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

a.trust

Certificate Policy
für einfache Zertifikate
a.sign MBS

Version: 1.0.1

Datum: 05.11.2003

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.

1.2 Identifikation

Name der Policy: a.trust Certificate Policy für einfache Zertifikate a.sign MBS

Version: 1.0.1/05.11.2003

Object Identifier: **1.2.040.0.17** (a.trust) **.1** (Policy) **.10.2** (a.sign MBS)
.1.0.1 (Version) vorliegende Version

Die vorliegende Policy stimmt mit den Anforderungen aus RFC 2527 (siehe [RFC2527]) überein.

1.3 Anwendungsbereich

Die a.sign MBS Policy gilt für einfache a.sign MBS Zertifikate entsprechend der Definition § 2 Abs. 8 [SigG], welche für einen geschlossenen Benutzerkreis im Rahmen des Multi Bank Standard ausgestellt werden. Die geheimen Schlüssel der Zertifikatsinhaber befinden sich auf deren Rechner.

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 MBS Zertifikate Beachtung fanden.

1.5 Berechtigung der Antragsteller

a.trust verfügt über eine Liste der berechtigten Personen, die mit entsprechender Authentifizierung die Ausstellung von MBS-Zertifikaten beantragen können. Wenn sich an diesem Personenkreis Änderungen ergeben (z. B. ein neuer Berechtigter wird eingemeldet), so kann dies formlos (mittels Fax, E-Mail oder Brief) an a.trust mitgeteilt werden. a.trust ist allerdings verpflichtet, für diese Änderungsmeldung eine telefonische Verifikation mit dem zuständigen Produktverantwortlichen vorzunehmen, damit ausgeschlossen werden kann, dass sich unbefugte Personen als MBS-Antragsteller anmelden.

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.

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

2.2 Verpflichtungen des Zertifikatsinhabers

a.trust bindet den Zertifikatsinhaber vertraglich an die Einhaltung der nachfolgend angeführten Verpflichtungen. Dem Zertifikatswerber werden die Vertragsbedingungen zugänglich gemacht und gleichzeitig mit der Bestellung bestätigt er deren Kenntnisnahme und Akzeptanz.

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 ordnungsgemäße Authentifizierung des Zertifikatswerbers mit einem bereits von a.trust ausgestellten persönlichen Zertifikat anlässlich der Bestellung des a.sign MBS-Zertifikats,

3. die Anwendung entsprechender Vorsicht, um den unbefugten Gebrauch des privaten Schlüssels zu verhindern und die sichere Vernichtung desselben nach Ablauf der Gültigkeitsperiode (ein Jahr),

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

- der private Schlüssel des Zertifikatsinhabers wurde möglicher Weise kompromittiert,
- die Kontrolle über den privaten Schlüssel ging verloren,
- die im Zertifikat beinhalteten Informationen sind inkorrekt oder haben sich geändert.

2.3 Verpflichtungen des Überprüfers von Zertifikaten

Ein Überprüfer, der ein a.sign MBS Zertifikat zur Verifizierung einer Signatur oder zur Durchführung einer Verschlüsselung verwendet, kann diesem nur dann vertrauen, wenn er

- eventuelle im Zertifikat oder den veröffentlichten Geschäftsbedingungen dargelegte Einschränkungen der Nutzung des Zertifikats beachtet (siehe dazu auch unten und Kapitel 1.3) und
- sämtliche anderweitig vorgeschriebene Vorsichtsmaßnahmen einhält.

2.4 Haftung

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

- für die Einhaltung der in dieser Certificate Policy festgelegten Richtlinien und die Einhaltung der Standards (ITU X.509) und
- dafür, dass ein a.sign MBS Zertifikat nur ausgestellt wird, nachdem sich der Zertifikatswerber zur Bestellung des a.sign MBS Zertifikats ordnungsgemäß mit einem von a.trust ausgestellten und an seine Person gebundenen Zertifikat authentifiziert hat.

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

3 Anforderung an die Erbringung von Zertifizierungsdiensten

Diese Policy ist auf die Erbringung von einfachen Zertifizierungsdiensten ausgerichtet. Dies umfasst die Bereitstellung von Registrierungsdiensten, Zertifikatserstellung und Zertifikatsausgabe.

3.1 Verlässlichkeit der Zertifizierungsdienste

a.trust hat die folgenden 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. a.trust macht den Zertifikatsinhabern und all jenen anderen Personen, die auf die Zuverlässigkeit des a.sign MBS Dienstes vertrauen, diese Policy zugänglich (siehe Kapitel 3.3.4).

3.2 Verwaltung der Schlüssel zur Erbringung von Zertifizierungsdiensten

3.2.1 Erzeugung der CA Schlüssel

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

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

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

3. Die Schlüssellänge und der Algorithmus wären ebenfalls für qualifizierte Zertifikate geeignet und entsprechen Anhang I [SigV].

3.2.2 Verteilung der öffentlichen CA Schlüssel

a.trust stellt durch die Ausstellung eines selbstsignierten Root-Zertifikats sicher, dass die Integrität und Authentizität der öffentlichen Schlüssel anlässlich der Verteilung gewahrt bleibt:

Das Zertifikat des CA Schlüssels zur Signatur von a.sign MBS Zertifikaten wird den Zertifikatsinhabern zugänglich gemacht. a.trust gewährleistet die Authentizität dieses Zertifikats.

3.2.3 Schlüsseloffenlegung

Eine Offenlegung der geheimen CA Schlüssel ist nicht vorgesehen.

3.2.4 Verwendungszweck von CA Schlüsseln

Der private Schlüssel der Zertifizierungsstelle wird nur für die Erstellung von a.sign MBS Zertifikaten innerhalb von physisch abgesicherten Räumlichkeiten verwendet.

3.2.5 Ende der Gültigkeitsperiode von CA Schlüsseln

Geheime Schlüssel zur Signatur von a.sign MBS Zertifikaten werden verwendet, solange die verwendeten Algorithmen den Sicherheitserwartungen entsprechen. Die Zertifikate über die Schlüssel der a.trust Zertifizierungsstelle werden alle fünf Jahre erneuert. Wenn die Algorithmen den Sicherheitserwartungen nicht mehr entsprechen, findet keine Erneuerung statt und die Schlüssel werden mit Erreichen des Endes der Gültigkeit gelöscht.

Eine Archivierung der geheimen Schlüssel ist nicht vorgesehen.

3.2.6 Erzeugung der Schlüssel für die Zertifikatsinhaber

Die Generierung der Schlüssel der Zertifikatswerber wird von diesen selbst in sicherer Weise vorgenommen.

a.trust erhält keine Kenntnis des privaten Schlüssels.

3.3 Lebenszyklus des Zertifikats

3.3.1 Registrierung des Zertifikatsinhabers

Die Maßnahmen zur Identifikation des Zertifikatsinhabers stellen sicher, dass der Antrag auf Ausstellung eines a.sign MBS Zertifikats autorisiert ist. Bei den Antragstellern handelt es sich um einen definierten Personenkreis, der mit einem a.sign Zertifikat eine Zugangsberechtigung zum Member Bereich der a.trust Web-Site hat.

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. Das Antragsformular ist über die Web-Seite von a.trust nach Authentifizierung elektronisch zugänglich.

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

   - den Namen des Zertifikatsinhabers (Common Name),
   - Organisation,
   - optional Organisationsuntereinheit,
   - optional E-Mailadresse,
   - die zu zertifizierende öffentliche Schlüsselkomponente (im PKCS#10-Format).

4. Der mit dem Antragsteller abzuschließende Vertrag beinhaltet insbesondere:

   - die Annahme der Verpflichtungen des Zertifikatsinhabers,
   - 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 Bestätigung der Korrektheit des Zertifikatsinhaltes.

5. Der Zertifikatsantrag und alle damit im Zusammenhang stehenden Daten und Dokumente werden auf die Dauer von mind. sieben Jahren nach Ablauf der Gültigkeit (elektronisch) archiviert.

6. Die Beachtung der Bestimmungen des Datenschutzgesetzes ([DSG]) ist durch die Prozesse, die seitens a.trust der Registrierungsstelle vorgeschrie-ben werden, sicher gestellt.

3.3.2 Neuausstellungen und Ausstellung

Es wird sicher gestellt, dass Anträge von Zertifikatswerbern vollständig, korrekt und ordnungsgemäß autorisiert sind. Die Maßnahmen gelten sowohl für Neuausstellung als auch für die Ausstellung nach Ablauf oder Widerruf eines Zertifikats.

1. Die Registrierungsstelle hat die im Zertifikat enthaltenen Daten 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.

3.3.3 Erstellung des Zertifikats

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

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

   - Versionsnummer des Zertifikats: es werden Zertifikate der Version 3 (codiert mit dem Wert 2) ausgestellt
   - Seriennummer des Zertifikats
   - Bezeichnung des Zertifikatsausstellers
   - Beginn und Ende der Gültigkeit des Zertifikats
   - Distinguished Name des Zertifikatsinhabers
     - Common Name
       Name des Zertifikatsinhabers

- E-Mailadresse: optional
- Organisation und optional eine Untereinheit der Organisation
- Land (AT)

- öffentlicher Schlüssel (mit Angabe des Algorithmus)
- Angabe des Algorithmus für die Signatur des Zertifikats
- Signatur über das Zertifikat
- Zertifikatserweiterungen, wie z. B.:
  - Information über die anzuwendende Policy
  - Zertifikatsverwendung

2. Die eindeutige Zuordnung des Zertifikats zum Zertifikatsinhaber ist sicher gestellt durch:
   - Erstellung des PKCS#10-Requests als Grundlage für die Zertifizierung durch den Antragsteller.
   - Erzeugung des Zertifikats nach Überprüfung der Berechtigung des Antragstellers durch a.trust.
3. Die in der Registrierungsstelle aufgenommenen Daten werden signiert und verschlüsselt (SSL) an die Zertifizierungsstelle übertragen. Vertraulichkeit und Integrität sämtlicher Daten sind damit sicher gestellt.

3.3.4 Bekanntmachung der Vertragsbedingungen

a.trust macht den Zertifikatsinhabern und den Benutzern, die auf die Zuverlässigkeit der a.trust Dienste vertrauen, die Bedingungen, welche die Benutzung des a.sign MBS Zertifikats betreffen, durch Veröffentlichung der folgenden Dokumente auf der a.trust Homepage zugänglich:

1. der gegenständlichen Certificate Policy,
2. der Allgemeinen Geschäftsbestimmungen von a.trust und
3. der sonstigen Mitteilungen.

Änderungen werden dem Zertifikatsinhaber mittels Bekanntmachung auf der a.trust Homepage oder auch individuell mitgeteilt.

In o. a. Dokumenten ist das Folgende eindeutig festgelegt:

- a.sign MBS Zertifikate werden an einen geschlossenen Benutzerkreis im Rahmen von MBS ausgegeben,
- die Verpflichtungen des Zertifikatsinhabers gem. Kapitel 2.2.
- die 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 MBS 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

a.sign MBS Zertifikate werden nicht im Verzeichnisdienst veröffentlicht.

3.3.6 Widerruf

Für a.sign MBS-Zertifikate werden keine Widerrufslisten (CRLs) erstellt.

3.4 a.trust Verwaltung

3.4.1 Sicherheitsmanagement

Es gelten die folgenden Bestimmungen:

1. a.trust ist für alle Prozesse im Rahmen der Zertifizierungsdienste verantwortlich; dies gilt auch für die an Vertragspartner ausgelagerten Dienste. Die Verantwortlichkeiten der Vertragspartner sind klar geregelt und Kontrollen zur Überprüfung der ordnungsgemäßen Tätigkeit eingerichtet.

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

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

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

5. Der Betrieb des Rechenzentrums ist an einen Vertragspartner ausgelagert. Auch dieser 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 auf das Folgende Wert gelegt:

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

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

3. Für alle Mitarbeiter von a.trust (unabhängig ob in einem temporären oder ständigen Beschäftigungsverhältnis angestellt) sind klare Stellenbeschreibungen

ausgearbeitet, in denen die Pflichten, Zugriffsrechte und Minimalkompetenzen dargelegt sind.

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

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

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

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

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

3.4.4 Physikalische und organisatorische 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 Zertifizierungsdienste erbracht 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 werden in einer gesicherten Umgebung betrieben, sodass eine Kompromittierung durch unautorisierte Zugriffe nicht möglich ist.

5. Die Abgrenzung der Systeme für die Zertifikatsgenerierung erfolgt durch klar definierte Sicherheitszonen, d. h. durch räumliche Trennung von anderen organisatorischen Einheiten sowie physischen Zutrittsschutz.

6. Die Sicherheitsmaßnahmen beinhalten den Schutz der Gebäude, der Computersysteme selbst und aller sonstigen Einrichtungen, die für deren Betrieb unerlässlich sind. Der Schutz der Einrichtungen für die Zertifikatserstellung umfasst physische Zutrittskontrolle, Abwendung von Gefahren durch Naturgewalten, Feuer, Rohrbrüche und Gebäudeeinstürze, Schutz vor Ausfall von Versorgungseinheiten sowie vor Diebstahl, Einbruch und Systemausfällen.

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

3.4.5 Betriebsmanagement

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

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

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

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

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

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

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

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

Die sicherheitskritischen Funktionen im Rahmen der Zertifizierungsdienste werden von den anderen (nicht sicherheitsrelevanten) Funktionen strikt getrennt.

Sicherheitskritische Funktionen beinhalten:

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

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

3.4.6 Zugriffsverwaltung

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

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

tionen 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 wird durch geeignete Maßnahmen gesichert, sodass ggf. sofort Gegenmaßnahmen ergriffen werden können.

3.4.7 Entwicklung und Wartung vertrauenswürdiger Systeme

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

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

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

3.4.8 Erhaltung des ungestörten Betriebes und Behandlung von Zwischenfällen

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

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

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

3.4.9 Einstellung der Tätigkeit

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

   - die privaten Schlüssel von a.trust von der Nutzung zurückgezogen.

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

3.4.10 Übereinstimmung mit gesetzlichen Regelungen

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

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

2. Die Anforderungen des Datenschutzgesetzes werden befolgt.

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

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

3.4.11 Aufbewahrung der Informationen zu a.sign MBS Zertifikaten

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

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

2. Alle Daten zu a.sign MBS Zertifikaten werden vollständig und vertraulich.

3. Aufzeichnungen, welche a.sign MBS 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 MBS Zertifikaten stehen, werden, sofern nicht ausdrücklich ein anderer Zeitraum genannt wird, für mind. sieben Jahre elektronisch aufbewahrt.

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

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

8. Die Vertraulichkeit der Daten der Zertifikatsinhaber ist gewährleistet.

9. Es werden alle Ereignisse, die den Lebenszyklus der Schlüssel von a.trust betreffen, aufgezeichnet.

10. Es werden alle Ereignisse, die den Lebenszyklus der Zertifikate betreffen, aufgezeichnet.

11. Alle Anträge auf Widerruf und die damit verbundenen Informationen werden aufgezeichnet.

3.5 Organisatorisches

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

3.5.1 Allgemeines

1. Alle Richtlinien und Vorgehensweisen sind nicht-diskriminierend.

2. Die Dienstleistungen von a.trust im Rahmen von a.sign MBS stehen einem geschlossenen Benutzerkreis 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 Zertifikatserstellungsdienste

Die für die Erbringung von Zertifizierungsdiensten vorgesehenen organisatorischen Einheiten sind hinsichtlich ihrer Entscheidungen über die Erbringung, Aufrechterhaltung und Beendigung der Dienstleistungen von a.trust unabhängig von anderen Gesellschaften. Die Geschäftsführung und das Personal, welches sicherheitskritische und leitende Funktionen ausübt, ist frei von kommerziellem, finanziellem und sonstigem Druck, der die Zuverlässigkeit ihrer Tätigkeit negativ beeinflussen könnte.

Die für die Zertifizierungsdienste bestimmten Einheiten verfügen über eine dokumentierte Struktur, die die Unvoreingenommenheit der Aufgabenausführung gewährleistet.

4 Anhang

A Begriffe und Abkürzungen

a.sign MBS Zertifikat	Ein nicht qualifiziertes Zertifikat, das für einen Server ausgestellt wird.
Certificate Policy, Policy	Ein Regelwerk, das den Einsatzbereich eines Zertifikates für eine bestimmte Benutzergruppe und/ oder Anwendungsklasse festhält.
Digitale Signatur	Elektronische Signatur, die mit Hilfe von Verfahren der asymmetrischen Kryptographie erzeugt wird.
E-Mail	Electronic Mail; Nachrichten, die in digitaler Form über computerbasierte Kommunikationswege versandt oder empfangen werden.
Elektronische Signatur	Eine Signatur in digitaler Form, die in Daten enthalten ist, Daten beigefügt wird oder logisch mit ihnen verknüpft ist und von einem Unterzeichner verwendet wird, um zu bestätigen, dass er den Inhalt dieser Daten billigt. Sie ist so mit den Daten verknüpft, dass eine nachträgliche Veränderung der Daten offenkundig wird.
Integrität (von Daten)	Ein Zustand, in dem Daten weder von Unbefugten verändert noch zerstört wurden.
Kompromittierung	Eine unautorisierte Offenlegung von oder der Verlust der Kontrolle über sicherheitskritische Informationen und geheim zu haltende Daten.
OCSP	Online Certificate Status Protocol
Öffentlicher Schlüssel	Öffentlicher Teil eines Schlüsselpaares. Er ist Bestandteil eines Zertifikates und wird zur Überprüfung von Digitalen Signaturen bzw. zur Verschlüsselung von Nachrichten/Daten verwendet.
Privater Schlüssel, Geheimer Schlüssel	Geheimer Teil eines Schlüsselpaares, der zum digitalen Signieren sowie zum Entschlüsseln von Nachrichten/Dokumenten erforderlich ist und geheim gehalten werden muss.
Public-Key System	Ein kryptographisches System, das ein Paar von durch einen mathematischen Algorithmus verbundenen Schlüsseln benutzt. Der öffentliche Teil dieses Schlüsselpaars kann jedermann zugänglich gemacht

	werden, der Informationen verschlüsseln oder eine digitale Signatur prüfen will, der geheime Teil wird von seinem Besitzer sicher bewahrt und kann Daten entschlüsseln oder eine digitale Signatur erstellen.
Qualifiziertes Zertifikat	Zertifikat, welches den Bestimmungen lt. § 5 [SigG] entspricht.
Registrierungsstelle, Registration Authority, RA	Eine vertrauenswürdige Einrichtung, welche die Überprüfung der Identität der Zertifikatsbewerber im Namen des Zertifizierungsdiensteanbieters durchführt und selbst keine Zertifikate ausstellt.
Schlüsselpaar	Ein privater Schlüssel und der dazugehörige öffentliche Schlüssel. Abhängig vom verwendeten Algorithmus kann man mit Hilfe des öffentlichen Schlüssels eine digitale Unterschrift, die mit dem dazu gehörigen privaten Schlüssel erstellt wurde, verifizieren bzw. mit dem privaten Schlüssel Daten entschlüsseln, welche mit dem zugehörigen öffentlichen Schlüssel verschlüsselt wurden.
Signaturerstellungseinheit	Komponenten, die vom Unterzeichner verwendet werden, um eine elektronische Signatur zu erstellen.
SSL	Secure Socket Layer, ein Protokoll zur sicheren Übertragung von Daten über das Internet mit Hilfe eines Public-Key Systems.
Verifizierung (einer digitalen Signatur)	Feststellung, dass eine digitale Signatur mit dem privaten Schlüssel, der zu dem in einem gültigen Zertifikat beinhalteten öffentlichen Schlüssel gehört, erstellt wurde und die Nachricht sich nach der Signatur nicht verändert hat.
Widerruf	Der irreversible Vorgang der vorzeitigen Beendigung der Gültigkeit eines Zertifikats ab einem bestimmten Zeitpunkt.
X.509	Der ITU-Standard für Zertifikate. X.509 v3 beschreibt Zertifikate, die mit verschiedenen Zertifikatserweiterungen erstellt werden können
Zertifizierungsdiensteanbieter, Certification Authority, CA	Eine Person oder Stelle, die Zertifikate ausstellt oder anderweitige elektronische Signaturdienste öffentlich anbieten darf.

B Referenzdokumente

[SigG]	Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG). BGBl. I Nr. 190/1999 (NR: GP XX RV 1999 AB 2065 S. 180. BR: AB 6065 S. 657.)
[SigV]	Verordnung zum Signaturgesetz, BGBl II 2000/30, 02. 02. 2000
[SigRL]	Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, 13. 12. 1999
[DSG]	Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000). BGBl. I Nr. 165/1999 (NR: GP XX RV 1613 AB 2028 S. 179. BR: 5992 AB 6034 S. 657.)
[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
[RFC2527]	RFC 2527, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, March 1999