 token),

3. der Allgemeinen Geschäftsbestimmungen von a.trust,

4. der sonstigen Mitteilungen.

Änderungen werden dem Zertifikatsinhaber 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 das Folgende eindeutig festgelegt:

- a.sign token Zertifikate werden an die Öffentlichkeit ausgegeben (kein eingeschränkter Benutzerkreis) und sind an die Verwendung mittels einer Signaturerstellungseinheit (a.sign token bzw. a.sign Premium Karte) gebunden,
- der Signator erzeugt mit einem a.sign token Signaturschlüssel fortgeschrittene digitale Signaturen,
- die Verpflichtungen des Zertifikatsinhabers entsprechend Kapitel 2.2.
- die Vorgehensweise zur Überprüfung eines Zertifikats inklusive der Notwendigkeit der Überprüfung des Zertifikatsstatus, so dass der Überprüfer mit gutem Grund dem Zertifikat vertrauen kann (siehe Kapitel 2.3),
- wie ggf. ein den Umfang der Haftung einschränkendes Transaktionslimit in a.sign token Zertifikaten zu erkennen ist,
- die Zeitdauer für die Aufbewahrung von Registrierungsinformationen (siehe Kapitel 3.3.1),
- die Zeitdauer für die Aufbewahrung von Aufzeichnungen wichtiger die Zertifizierungsstelle betreffender Ereignisse (siehe Kapitel 3.4.11),
- die Tatsache, dass der Betrieb als Zertifizierungsdiensteanbieter der Aufsichtsstelle gemäß §6 [SigG] angezeigt wurde,
- Vorgehensweisen zur Behandlung von Beschwerden und Streitfällen,
- die Anwendbarkeit des [SigG] und [SigV].

3.3.5 Veröffentlichung der Zertifikate

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

1. Anlässlich der Erstellung eines Zertifikats wird dieses am Ende des Registrierungsvorgangs auf die a.sign token Karte (bzw. die a.sign Premium Karte) des Zertifikatsinhabers gespeichert.

2. Wenn der Zertifikatsinhaber 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 token" einfach herstellbar.

5. Der Verzeichnisdienst ist an sieben Tagen pro Woche jeweils 24 Stunden verfügbar. Unterbrechungen von mehr als 30 Minuten werden gemäß § 13 Abs. 5 [SigV] als Störfälle dokumentiert.

6. Die Verzeichnisdienste sind öffentlich und international zugänglich.

3.3.6 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 Vorgangsweise für das Auslösen von Sperre und Widerruf ist in der Zertifizierungsrichtlinie für a.sign token 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 Zertifikatsinhaber 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 Sperr- und Widerrufsanträgen beim Widerrufsdienst ist an die Kenntnis eines dafür eigens vorgesehenen Sperr- und Widerrufspass-

worts gebunden. In Ausnahmefällen (bei Sperre) können auch andere mit dem Zertifikatsinhaber verknüpfte Informationen zur Identifikation der Rechtmäßigkeit herangezogen werden. Bei der Aufhebung einer Sperre muss der Signator das bei der Durchführung der Sperre bekannt gegebene Sperraufhebungspasswort wissen und dem Mitarbeiter des Widerrufsdienstes mitteilen.

4. Beim Antrag auf Widerruf eines Zertifikats muss der Grund für den Widerruf angegeben werden.

5. Eine Sperre gilt, sofern sie nicht vorher aufgehoben wird, vom Zeitpunkt der Aufgabe bis 23:00 Uhr des neunten auf den Tag der Sperre folgenden Tags, an dem sie in einen Widerruf übergeführt wird.

6. Von der Durchführung eines Widerrufs oder einer Sperre wird der Zertifikatsinhaber von a.trust schriftlich verständigt.

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

8. 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.

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

   - Versionsnummer der CRL: Version 2 (codiert mit dem Wert 1)
   - Bezeichnung des Ausstellers
   - Zeitpunkt der CRL-Ausstellung sowie der nächsten geplanten Ausstellung
   - Informationen über die in der CRL enthaltenen Zertifikate:
     - Seriennummer,
     - Zeitpunkt der Eintragung in die CRL,
     - Eintragungsgrund

- CRL-Erweiterungen
- Angabe des Algorithmus für die Signatur über die CRL
- Signatur über die CRL.

10. Die Widerrufsdienste können jeden Tag jeweils 24 Stunden kontaktiert werden. Spätestens innerhalb von drei Stunden ab Bekanntwerden des Widerrufsgrundes erfolgt eine Aktualisierung der Widerrufsliste.

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

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

13. 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 Kartenproduktion. 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 token veröffentlicht.

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

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

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

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

3.4.2 Informationsklassifikation und -verwaltung

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

3.4.3 Personelle Sicherheitsmaßnahmen

Das Personal der a.trust und die 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 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 der administrativen und Management-Funktionen 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, das Verantwortung für sicherheitskritische Tätigkeiten trägt, verfügen.

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

7. Alle vertrauenswürdigen Positionen sind in der a.sign token Zertifizierungsrichtlinie im Detail beschrieben.

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

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

3.4.4 Physikalische und organisatorische Sicherheitsmaßnahmen

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

1. Der Zutritt zu den Räumlichkeiten, in denen Zertifizierungs- und Widerrufsdienste erbracht und in denen die Karten erstellt werden, ist auf autorisiertes Personal beschränkt. Die Systeme, welche Zertifikate ausstellen, sind vor Gefährdung durch Umweltkatastrophen geschützt.

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

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

4. Die Systeme für die Zertifikatsgenerierung, 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 sowie physischen Zutrittsschutz.

6. Die Sicherheitsmaßnahmen beinhalten den Gebäudeschutz, die Computersysteme selbst und alle sonstigen Einrichtungen, die für deren Betrieb unerlässlich sind. Der Schutz der Einrichtungen für die Zertifikatserstellung, Kartenproduktion und Bereitstellung der Widerrufsdienste umfasst physische Zutrittskontrolle, Abwendung von Gefahren durch Naturgewalten, Feuer, Rohr-

brüche und Gebäudeeinstürze, Schutz vor Ausfall von Versorgungseinheiten, sowie vor Diebstahl, Einbruch und Systemausfällen.

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

3.4.5 Betriebsmanagement

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

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

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

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

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

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

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

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

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

Sicherheitskritische Funktionen inkludieren:

1. Betriebliche Funktionen und Verantwortungen

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

Diese Aufgaben werden von a.trust-Sicherheitsbeauftragten geregelt, können aber von betrieblichem Personal (unter Beaufsichtigung) gem. Sicherheitskonzept und Stellenbeschreibungen durchgeführt werden.

3.4.6 Zugriffsverwaltung

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

1. Sicherungsmaßnahmen wie z. B. Firewalls bewahren das interne Netzwerk vor Zugriffen durch Dritte.
2. Vertrauliche Daten werden geschützt, wenn sie über unsichere Netzwerke ausgetauscht werden, wie z. B. die Registrierungsdaten.
3. Eine Benutzerverwaltung, die den verschiedenen Funktionen unterschiedliche Zugriffsrechte einräumt, ist eingerichtet; insbesondere werden sicherheitsrelevante Funktionen von unkritischen sauber getrennt. Änderungen in den Zugriffsrechten werden im System sofort nachgezogen. Die Kontrolle der Benutzerverwaltung ist Teil des internen Audits.
4. Zugriff auf Informationen und Anwendungen ist auf Grund der vergebenen Zugriffsrechte eingeschränkt. Die dafür geltenden Definitionen sind in der Zertifizierungsrichtlinie für a.sign token angeführt. Administrative und den Betrieb betreffende Funktionen sind streng getrennt. Die Verwendung von System-Utility-Programmen ist besonders eingeschränkt.
5. Das Personal muss sich vor jedem kritischen Zugriff auf Applikationen, die in Zusammenhang mit dem Zertifikatsmanagement stehen, authentifizieren.

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

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

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

9. Die Entdeckung von unautorisierten und/oder außergewöhnlichen Zugriffsversuchen auf die eigentliche Zertifizierungsstelle und die Widerrufsdienste wird durch geeignete Maßnahmen gesichert, sodass ggf. sofort Gegenmaßnahmen ergriffen werden können.

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

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

3.4.7 Entwicklung und Wartung vertrauenswürdiger Systeme

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

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

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

3.4.8 Erhaltung des ungestörten Betriebes und Behandlung von Zwischenfällen

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

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

2. Sollte dieser Fall eintreten, so hat a.trust die Aufsichtsstelle (siehe § 6 Abs 5 [SigG]), die Zertifikatsinhaber, die auf die Verlässlichkeit der Zertifizierungsdienste vertrauenden Personen und ggf. andere Zertifizierungsdiensteanbieter, mit denen Vereinbarungen bestehen, davon zu unterrichten und mitzuteilen, dass die Widerrufs- und Zertifikatsinformationen nicht mehr als zuverlässig anzusehen sind.

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

3.4.9 Einstellung der Tätigkeit

Gem. § 12 [SigG] wird a.trust die Einstellung der Tätigkeit unverzüglich der Aufsichtsstelle anzeigen und sicherstellen, dass eine eventuelle Beeinträchtigung ihrer Dienstleistungen sowohl gegenüber Zertifikatsinhabern als auch gegenüber allen auf die Zuverlässigkeit der a.trust-Dienste vertrauenden Parteien möglichst gering gehalten wird.

1. Vor Beendigung der Dienstleistung werden

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

   - die Verträge mit Subunternehmern (Registrierungsstellen, 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 Kapitel 3.2.6 deaktiviert.

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

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

   - für die Benachrichtigung der betroffenen Personen und Organisationen,

   - für die Übertragung der Verpflichtungen auf Dritt-Parteien und

- wie der Widerrufsstatus von nicht abgelaufenen Zertifikaten gehandhabt wird.

3.4.10 Übereinstimmung mit gesetzlichen Regelungen

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

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

2. Die Anforderungen des Datenschutzgesetzes werden befolgt.

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

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

3.4.11 Aufbewahrung der Informationen zu a.sign token Zertifikaten

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

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

2. Die Datensätze zu a.sign token Zertifikaten werden vollständig, vertraulich und in Übereinstimmung mit der veröffentlichten Zertifizierungsrichtlinie archiviert.

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

4. Die Aufzeichnungen umfassen auch den genauen Zeitpunkt des Eintretens wichtiger Ereignisse, die in Zusammenhang mit der Systemumgebung, dem Schlüssel- und dem Zertifikats-Management stehen.

5. Alle Daten, die in Zusammenhang mit a.sign token Zertifikaten stehen, werden, sofern nicht ausdrücklich ein anderer Zeitraum genannt wird, für mind. sieben Jahre elektronisch aufbewahrt. Der unterschriebene Signaturvertrag wird zusätzlich für drei Jahre in der betreffenden Registrierungsstelle im Original aufbewahrt.

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

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

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

9. Die aufzuzeichnenden Registrierungsinformationen beinhalten insbesondere:

   - die Art des Identifikationsdokuments, das anlässlich der Registrierung vorgelegt wurde,
   - die Daten des Identifikationsdokuments insbesondere dessen eindeutige Nummer,
   - die Akzeptanz der vertraglichen Vereinbarungen
   - vom Zertifikatsinhaber gewählte und akzeptierte Zertifikatsinhalte,
   - Angabe der Registrierungsstelle und des zuständigen Mitarbeiters.

10. Die Vertraulichkeit der Daten der Zertifikatsinhaber ist gewährleistet.

11. Es werden alle Ereignisse, die den Lebenszyklus der Schlüssel der 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 Zertifikatsinhaber stehen, aufgezeichnet.

14. Es werden alle Ereignisse, die im Zusammenhang mit der Erstellung der a.sign token Karte stehen, aufgezeichnet.

15. Alle Anträge auf Sperre, Sperraufhebung und Widerruf und die damit verbundenen Informationen werden aufgezeichnet.

3.5 Organisatorisches

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

3.5.1 Allgemeines

1. Alle Richtlinien und Vorgehensweisen sind nicht-diskriminierend.
2. Die Dienstleistungen von a.trust stehen allen volljährigen EU-Bürgern zur Verfügung.
3. a.trust ist eine juristische Person (Gesellschaft mit beschränkter Haftung).
4. a.trust verfügt über Systeme zur Qualitätssicherung und Gewährleistung der Informationssicherheit, die den angebotenen Zertifizierungsdiensten angemessen sind.
5. Hinsichtlich der finanziellen Ausstattung befolgt a.trust die Bestimmungen in § 2 [SigV].
6. Das von a.trust beschäftigte Personal verfügt entsprechend den Bestimmungen des [SigG] (siehe auch Kapitel 3.4.3) über die nötige Schulung, Training, technisches Wissen und Erfahrung und ist in ausreichender Zahl vorhanden, um den geplanten Umfang der Zertifizierungsdienste bewerkstelligen zu können.
7. Es sind Richtlinien und Vorgehensweisen für die Behandlung von Beschwerden und Streitfällen vorhanden, die von Kunden oder anderen Parteien an a.trust herangetragen werden und die Erbringung ihrer Dienstleistungen betreffen.
8. Die rechtlichen Beziehungen zu Subunternehmern, welche Dienstleistungen für a.trust erbringen, sind vertraglich geregelt und ausführlich dokumentiert.
9. Es gibt keine aktenkundigen Gesetzesverletzungen seitens a.trust.

3.5.2 Zertifikatserstellungs- und Widerrufsdienste

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

hängig von anderen Gesellschaften. Die Geschäftsführung und das Personal, welches sicherheitskritische und leitende Funktionen ausübt, ist frei von kommerziellem, finanziellem und sonstigem Druck, der das Vertrauen in ihre Tätigkeit negativ beeinflussen könnte.

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

4 Anhang

A Begriffe und Abkürzungen

a.sign token Karte	Eine Prozessorchipkarte, die geheime Schlüssel des Karteninhabers enthält und zur Erstellung und Verifizierung digitaler Signaturen dient.
a.sign token Zertifikat	Ein nicht qualifiziertes Zertifikat: ein Signatur- oder Verschlüsselungszertifikat, das auf einer a.sign token oder ein Verschlüsselungszertifikat, das auf einer a.sign Premium Karte basiert.
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 Teil eines Schlüsselpaares, der zum digitalen Signieren sowie zum Entschlüsseln von Nachrichten/Dokumenten erforderlich ist und geheim gehalten werden muss.
Public-Key System	Ein kryptographisches System, das ein Paar von durch einen mathematischen Algorithmus verbundenen Schlüsseln benutzt. Der öffentliche Teil dieses Schlüsselpaars kann jedermann zugänglich gemacht werden, der Informationen verschlüsseln oder eine digitale Signatur prüfen will, der geheime Teil wird von seinem Besitzer sicher bewahrt und kann Daten entschlüsseln oder eine digitale Signatur erstellen.
PUK	Personal Unblocking Key
Qualifiziertes Zertifikat	Zertifikat, welches den Bestimmungen lt. § 5 [SigG] entspricht.
Registrierungsstelle, Registration Authority, RA	Eine vertrauenswürdige Einrichtung, welche die Überprüfung der Identität der Zertifikatsbewerber im Namen des Zertifizierungsdiensteanbieters unter Berücksichtigung der Zertifizierungsrichtlinien durchführt und selbst keine Zertifikate ausstellt.
Schlüsselpaar	Ein privater Schlüssel und der dazugehörige öffentliche Schlüssel. Abhängig vom verwendeten Algorithmus kann man mit Hilfe des öffentlichen Schlüssels eine digitale Unterschrift, die mit dem dazu gehörigen privaten Schlüssel erstellt wurde, verifizieren bzw. mit dem privaten Schlüssel Daten entschlüsseln, welche mit dem zugehörigen öffentlichen Schlüssel verschlüsselt wurden.
Signator	Eine Person, die eine elektronische Signatur erstellt, Inhaber eines Signaturzertifikats
Signaturerstellungseinheit	Komponenten, die vom Unterzeichner verwendet werden, um eine elektronische Signatur zu erstellen.

SSL	Secure Socket Layer, ein Protokoll zur sicheren Übertragung von Daten über das Internet mit Hilfe eines Public-Key Systems.
Verifizierung (einer digitalen Signatur)	Feststellung, dass eine digitale Signatur mit dem privaten Schlüssel, der zu dem in einem gültigen Zertifikat beinhalteten öffentlichen Schlüssel gehört, erstellt wurde und die Nachricht sich nach der Signatur nicht verändert hat.
Widerruf	Der irreversible Vorgang der vorzeitigen Beendigung der Gültigkeit eines Zertifikats ab einem bestimmten Zeitpunkt.
X.509	Der ITU-Standard für Zertifikate. X.509 v3 beschreibt Zertifikate, die mit verschiedenen Zertifikatserweiterungen erstellt werden können
Zertifikats-Widerrufsliste, CRL	Eine digital signierte Datenstruktur, die widerrufene Zertifikate anführt, welche von einem bestimmten Zertifizierungsdiensteanbieter ausgestellt wurden.
Zertifizierungsdienste-anbieter, Certification Authority, CA	Eine Person oder Stelle, die Zertifikate ausstellt oder anderweitige elektronische Signaturdienste öffentlich anbieten darf.
Zertifizierungsrichtlinie	Siehe CPS

B Referenzdokumente

[SigG]	Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG). BGBl. I Nr. 190/1999 (NR: GP XX RV 1999 AB 2065 S. 180. BR: AB 6065 S. 657.)
[SigV]	Verordnung zum Signaturgesetz, BGBl II 2000/30, 02. 02. 2000 und BGBl. II Nr. 527/2004 vom 30.12.2004
[SigRL]	Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, 13. 12. 1999
[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 a.sign token
[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
[RFC3647]	RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003