A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Zahlungsverkehr 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

Sicherheits- und Zertifizierungskonzept a.sign Uni

Version: 1.3.2

Datum: 25.11.2002

Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH.
A-1030 Wien, Landstraßer Hauptstraße 5

VORWORT

Unter der Marke a.sign bietet a.trust Gesellschaft für Sicherheitsssteme im elektronischen Datenverkehr unterschiedliche Zertifikate an:

Zertifikate:

User Zertifikate: werden ausschließlich für natürliche Personen ausgestellt. Die Überprüfung der Zertifikatswerber erfolgt je nach Zertifikatsklasse (a.sign Projects mit den Varianten Light und Strong; a.sign Uni).

Nachfolgende Ausführung betreffen ausschließlich den Bereich der User-Zertifikate. Die wesentlichsten Unterschiede innerhalb der Zertifikatsklassen bestehen

1. in der rechtlichen Wirksamkeit und im Einsatzbereich

   a.sign Zertifikate Projects werden in den Varianten Light und Strong ausgegeben: Diese stellen einfache Zertifikate im Sinne des Österreichischen Signaturgesetzes dar. Eine elektronische Signatur auf Basis eines Zertifikates a.sign Projects wird in den Rechtswirkungen nicht der eigenhändigen Unterschrift gleichgestellt. Diese Zertifikate dürfen zum elektronischen Signieren von Nachrichten und Dokumenten, zur Verschlüsselung von Nachrichten und Dokumenten sowie zur Authentisierung in Netzen verwendet werden.

   Für die Varianten Light und Strong wurden jeweils eigene Policies erstellt. Das dazugehörige Certification Practice Statement und die Policies sind im Informationsdienst unter http://www.a-trust.at/ öffentlich verfügbar.

   Das a.sign Uni Zertifikat entspricht den Anforderungen des Österreichischen Signaturgesetzes an ein qualifiziertes Zertifikat und ermöglicht unter Einhaltung bestimmter Bedingungen die Erstellung einer sicheren elektronischen Signatur. Nur die sichere elektronische Signatur entfaltet die Rechtswirkungen der eigenhändigen Unterschrift im Sinne des Österreichischen Signaturgesetzes.

   Das a.sign Uni Zertifikat darf ausschließlich zur Erstellung sicherer elektronischer Signaturen verwendet werden.

2. in der Art und Weise der Identitätsüberprüfung der Zertifikatswerber und der Generierung und Speicherung der privaten Schlüssel

   Die Überprüfung der Zertifikatswerber bei a.sign Zertifikaten Projects (=einfache Zertifikate) erfolgt

   - Light: online Überprüfung der E-Mail-Adresse
   - Strong: persönlich anhand eines amtlichen Lichtbildausweises in der lokalen Registrierungsstelle

Der private Schlüssel kann auf einem vom Zertifikatswerber frei wählbaren Medium (z.B. Festplatte) gespeichert werden. Der private Schlüssel ist durch ein Passwort bzw. eine PIN zu schützen.

- Qualifizierte Zertifikate:
  a.sign Uni Zertifikate werden ausschließlich nach persönlicher Überprüfung der Identität des Zertifikatswerbers mittels eines amtlichen Lichtbildausweises ausgestellt. Die Ausgabe des Zertifikates erfolgt in Verbindung mit einer Chipkarte. Die Generierung des privaten Schlüssels erfolgt auf dem Chip - der private Schlüssel verlässt diesen Chip nicht. Der Schutz des privaten Schlüssels wird durch eine 8-stellige PIN gesichert.

Das vorliegende a.sign Sicherheits- und Zertifizierungskonzept für a.sign Uni Zertifikate wurde auf Basis der Policy für den Signatur- und Zertifizierungsdienst a.sign Uni der a.trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH entwickelt und gilt ausschließlich für a.sign Uni Zertifikate.

BEACHTEN SIE: Ausschließlich a.sign Uni Zertifikate entsprechen qualifizierten Zertifikaten im Sinne des Österreichischen Signaturgesetzes. Der Verwendungszweck dieses Zertifikates ist auf die Erstellung sicherer elektronischer Signaturen beschränkt. Die Verschlüsselung und/oder Authorisierung mit einem a.sign Uni Zertifikat ist verboten.

ZUSAMMENFASSUNG

Diese Zusammenfassung dient ausschließlich dazu, dem Leser einen ersten Überblick über dieses Dokument zu geben. Bezüglich der Details und anderer wichtiger, in dieser Zusammenfassung nicht angesprochener Themen wird der Leser auf die nachfolgenden Kapitel des Sicherheits- und Zertifizierungskonzept verwiesen.

- Dieses Sicherheits- und Zertifizierungskonzept regelt die Implementierung der angebotenen a.sign Zertifizierungs-dienstleistungen im Bereich der a.sign Uni Zertifikate (Beantragung, Ausstellung, Abholung, Gebrauch, Verlängerung und Widerrufen eines *Zertifikates* usw.) durch die a.sign *Certification Authority Uni.*

- Nur a.sign Uni Zertifikate entsprechen qualifizierten Zertifikaten im Sinne des Österreichischen Signaturgesetzes.

- Nur eine mittels eines a.sign Uni-Zertifikates unter Einhaltung der vom Zertifizierungsdiensteanbieter geforderten Bedingungen erstellte elektronische Signatur, gilt als sichere elektronische Signatur im Sinne des Österreichischen Signaturgesetzes und führt zur Gleichstellung mit der eigenhändigen Unterschrift im Sinne dieses Gesetzes (Beachte: einzelne Teilbereiche z.B. Bürgschaften sind von dieser Gleichstellung ausgenommen; vgl. § 4 Abs. 2 öSigG)

- Mit einem a.sign Uni Zertifikat dürfen ausschließlich sichere elektronische Signaturen erstellt werden. Die Verschlüsselung und/oder Authentisierung mit einem a.sign Uni Zertifikat ist untersagt.

- Allgemeines Informationsmaterial über die Themen *Digitale Signatur*, *Zertifikate*, *Öffentliche* und *Private Schlüssel* usw. wird vom Support des Zertifizierungsdiensteanbieters a.trust angeboten.

- Das Schlüsselpaar (bestehend aus Öffentlichem und Privatem Schlüssel) wird in der lokalen Registrierungsstelle unter Aufsicht des Zertifikatswerbers generiert. Der Private Schlüssel muss vom Zertifikatswerber durch Vergabe einer PIN geschützt werden.

- Jedem Empfänger einer *Digitalen Signatur* (*Dritter*) wird empfohlen, die *Digitale Signatur* bzw. das zugehörige *Zertifikat* zu überprüfen, bevor er der *Digitalen Signatur* bzw. dem *Zertifikat* vertraut.

- In bestimmten Fällen müssen *Signatoren* oder die *Certification Authority* das *a.sign Uni Zertifikat* widerrufen. Die zulässigen Verfahren für den Widerruf eines *Zertifikates a.sign Uni* sowie für die Veröffentlichung widerrufener *a.sign Uni Zertifikate* werden in diesem Sicherheits- und Zertifizierungskonzept definiert.

- Dieses Sicherheits- und Zertifizierungskonzept regelt zusätzlich Bereiche im Umfeld des eigentlichen Zertifizierungsprozesses, wie beispielsweise Haftungsfragen, die rechtliche Bedeutung von *Zertifikaten,* Entgelte, interne Kontrollen, Datenschutz, Urheberrechte, Behandlung von Ausnahmesituationen, Sicherheitsmaßnahmen, Profil von *a.sign Zertifikaten* sowie die Administration dieses Sicherheits- und Zertifizierungskonzepts.

Inhaltsverzeichnis

Tabellenverzeichnis

1 Einführung

Dieses Kapitel gibt dem Leser einen Überblick über das vorliegende Dokument und beschreibt die Einheiten, die am a.sign Zertifizierungsdienst a.sign Uni beteiligt sind, sowie die Einsatzmöglichkeiten der ausgestellten Zertifikate Uni.

1.1 Überblick

1.1.1 Ziel dieses Dokumentes

Das Ziel des vorliegenden a.sign Sicherheits- und Zertifizierungskonzepts besteht darin, die Umsetzung der Ausgabe, Administration und Anwendung von Zertifikaten a.sign Uni derart festzulegen, dass eine sichere und zuverlässige Durchführung der angebotenen Zertifizierungsdienstleistung a.sign Uni sowie der Anwendung der ausgegebenen Zertifikate gewährleistet ist.

1.1.2 Verhältnis des a.sign Sicherheits- und Zertifizierungskonzept zu den restlichen a.sign Dokumenten

Die Policies für Zertifikate a.sign Projects in den Varianten Light und Strong sowie das Certification Practice Statement für a.sign Projects regeln ausschließlich den Bereich der einfachen Zertifikate im Sinne des Österreichischen Signaturgesetz.

a.sign Uni Zertifikate werden ausschließlich durch nachfolgend angeführte Dokumente geregelt. Die Dokumente der Zertifizierungsdienstleistung a.sign Projects bilden aufgrund ihrer Funktionen eine 3-stufige Hierarchie (siehe nachstehende Abbildung):

- Die Policy a.sign Uni enthält die globalen Richtlinien, die von den Service-Betreibern und Signatoren einzuhalten sind.
- Das Sicherheits- und Zertifizierungskonzept für a.sign Uni Zertifikate der Certification Authority Uni enthält Angaben darüber, wie die in der Policy a.sign Uni enthaltenen globalen Richtlinien von der CA a.sign Uni umgesetzt werden. Das vorliegende Dokument enthält die Umsetzung der Policy a-sign Uni durch die CA a-sign Uni.

- Die Operation Quality Assurance Documents dienen der internen Qualitätssicherung. Da sie internes Know-How bzw. detaillierte Beschreibungen der Vorgänge und Strukturen, auf denen der Signatur- und Zertifizierungsdienst beruht, enthalten, werden sie nicht der Öffentlichkeit zugänglich gemacht.

1.1.3 Beziehung zwischen Zertifikat und a.sign Sicherheits- und Zertifizierungskonzept für a.sign User Zertifikate Uni

Das a.sign Uni Zertifikat enthält Verweise auf die entsprechende Policy a.sign Uni sowie auf dieses Sicherheits- und Zertifizierungskonzept, so dass dem Anwender des Zertifikates die Möglichkeit eingeräumt wird, sich darüber zu informieren, welche Richtlinien bzw. Realisationen dem a.sign Uni Zertifikat zugrunde liegen und ob das Zertifikat den Erfordernissen des geplanten Verwendungszwecks genügt.

1.1.4 Beziehung zwischen den Allgemeinen Geschäftsbedingungen und dem a.sign Sicherheits- und Zertifizierungskonzept

Dieses Sicherheits- und Zertifizierungskonzept stellt eine Erweiterung der Allgemeinen Geschäftsbedingungen der a.trust dar. Die Informationen über diese Allgemeinen Geschäftsbedingungen finden Sie auf folgender Webseite:
http://www.a-trust.at.

1.2 Identifikation des Sicherheits- und Zertifizierungskonzepts

Name des CPS: a.sign Sicherheits- und Zertifizierungskonzept / Version 1.3.2.

1.3 a.sign Zertifizierungsinfrastruktur

Informationen über die a.sign Signatur- und Zertifizierungsdienste befinden sich im Web unter der folgenden Webadresse: http://www.a-trust.at/.

1.3.1 Einheiten der a.sign Zertifizierungsinfrastruktur

Dieser Abschnitt beschreibt die einzelnen Komponenten der a.sign Zertifizierungshierarchie und stellt die hierarchischen Beziehungen dieser Komponenten zueinander dar.

1.3.1.1 CA

Die CA stellt a.sign Uni Zertifikate für Signatoren aus und ist für das Management von Zertifikaten für Signatoren verantwortlich.

Das a.sign Sicherheits- und Zertifizierungskonzept legt die Richtlinien der CA a.sign Uni dar.

1.3.1.2 GRAs

Die Globale Registrierungsstelle (GRA) ist der CA zugeordnet. Sie ist für die Archivierung der Registrierungsdaten, die ihr übermittelt werden, verantwortlich und führt gegebenenfalls zusätzliche Überprüfungen dieser Daten durch.

1.3.1.3 LRAs

Die Lokalen Registrierungsstellen (LRAs) führen im Auftrag der übergeordneten CA a.sign Uni die Registrierung und Überprüfung von Zertifikatswerber-Daten durch.

1.3.1.4 Signatoren

Signatoren von Zertifikaten a.sign Uni sind ausschließlich natürliche Personen.

1.3.1.5 a.sign Informationsdienst

Der a.sign Informationsdienst stellt Zertifikatsverzeichnisse, Widerrufslisten, die a.sign Richtlinien sowie andere relevante Informationen bezüglich der a.sign Services online und öffentlich zugänglich zur Verfügung.

Auf den a.sign Informationsdienst kann man unter der folgenden Web-Adresse zugreifen: http://www.a-trust.at.

1.4 Kontaktinformation

1.4.1 Zertifizierungsdiensteanbieter a.trust

Kontaktinformationen bzgl. des a.sign Zertifizierungsdienstеanbieters finden Sie in folgender Tabelle:

Firmenname:	A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH
Adresse:	A-1030 Wien Landstraßer Hauptstraße 5
Telefon:	0900/833 201
Web:	http://www.a-trust.at
Widerruf	01/501 45 – 1354 (Mo:00:00 bis Sonntag 24:00)

Tabelle 1 Kontaktinformationen

1.4.2 a.trust Web-Schnittstellen

Unter der Web-Adresse http://www.a-trust.at/ bietet a.sign Informationen über folgende Themen an:

Zertifizierungsinstanzen

Allgemeine Information	*Zertifizierungsdienst*	*Informationsdienst *)*
Information über a.sign Produkte Digitale Signatur Anwendung von Zertifikaten Support	Zertifizierung Zertifikat-Erneuerung Zertifikat-Widerruf	a.sign Verzeichnisdienst a.sign Widerrufslisten a.sign Richtlinien

Tabelle 2 Web-Schnittstellen

Anmerkung zum a.sign Informationsdienst

a) Verzeichnisdienst

online-Abfrage der User Zertifikate allg:

http://a-sign.datakom.at/servlet/X500Servlet?func=searchUserCert

https://a-sign.datakom.at/servlet/X500Servlet?func=searchUserCert

UserCRL (im DER und BASE 64-Format):

http://a-sign.datakom.at/servlet/X500Servlet?func=downloadUserCRL

https://a-sign.datakom.at/servlet/X500Servlet?func=downloadUserCRL

LDAP-Server:
extern erreichbar über a-sign.datakom.at; Port (Standard LDAP) 389

Secure LDAP-Server:
extern erreichbar über a-sign.datakom.at; Port (Standard LDAPS) 636

b) Richtlinien

- Policies Light und Strong; Certfication Practice Statement: Bereich der einfachen Zertifikate.
- a.sign Uni Policy, a.sign Uni Sicherheits- und Zertifizierungskonzept und Zertifikatswerber-Vertrag: Bereich der qualifizierten Zertifikate

2 Allgemeine Richtlinien

In diesem Kapitel wird dem Leser ein Überblick über die allgemeinen Grundlagen der angebotenen Signatur- und Zertifizierungsdienste gegeben.

2.1 Pflichten

2.1.1 Verpflichtungen einer a.sign Uni CA

2.1.1.1 Allgemeine Verpflichtungen

Die CA a.sign Uni hält die Richtlinien des Zertifizierungsdienstes a.sign Uni ein. Dies bedeutet insbesondere, dass die CA

- die in der Policy a.sign Uni sowie in diesem Sicherheits- und Zertifizierungskonzept spezifizierten Identifikations- und Authentifikations-Mechanismen sicherstellt,
- Zertifikate für Signatoren gemäß der Policy a.sign Uni sowie gemäß dem Sicherheits- und Zertifizierungskonzept ausstellt,
- Zertifikate für Signatoren gegebenenfalls widerruft,
- den Publikations- und Informationspflichten nachkommt und
- die Aktivitäten der ihr zugeordneten GRA und der ihr unterstellten LRAs überwacht.

2.1.1.2 Schutz des Privaten Schlüssels der CA

Die CA a.sign Uni sorgt durch geeignete organisatorische, infrastrukturelle, personelle und sicherheitstechnische Maßnahmen für den Schutz des Privaten Schlüssels der CA a.sign Uni.

2.1.1.3 Verwendung des Privaten Schlüssels der CA a.sign Uni

Der Private Schlüssel der CA wird ausschließlich zum Signieren von Zertifikaten für Signatoren und zum Signieren von Widerrufslisten eingesetzt.

2.1.1.4 Implementierung eines Sicherheitskonzeptes

Entsprechend den Abschitten 7 und 8 dieses Sicherheits- und Zertifizierungskonzept wird von der CA a.sign Uni ein Sicherheitskonzept entwickelt und implementiert.

2.1.1.5 Publikation / Information

Ausgestellte Zertifikate werden gemäß dem Sicherheits- und Zertifizierungskonzept a.sign Uni veröffentlicht. Zertifikatswerber werden von einer erfolgten Ausstellung des Zertifikates in Kenntnis gesetzt.

Widerrufene Zertifikate werden entsprechend dem Sicherheits- und Zertifizierungskonzept in Form von CRLs veröffentlicht. Zertifikatinhaber werden von einem erfolgten Widerruf ihres Zertifikates in Kenntnis gesetzt.

2.1.2 Verpflichtungen von a.sign GRAs

Die GRA erfüllt die von der zugeordneten CA a.sign Uni spezifizierten Sicherheitsanforderungen.

Die GRA führt die im Zuge der Registrierungs- und Authentifizierungsverfahren anfallenden, von der a.sign Uni CA festgelegten Überprüfungs-, Protokollierungs- und Archivierungs-aufgaben durch.

2.1.3 Verpflichtungen von a.sign LRAs

Die LRAs erfüllen die von der übergeordneten CA a.sign Uni spezifizierten Sicherheitsanforderungen.

Die LRAs halten die von der übergeordneten CA a.sign Uni festgelegten Richtlinien bzgl. der Registrierungs- und Authentifizierungsverfahren ein.

2.1.4 Verpflichtungen von Signatoren

2.1.4.1 Allgemeine Verpflichtungen

Signatoren sind verpflichtet,

- für die Richtigkeit der angegebenen Daten im Rahmen der Registrierung Sorge zu tragen und
- die Verfahren zur Identifizierung und Authentifizierung gemäß der ausstellenden CA a-sing Uni in diesem Zertifizierungskonzept festgelegten Richtlinien einzuhalten.

2.1.4.2 Schutz des Privaten Schlüssels

Signatoren sind verpflichtet,

- den Privaten Schlüssel mittels einer PIN zu schützen, d.h. den Zugriff anderer Personen auf den Privaten Schlüssel zu unterbinden,
- die Weitergabe der PIN zu unterlassen,
- die Chipkarte sorgsam zu verwahren und vor Zugriffen Dritter zu schützen sowie
- ausgestellte Zertifikate zu widerrufen, falls die Notwendigkeit dazu gegeben ist.

2.1.4.3 Einschränkungen bezüglich der Anwendung Privater Schlüssel bzw. ausgestellter Zertifikate

Signatoren ist es untersagt, selbst Zertifikate auszustellen.

a.sign Uni Zertifikate dürfen nur zur Erstellung einer sicheren elektronischen Signatur verwendet werden.

Für a.sign Uni Zertifikate gilt jene Version der Policy bzw. des Sicherheits- und Zertifizierungskonzepts, die zum Zeitpunkt der Ausstellung des Zertifikates gültig war.

2.1.5 Signaturprüfung - Anwender/Empfänger elektronischer Signaturen

Grundsätzlich kann der Anwender (=Empfänger) einer elektronischen Signatur nicht zur sicheren Signaturprüfung verpflichtet werden (analog zur eigenhändigen Unterschrift). Der Empfänger hat diesbezüglich Wahlfreiheit. Das bedeutet, dass der Empfänger entscheiden kann, ob er die Signatur sicher verifizieren will oder ausschließlich eine Plausibilitätskontrolle vornimmt. Will der Empfänger die sichere Signaturprüfung vornehmen, so hat er jedenfalls ein vom Zertifizierungsdienste-

anbieter empfohlenes Signaturprodukt (Liste wird im a.sign Web veröffentlicht) zu verwenden sowie die Gültigkeit des Zertifikates durch Überprüfung im Verzeichnis- oder Widerrufsdienst vorzunehmen.

2.1.6 Verpflichtungen des a.sign Informationsdienstes

Der Informationsdienst veröffentlicht im Auftrag der CAs die im Punkt 2.5 spezifizierten Informationen (Richtlinien, Zertifikatsverzeichnisse, Widerrufslisten und Informationen zur Unterrichtung von Signatoren) unter den dort angeführten Bedingungen und unter den im Punkt 2.6 festgelegten Einschränkungen (Datenschutz).

2.2 Haftung

Die Haftungsregelungen im Zusammenhang mit Zertifizierungsdienstleistungen a.sign Uni entsprechen den Haftungserfordernissen des Österreichischen Signaturgesetzes und der auf dessen Grundlage ergangenen Verordnungen an qualifizierte Zertifikate resp. sichere elektronische Signaturen (siehe dazu auch nachfolgendes Kapitel 2.3).

2.3 Rechtliche Hinweise

Der Antrag auf Ausstellung eines Zertifikates a.sign Uni erfolgt in der lokalen Registrierungsstelle. Der Zertifikatswerber-Vertrag wird vom Zertifikatswerber eigenhändig unterschrieben. Mit Unterfertigung des Zertifikatswerber-Vertrages erklärt sich der Zertifikatswerber mit den Bedingungen des Zertifizierungsdienstanbieters einverstanden.

a.sign Uni Zertifikate erfüllen die Anforderungen des Österreichischen Signaturgesetzes und der auf dessen Grundlage ergangenen Verordnungen an ein qualifiziertes Zertifikat und ermöglichen unter gewissen Voraussetzung die Erstellung einer sicheren elektronischen Signatur, die der eigenhändigen Unterschrift im Sinne des Österreichischen Signaturgesetzes gleichgestellt wird. Im Rahmen der Antragstellung wird der Zertifikatswerber schriftlich entsprechend den Vorschriften des Österreichischen Signaturgesetzes unterrichtet.

2.4 Entgelte

Die Entgelte für die angebotenen Dienstleistungen werden von der a.trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH festgelegt. Die aktuellen Entgelte sind dem Informationsdienst zu entnehmen.

Folgende Services der a.sign CAs sind kostenlos:

- Ausgabe und Bezug von CRLs,
- die Veröffentlichung dieses Sicherheits- und Zertifizierungskonzepts ausgenommen Selbstkosten bei einer Ausgabe auf entsprechenden Medien.

2.5 Veröffentlichungen

2.5.1 Veröffentlichte Inhalte

Die CA a.sign Uni ist für die Veröffentlichung folgender Inhalte verantwortlich:

2.5.1.1 Richtlinien für eine CA a.sign Uni

Dieses Sicherheits- und Zertifizierungskonzept wird in der aktuellen und allen vorangegangenen Versionen durch den Informationsdienst via Web veröffentlicht.

2.5.1.2 Zertifikatsverzeichnisse

Die von CA a.sign Uni ausgestellten Zertifikate für Signatoren werden im Verzeichnisdienst veröffentlicht. Für jedes Zertifikat wird der aktuelle Status angegeben, wobei folgende Attribute vorgesehen sind:

Status	Bedeutung
valid	Das Zertifikat ist gültig.
revoked	Das Zertifikat wurde revoziert.
expired	Die Gültigkeit des Zertifikates ist abgelaufen.

Tabelle 3 Statusinformationen

Bei Zertifikaten, die widerrufen wurden (Status *revoked*), wird auch der Zeitpunkt des Widerrufes angegeben.

Zertifikate werden mindestens so lange im Verzeichnisdienst geführt, wie der im Zertifikat aufgeführte Algorithmus mit den dazugehörigen Parametern als geeignet beurteilt wird.

2.5.1.3 Widerrufslisten (CRLs)

Widerrufe von Zertifikaten werden mittels Widerrufslisten (CRLs) vom Verzeichnisdienst veröffentlicht. Widerrufene Zertifikate werden mindestens solange in den CRLs geführt, bis die ursprüngliche Gültigkeitsdauer des Zertifikates überschritten ist.

CRLs für a.sign Uni Zertifikate werden jedenfalls innerhalb der im Gesetz genannten Geschäfts- und Widerrufszeiten aktualisiert. Zertifikatsinhaber werden über einen erfolgten Widerruf informiert.

2.5.1.4 Unterrichtung von Signatoren

Zertifikatswerber werden über den Umgang mit Zertifikaten a.sign Uni, den Umgang mit ihrem Privaten Schlüssel, den Schutz ihres Privaten Schlüssels und die Prüfung von Digitalen Signaturen unterrichtet.

Die Unterrichtung des Zertifikatswerbers erfolgt bei Zertifikaten a.sign Uni in der lokalen Registrierungsstelle durch Übergabe eines dauerhaften Datenträgers.

2.5.2 Durchführung von Veröffentlichungen

Die a.sign CAs beauftragen den a.sign Informationsdienst mit der Veröffentlichung der in Kapitel 2.5.1 angeführten Inhalte. Der a.sign Informationsdienst ist rund um die Uhr unter folgender Web-Adresse zugänglich: http://www.a-trust.at.

2.6 Datenschutz

2.6.1 Vertrauliche Daten

2.6.1.1 Typen vertraulicher Daten

Als vertrauliche Daten gelten

- alle persönlichen Daten bzw. Organisations-Daten, die nicht in den ausgestellten Zertifikaten enthalten sind,
- Protokolldaten, die beim Beantragen, Verlängern und Widerrufen von Zertifikaten usw. archiviert wurden, sowie
- Auditdaten, die internes Know-How wiederspiegeln.

2.6.1.2 Behandlung vertraulicher Daten

Die Veröffentlichung oder Weitergabe vertraulicher Daten ist unzulässig und erfolgt nur mit expliziter Zustimmung des betroffenen Zertifikatinhabers oder durch behördliche Anordnung auf Grund geltender Gesetze und Befugnisse.

Sämtliche Zertifikatinhaber stimmen der internen Speicherung und Verarbeitung ihrer erfassten Daten durch die CA a.sign Uni zu.

2.6.2 Zu veröffentlichende Daten

2.6.2.1 Typen von zu veröffentlichenden Daten

Als zu veröffentlichende Daten gelten

- alle Zertifikatinhalte, vorbehaltlich der Zustimmung des Zertifikatsinhabers sowie
- CRLs.

2.6.2.2 Behandlung von zu veröffentlichenden Daten

Die CA a.sign Uni ist zur Veröffentlichung aller Zertifikatinhalte berechtigt.

Die CA a.sign Uni ist zur Veröffentlichung der Widerrufe von Zertifikaten berechtigt.

3 Identifizierung, Authentifizierung

3.1 Erstregistrierung

3.1.1 Identifikationsmerkmale

3.1.1.1 CA a.sign Uni

Die CA a.sign wird durch folgende Namensstruktur eindeutig definiert:

- Common Name (CN)
- Organizational Unit (OU)
- Organization (O)
- Country (C)

3.1.1.2 Signatoren

Ein a.sign Uni Zertifikat enthält jedenfalls folgende persönliche Identifikationsmerkmale des Zertifikatsinhabers: Vor- und Nachname des Zertifikatsinhabers.

3.1.1.3 Zulässige amtliche Lichtbildausweise

Die für eine persönliche Registrierung eines Signators zugelassenen Ausweise sind im Abschnitt 4.1.2 spezifiziert.

3.1.1.4 Zusätzlich erfasste Daten für interne Ablage

Die zusätzlich für die interne Ablage erfassten Daten können dem Abschnitt 4.1.1 (Enrollment-Daten) entnommen werden.

3.1.2 Eindeutigkeit der Identifikationsmerkmale

Die in den Zertifikaten angeführten Identifikationsmerkmale enthalten keinen eindeutigen Identifier (Sozialversicherungsnummer o.ä.), d.h. der Zertifikatsinhaber

kann aufgrund dieser Merkmale nicht eindeutig identifiziert werden. Eine eindeutige Zuordnung ist über die Seriennummer möglich.

3.1.3 Nachweis des Besitzes des Privaten Schlüssels

Der Nachweis des Privaten Schlüssels erfolgt indirekt. Es erfolgt ein Vergleich des Public Keys der Chipkarte mit dem Public Key im a.sign Uni Zertifikat.

3.1.4 Identitätsüberprüfung bei Zertifikaten a.sign Uni

- Für die Überprüfung/Registrierung ist das persönliche Erscheinen des Zertifikatswerbers in der lokalen Registrierungsstelle sowie das Vorlegen eines amtlich anerkannten Ausweisdokumentes (siehe Abschnitt 4.1.2) erforderlich.
- Durch das Registrierungsverfahren wird der Name des Zertifikatswerbers direkt überprüft.

3.2 Verlängerung der Gültigkeit von Zertifikaten a.sign Uni

Das Verfahren zur Identifizierung bzw. Authentifizierung bei der Verlängerung der Gültigkeit eines Zertifikates ist zu jenem bei der Erstregistrierung identisch. Die Verlängerung wird im Zertifikat durch die „Renewal OID/Zähler der Verlängerungen“ angezeigt (<0 nicht verlängert; 1=einmal verlängert; 2=zweimal verlängert)

3.3 Widerruf von Zertifikaten für Signatoren

Um eine rasche Abwicklung des Widerrufs eines Zertifikates a.sign Uni zu ermöglichen, akzeptiert die CA a.sign Uni bzw. die ihr unterstellten LRAs folgende Identifikations- bzw. Authentifikationsmechanismen: Widerruf via Telefon, persönlicher Widerruf in der lokalen Registrierungsstelle.

4 Verfahrensanforderungen

Im nachfolgenden wird das Verfahren zur Erhalt eines Zertifikates a.sign Uni beschrieben.

4.1 Zertifizierung von Signatoren

Der Antrag auf Ausstellung eines Zertifikates a.sign Uni erfolgt durch den Zertifikatswerber persönlich in der lokalen Registrierungsstelle. Im Rahmen des Zertifikatsantrages sind die unter Pkt. 4.1.1. angegebenen Daten des Zertikatswerbers zu erfassen. Eine Vorerfassung der Daten übers Web ist möglich.

4.1.1 Enrollment-Daten - Antrag auf Ausstellung eines Zertifikates a.sign Uni

Der Zertifikatswerber hat im Rahmen des Zertifikatsantrages folgende persönliche Daten anzugeben:

Information	v/o	ZI	Anmerkung
Beim Enrollment-Formular ist einzugeben:			
Vorname	V	Ja	a.sign CAs behalten sich vor, fallweise oder permanent zusätzliche, in dieser Tabelle nicht enthaltene Daten beim Enrollment zu erfassen.
Nachname	V	Ja	
E-Mail-Adresse	o	Nein	
Akad. Titel (falls vorhanden)	o	Nein	
Geburtsdatum	v	Nein	
Geburtsort	V	Nein	
Geschlecht	V	Nein	
Weitere persönliche Daten: Straße, Postleitzahl, Ort, Land Telefonnummer Faxnummer	v o o	Nein Nein Nein	
Typ des verwendeten Ausweises (Reisepass, Führerschein oder Personalausweis)	v	Nein	
Ausweisnummer	v	Nein	
Ausstellende Behörde	v	Nein	
Ausstellungsdatum	v	Nein	
Persönliches Passwort	v	Nein	
Schlüssel-Länge	F	Ja	
Der Zertifikatswerber hat zur LRA mitzubringen:			
Bestätigung über die Identität des Zertifikatswerbers	V	Nein	Reisepass, Führerschein oder Personalausweis

Tabelle 4 Zertifikatsantrag

v/o ... verpflichtend / optional anzugeben

ZI ... Zertifikatinhalt

f ... fix

4.1.2 Zugelassene Ausweise und Dokumente

Der Nachweis der im vorigen Abschnitt (Kapitel 4.1.1) spezifizierten Informationen ist nur mit den in der unten angegebenen Tabelle angeführten Ausweisen und Dokumenten zulässig:

Überprüfte Einheit		Zugelassener Ausweis, zugelassenes Dokument
Signator	Inland	Reisepass Führerschein oder Personalausweis
	Ausland	Reisepass

Tabelle 5 Ausweisdokumente

4.1.3 Darstellung des Verfahrens zum Erhalt des Zertifikates a.sign Uni

Der Antrag auf Ausstellung eines Zertifikates a.sign Uni erfolgt in der lokalen Registrierungsstelle durch den Zertifikatswerber. Anschließend erfolgt die persönliche Überprüfung der Identität des Antragstellers anhand des amtlichen Lichtbildausweises in der lokalen Registrierungsstelle.

Die Mitarbeiter der LRA haben dabei folgende Aufgaben zu erfüllen:

- Kontrolle der Daten im Zertifikatsantrag anhand des vom
- Zertifikatswerber mitgebrachten Ausweisdokumentes und
- Anfertigen einer Kopie des Dokumentes
- Der LRA-Operator überprüft die Gültigkeit des mitgebrachten Ausweisdokumentes.
- Der LRA-Operator vergleicht das im mitgebrachten Ausweisdokument enthaltene Lichtbild mit dem Erscheinungsbild des Zertifikatswerbers.
- Der LRA-Operator fertigt eine Ablichtung des mitgebrachten Ausweisdokumentes an.

Anmerkung: Liefert eine der angeführten Überprüfungen ein negatives Ergebnis, so wird der Zertifikatsantrag vom LRA -Operator abgelehnt. Der LRA –Operator hält den Ablehnungsgrund fest und teilt dem Zertifikatswerber den Ablehnungsgrund sowie die weitere Vorgangsweise mündlich mit.

Erfassen der Daten

- Der LRA-Operator steckt seine "persönliche" LRA-Operator Chipkarte in den Chipkarten Reader auf eine eigens dafür vorgesehenen Workstation. Der LRA Operator erfasst die Daten, mittels des "Ausstellprogramms".

Hinweis: Der Zugriff auf die LRA-Operator-Chipkarte wird mittels einer PIN geschützt. Die LRA-Operator-Chipkarte verkörpert das Recht und die Pflicht des LRA-Operators zur Freigabe eines Zertifikatsantrages nachdem die Überprüfung des Zertifikatswerbers eine positives Ergebnis geliefert hat. Der LRA-Operator hat die Weitergabe der LRA-Operator-Chipkarte und allfälliger damit im Zusammenhang stehender PINs und Passwörter zu unterlassen. Insbesondere sind die im LRA-Operator-Vertrag festgelegten Sorgfaltspflichten zu beachten.

- Danach wird der Zertifikatsantrag vom LRA-Operator freigegeben.

Ausstellvorgang und Personalisierung der Chipkarte

- Mittels Ausstellprogramm druckt der LRA Operator eine Kopie aller eingegeben Daten aus. Der Kunde bestätigt mit einer Unterschrift die Richtigkeit seiner Daten sowie den Antrag auf Ausstellung eines a.sign Uni Zertifikates.

- Bevor die Personalisierung der Chipkarte durch die LRA-Applikation gestartet wird, vergibt der Zertifikatswerber persönlich eine achtstellige PIN mittels eines externen Tastaturblocks. Die PIN-Eingabe erfolgt zweimal mit Verification. Die Eingabe der PIN wird aus Sicherheitsgründen nicht angezeigt. Die PIN ist daher nur dem Signator bekannt.

- Anschließend erfolgt die Personalisierung der Smartcard.

- Optional: Es besteht nun die Möglichkeit, die Chipkarte nach kundenspezifischen Merkmalen zu bedrucken. In diesem Fall startet die LRA-Applikation das Bedrucken der Smartcard mit den aus der Datenbank übernommenen Daten.

- Es erfolgt der Export des Öffentlichen Schlüssels in den Zertifikatsantrag.

- Der LRA-Operator wird aufgefordert, den PIN einzugeben. Durch Eingabe der PIN signiert der LRA-Operator die Daten des Zertifikatswerbers, sowie des öffentlichen Schlüssels der Karte.

- Übermittlung des Zertifikatsantrages über eine SSLv2-Verbindung an die CA a.sign Uni.
- Die CA a.sign Uni protokolliert die erhaltenen Daten in der CA-Datenbank.
- Danach wird aus den Daten des Zertifikatswerbers erneut ein Hashwert gebildet und dieser mittels des Programms Keyworks und der Signatur des Operators auf Gültigkeit überprüft.
- Danach wird das Zertifikat mit welchem die Antragsdaten signiert wurden gegen eine ACL geprüft. Diese Vorgänge werden ebenfalls auf der CA a.sign Uni protokolliert.
- Wenn diese Überprüfungen positiv abgeschlossen wurden, werden die Antragsdaten für die Erstellung eines Zertifikats a.sign Uni verwendet. Ansonsten wird der Zertifikatsantrag und die Ausstellung des Zertifikates a.sign Uni durch die CA a.sign Uni verweigert.
- Sobald die Generierung erfolgt ist, wird das Zertifikat mittels SSLv2- wieder Rückübertragen an das wartende "Ausstellprogramm" (am PC in der die lokale Registrierungsstelle). Diese Vorgänge werden ebenfalls auf der CA a.sign Uni protokolliert.
- Nach dem Erhalt des Zertifikates überprüft das "Ausstellprogramm" den öffentlichen Schlüssel, der im Zertifikat enthalten ist mit dem öffentlichen Schlüssel der Karte übereinstimmt. Wenn eine Übereinstimmung gegeben ist wird das a.sign Uni Zertifikat auf die Karte geschrieben.
- Der Zertifikatswerber wird dem Signaturgesetz folgend schriftlich oder anhand eines dauerhaften Datenträgers über den Umgang mit Zertifikaten a.sign Uni, insbes. rechtliche Konsequenzen, Rechte und Pflichten des Signators usw. unterrichtet.
- Der LRA-Operator druckt den Zertifikatswerber-Vertrag in zweifacher Ausfertigung aus. Beide Ausfertigungen werden sowohl vom Zertifikatswerber als auch vom LRA-Operator manuell unterschrieben. Eine der beiden Ausfertigungen enthält ein Revoke-Passwort.
- Diese Ausfertigung wird dem Zertifikatswerber ausgehändigt.

Hinweis zum Revoke-Passwort: Dieses Passwort dient als zusätzlicher Authentisierungsmechanismus beim telefonischen Widerruf von a.sign Uni Zertifikaten.

- Zur Unterstützung der Auditierbarkeit des Zertifizierungsprozesses müssen die Ausfertigung des Zertifikatswerber-Vertrages, die nicht dem Zertifikatswerber

ausgehändigt wurde, und die Ablichtung des vom Zertifikatswerber mitgebrachten Ausweisdokumentes archiviert werden.

- Der LRA-Operator legt den Vertrag und die Dokument-Ablichtung in dem LRA-Tresor ab.
- Anschließend erfolgt die Ausgabe der Signaturkarte an den Zertifikatsinhaber
- Veröffentlichung des Zertifikates (wenn Zustimmung des Zertifikatswerbers vorhanden) im a.sign Verzeichnisdienst.

4.2 Überprüfung der Gültigkeit von Zertifikaten

Die CA a.sign Uni stellt mittels des a.sign Informationsdienstes eine online-Überprüfung des Status von Zertifikaten zur Verfügung.

Auf den a.sign Informationsdienst kann man unter der folgenden Web-Adresse zugreifen: http://www.a-trust.at.

4.3 Einsatzbereich von Zertifikaten a.sign Uni

Der Einsatzbereich der a.sign Uni Zertifikate ist auf die sichere elektronische Signatur von Dokumenten beschränkt. Zur Erstellung der sicheren elektronischen Signatur im Sinne des Österreichischen Signaturgesetzes und der auf dessen Grundlage ergangenen Verordnungen sind nur bestimmte Dokumentenformate geeignet.

Die Liste und Spezifikation der vom Zertifizierungsdienst a.sign Uni empfohlenen Dokumentenformate sowie der empfohlenen Signaturprodukte werden im Rahmen des Informationsdienstes unter http://www.a-trust.at veröffentlicht.

4.4 Überprüfung der Gültigkeit einer sicheren elektronischen Signatur

Eine sichere elektronische Signatur kann nur auf Basis eines qualifzierten Zertifikates und unter Einhaltung/Anwendung der vom Zertifizierungsdiensteanbieter angegebenen Dokumentenformate und Signaturprodukte erstellt werden. Die sichere Signaturprüfung kann mit einem vom Zertifizierungsdienst a.sign Uni empfohlenen Signaturprodukt vorgenommen werden. Die Liste der empfohlenen Signaturprodukte und Dokumentenformate werden im Informationsdienst veröffentlicht. Bestandteil der

sicheren Signaturprüfung ist auch die Überprüfung der Gültigkeit des Zertifikates über den Verzeichnis- bzw. Widerrufsdienst.

4.5 Zeitraum und Verfahren des Nachsignierens eines sicher elektronisch signierten Dokumentes

Die Parameter zur Erstellung einer sicheren elektronische Signatur, basierend auf dem a.sign Uni Zertifikat (Hashverfahren: SHA1; Verschlüsselungsalgorithmus RSA, 1024bit) entsprechen den Anforderungen des Österreichischen Signaturgesetzes und der auf dessen Grundlage ergangenen Verordnung und werden bis zum 31.12.2005 als sicher eingestuft (Signaturverordnung Anhang 1).

Elektronische Signaturen, die über den 31.12.2005 hinaus gültig und vor Manipulationen geschützt werden sollen (z.B. für Beweiswürdigung, Rechtsverbindlichkeit), müssen nachsigniert werden. Darunter versteht man das erneuerte Anbringen einer sicheren elektronischen Signatur vor Ablauf der oben angeführten Sicherheitsperiode (also vor dem 31.12.2005). Der Zeitpunkt des Nachsignierens muss mittels eines Zeitstempels dokumentiert werden. Das Nachsignieren ist daher nur bei gültigen sicheren elektronischen Signaturen zielführend. Eine gültige sichere elektronische Signatur liegt vor, wenn die Signatur auf Basis eines Zertifikates a.sign Uni erstellt und die Dokumentenvorgaben des Zertifizierungsdienstanbieters eingehalten wurden. Soll dem sicher elektronisch signierten Dokument nach dem 31.12.2005 dasselbe Sicherheitsniveau zugewiesen werden, muss es daher spätestens bis zum 31.12.2005 nachsigniert werden.

Das Nachsignieren eines sicher elektronisch signierten Dokumentes ist ein rein technischer Vorgang und muss nicht von einer bestimmten Person durchgeführt bzw. veranlasst werden. Das Nachsignieren kann somit auch von einer beliebig wählbaren vertrauenswürdigen Person vorgenommen werden. Veranlasst wird das Nachsignieren in der Regel von der Person, die an der Erhaltung des Sicherheitsniveaus der elektronischen Signatur interessiert ist. Wesentlich ist, dass der Sicherheitswert der sicheren elektronischen Signatur beibehalten wird und das Nachsignieren innerhalb der genannten Sicherheitsperiode durchgeführt wird.

5 Widerruf von Zertifikaten

5.1 Veröffentlichung widerrufener a.sign Uni Zertifikate

Widerrufe von Zertifikaten werden mittels Widerrufslisten (CRLs) im Format CRLv2 vom Verzeichnisdienst veröffentlicht. Widerrufene Zertifikate werden mindestens solange in den CRLs geführt, bis die ursprüngliche Gültigkeitsdauer des Zertifikates überschritten ist.

5.2 Aktualisierung der Widerrufslisten (CRLs)

Die Aktualisierung der Widerrufsdienste erfolgt grundsätzlich nach jedem durchgeführten Zertifikats-Widerruf. Zertifikatsinhaber werden vom erfolgten Widerruf verständigt.

Der Widerruf eines Zertifikates a.sign Uni enthält den Zeitpunkt, von dem an er gilt. Ein rückwirkender Widerruf von Zertifikaten ist nicht möglich.

5.3 Zum Widerruf Berechtigte

Der Widerruf eines Zertifikates a.sign Uni kann

- durch den Zertifikatsinhaber (ohne Angabe von Gründen)
- durch eine vom Zertifikatsinhaber genannte vertretungsbevollmächtigte Person (ohne Angabe von Gründen)
- durch die ausstellende CA a.sign Uni (ohne Angabe von Gründen)

veranlasst werden.

5.4 Gründe für den Widerruf eines Zertifikates a.sign Uni

5.4.1 Widerrufsgründe des Zertifikatsinhabers

Der Widerruf eines Zertifikates durch den Zertifikatsinhaber bzw. die vertretungsbevollmächtigte Person ist

- bei jeder Änderung der im Zertifikat enthaltenen persönlichen Daten,
- bei Verlust des Privaten Schlüssels,
- bei einem vermuteten oder erfolgten Diebstahl des Privaten Schlüssels sowie
- bei einem vermuteten oder erfolgten unbefugten Zugriff auf den Privaten Schlüssel

zu veranlassen.

5.4.2 Widerrufsgründe des Zertifizierungsdiensteanbieters

Der Widerruf eines Zertifikates a.sign Uni durch den Zertifizierungsdiensteanbieter ist umgehend zu veranlassen, wenn

- der Signator oder ein im Zertifikat genannter Machtgeber dies verlangt (Code 0),
- der Zertifizierungsdiensteanbieter Kenntnis vom Ableben des Signators erhält (Code 5)
- der Zertifizierungsdiensteanbieter Kenntnis von der Änderung der im Zertifikat bescheinigten Umstände erlangt (Code 3)
- das Zertifikat auf Grund unrichtiger Angaben erwirkt wurde (Code 0),
- der Zertifizierungsdiensteanbieter die Tätigkeit einstellt und die Verzeichnis- und Widerrufslisten nicht von einem anderen Zertifizierungsdiensteanbieter übernommen werden (Code 0),
- die Aufsichtssstelle gem. § 14 SigG den Widerruf des Zertifikates anordnet (Code 1)

- Gefahr der mißbräuchlichen Verwendung des Zertifikates besteht oder (Code 1)
- der Zertifikatsinhaber nicht die mit dem Zertifikat verknüpften Bestimmungen einhält (Code 0)

5.5 Widerrufsmöglichkeiten und -zeiten des Zertifizierungsdienstanbieters

Der Widerruf eines Zertifikates a.sign Uni kann telefonisch beim Widerrufsdienst erfolgen.

Telefonnummer: 01/501 45-1354

Widerrufszeiten: Montag - Sonntag : 00:00 - 24:00

5.6 Verfahren zur Beantragung eines Widerrufs

Für den Widerruf von Zertifikaten gelten folgende Bestimmungen:

- Ist der Widerruf eines Zertifikates notwendig, so hat der Widerruf unverzüglich zu erfolgen.
- Der Widerruf eines Zertifikates kann nicht rückgängig gemacht werden.
- Vor der Durchführung des Widerrufs eines Zertifikates überprüft die a.sign CA die Identität jener Person, die den Widerruf beantragt hat. In Übereinstimmung mit Abschnitt 3.3 sind nur die in den nachfolgenden Kapiteln angeführten Verfahren zulässig.

5.6.1 Widerruf eines Zertifikates via Telefon

Schritt	Aktion	Input	Output	Location
1	In der CA kann telefonisch durch Angabe persönlicher Daten (siehe unten) der Widerruf eines Zertifikates eingeleitet werden. Folgende persönliche Daten sind zu übermitteln: Vor- und Nachname, Geburtsort, Geburtsdatum, Pers. Passwort, Reason Code (optional)	persönliche Signator-Daten		Aufstellungsort des vom Zertifikatswerber verwendeten Telefons, ausstellende CA
2	Die CA überprüft die Angaben des gem. dem telefonischen Widerruf Ist die Überprüfung erfolgreich, wird ein Antrag auf Widerruf abgesetzt.	erfolgreicher Rückruf	Antrag auf Widerruf	Aufstellungsort des vom Zertifikatswerber verwendeten Telefons, ausstellende CA
3a	Ist die Zuordnung erfolgreich, d.h. gibt es eine Übereinstimmung bzgl. der übermittelten persönlichen Daten, so wird dies dem Signator mitgeteilt und das entsprechende Zertifikat revoziert.	erfolgreiche Übereinstimmung	Zertifikat-Widerruf, Information an den Signator	Aufstellungsort des vom Zertifikatswerber verwendeten Telefons, ausstellende CA
3b	Ist die Zuordnung nicht möglich, so wird dem Signator das Fehlschlagen des Revozierungsantrages mitgeteilt.	fehlende Übereinstimmung	Mitteilung an den Zertifikatsinhaber	Aufstellungsort des vom Zertifikatswerber verwendeten Telefons, ausstellende CA

Tabelle 6 Widerruf via Telefon

5.6.2 Widerruf eines Zertifikates in der lokalen Registrierungsstelle

Die Durchführung eines Zertifikat-Widerrufes in der lokalen Registrierungsstelle ist für a.sign Uni Zertifikate möglich.

Schritt	Aktion	Input	Output	Location
1	In der LRA kann persönlich durch Angabe persönlicher Daten (siehe unten) der Widerruf eines Zertifikates a.sign Uni eingeleitet werden. Folgende persönliche Daten sind zu übermitteln und anhand eines amtlichen Lichtbildausweises zu dokumentieren. Vor- und Nachname, Geburtsort, Geburtsdatum, Reason Code (optional)	persönliche Signator-Daten		LRA Austellende CA
2	Der LRA-Operator überprüft den amtlichen Lichtbildausweis anhand der angegebenen Daten und führt eine Sichtkontrolle durch.	erfolgreicher Rückruf	Antrag auf Widerruf	Ausstellende CA
3a	Liefert die Überprüfung ein positives Ergebnis, wird vom Ausweisdokument eine Ablichtung angefertigt und anschleißend das Zertifikat widerrufen.	erfolgreiche Übereinstimmung	Zertifikat-Widerruf	Ausstellende CA
3b	Ist die Zuordnung nicht möglich, so wird dem Signator das Fehlschlagen des Revozierungsantrages mitgeteilt.	fehlende Übereinstimmung	Mitteilung an den Zertifikat-Inhaber	Ausstellende CA

Tabelle 7 Widerruf in der LRA

Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH.
A-1030 Wien, Landstraßer Hauptstraße 5

5.7 Schlüsselaustausch bei einem Signator

Ein Schlüsselaustausch bedeutet, dass die Identität des Zertifikatinhabers an ein neues Schlüsselpaar gebunden wird. Dies ist ausschließlich durch Beantragung eines neuen Zertifikates möglich.

6 Archivierung

6.1 Zielsetzung

Die CA a.sign Uni archiviert die relevanten Informationen über alle Ereignisse im Zusammenhang mit dem Zertifizierungsprozess, um

- die Rekonstruktion von Vorgängen im Zusammenhang mit dem Zertifizierungsprozess zu ermöglichen und
- die Einhaltung der im vorliegenden Dokument angeführten Zertifizierungs-richtlinien und Sicherheitsmaßnahmen dokumentieren zu können.

6.1.1 Protokollierte Ereignisse und archivierte Daten

Folgende Ereignisse und Daten werden archiviert:

- Dokumentation des Lebenszyklus eines Zertifikates
  - Enrollment
  - Akzeptieren / Ablehnen eines Zertifikat-Antrages
  - Ausstellen eines Zertifikates
  - Widerruf eines Zertifikates
  - usw.
- Management des Privaten CA-Schlüssels
  - Protokollierung jedes Einsatzes des Privaten CA-Schlüssels
- CA-Management
  - Anlegen einer CA
  - Autorisierung von GRAs und LRAs
- Management der anzuwendenden Richtlinien

- Dokumentation von Verfahrensänderungen beim Beantragen eines Zertifikates, Widerrufen eines Zertifikates, Überprüfen der Enrollment-Daten usw.
- Dokumentation von Änderungen von Richtlinien durch Führen einer Aufstellung, nach welchem CPS und welchen Policies in welchen Versionen die einzelnen CAs arbeiten

6.1.2 Archivierungsdauer

Die Archivierungsdauer erfolgt analog der im Signaturgesetz und der auf dessen Grundlagen ergangenen Verordnungen angebenen Fristen (33 Jahre).

6.1.3 Schutz der Aufzeichnungen

Sowohl Aufzeichnungen in elektronischer Form als auch solche, die in Papierform vorliegen, werden vor Verlust oder Beschädigung sowie vor unbefugtem Zugriff geschützt.

6.1.4 Datensicherung

Der Systemadministrator einer a.sign CA Uni (siehe Kapitel 7.2) erstellt täglich eine Sicherung des Archivs.

6.1.5 Aufbewahrungsort der Aufzeichnungen

Die angefallenen Daten werden intern in geeigneter Form aufbewahrt. Zusätzlich werden die in Abschnitt 6.1.4 angesprochenen Datensicherungen an einen externen Ort gebracht und dort in geeigneter Weise aufbewahrt.

6.1.6 Zugriff auf Aufzeichnungen

Der direkte Zugriff auf die archivierten Daten erfordert Zugriffsrechte, über die nur die dazu berechtigten Angestellten verfügen.

6.2 Ausnahmesituationen bezüglich Privater Schlüssel einer a.sign CA

6.2.1 Verlust eines Privaten CA-Schlüssels

Ist der Private CA-Schlüssel verloren gegangen, ohne dass eine Kompromittierung erfolgte oder vermutet werden muss, so werden folgende Maßnahmen durchgeführt:

- Setzt die betroffene a.sign CA mit einem neuen CA-Schlüssel den Betrieb fort, so geht sie analog zu Abschnitt 6.2.2 (Austausch eines Privaten CA-Schlüssels) vor.
- Stellt die a.sign CA hingegen ihren Betrieb ein, so geht sie analog zu Abschnitt 6.3 (Einstellen des Betriebes einer CA) vor.

6.2.2 Austausch eines Privaten CA-Schlüssels

Beim Austausch des Privaten Schlüssels einer a.sign CA wird folgende Vorgangsweise angewendet:

- Die a.sign CA generiert ein neues Schlüsselpaar. Dieser Vorgang muss 3 Monate vor dem geplanten Schlüsselaustausch abgeschlossen sein.
- Die Gültigkeit des alten Schlüsselpaares endet nicht mit dem Zeitpunkt des Schlüsselaustausches. Das alte Schlüsselpaar ist noch mindestens so lange gültig, dass die Gültigkeitsdauer von Zertifikaten, die vor dem Schlüsseltausch ausgegeben werden, jene des CA-Zertifikates bzgl. des alten Schlüsselpaares nicht überschreitet.

6.2.3 Kompromittierung eines Privaten CA-Schlüssels

Nach einer vermuteten oder erfolgten Kompromittierung des Privaten Schlüssels einer CA a.sign Uni werden folgende Maßnahmen durchgeführt:

- Information jedes Inhabers eines gültigen, von der CA mit dem kompromittierten Schlüssel signierten Zertifikates
- Revozieren des CA-Zertifikates durch nach dem 4-Augen-Prinzip.

- Generieren eines neuen Schlüsselpaares und Ausstellung eines neuen CA-Zertifikates a.sign Uni
- Widerruf aller Zertifikate für Signatoren, die mit dem kompromittierten Schlüssel signiert wurden
- Informieren aller von den im vorigen Punkt spezifizierten Widerrufen betroffenen Zertifikatinhaber von der erfolgten Revozierung ihrer Zertifikate
- Der Verzeichnisdienst (insbesondere CRLs) wird gegebenenfalls von der CA a.sign Uni weitergeführt, um authentische CRLs veröffentlichen zu können.
- Jedem Signator wird von der CA a.sign Uni ein neues Zertifikat ausgestellt.

6.3 Einstellen des Betriebes der a.sign Uni CA

- Die dauerhafte Einstellung des Betriebes der CA a.sign erfolgt gemäß den Vorgaben des Österreichischen Signaturgesetzes und der auf dessen Grundlage ergangenen Verordnungen.
- Die Einstellung der Tätigkeit wird unverzüglich der Aufsichtsstelle durch eine autorisierte Person angezeigt.
- Der Zertifizierungsdiensteanbieter stellt sicher, dass die bis zum Zeitpunkt der Einstellung der Tätigkeit gültigen Zertifikate widerrufen oder dass seine Verzeichnis- und Widerrufsdienste von einem anderen Zertizierungsdiensteanbieter übernommen werden. Im Falle des Widerrufs wird sichergestellt, dass die Widerrufsdienste jedenfalls weitergeführt werden.
- Die Signatoren werden unverzüglich über die Einstellung der Tätigkeit der CA a.sign Uni sowie den Widerruf bzw. die Übernahme der Verzeichnis- und Widerrufsdienste von einem anderen Zertifizierungsdiensteanbieter informiert.

7 Infrastrukturelles, organisatorisches und personelles Sicherheitskonzept

Die CA a.sign Uni definiert ein Sicherheitskonzept, das die in den Abschnitten 7 und 8 behandelten Aspekte abdeckt und als Grundlage für Audits herangezogen wird.

7.1 Infrastrukturelle Sicherheitsmaßnahmen

In diesem Kapitel werden die eingesetzten infrastrukturellen Sicherheitsmaßnahmen bzgl. a.sign CAs und GRAs (Kapitel 7.1.1 – 7.1.8) sowie LRAs (Kapitel 7.1.9) angeführt.

7.1.1 Verwendete Räumlichkeiten

Die Hauptkomponenten der a.sign CAs und GRAs befinden sich bei der Telekom Austria GmbH, Wiedner Hauptstraße 73, A-1040 Wien, in speziell dafür vorgesehenen und eingerichteten Räumlichkeiten.

7.1.2 Zugangskontrollen

Die Zugangskontrolle erfolgt über ein Zugangskontrollsystem mit folgenden Eigenschaften:

- Zugangskontrolle unter Verwendung einer Sicherheitskarte mit integriertem passivem Schwingkreis und berührungsloser Registrierung
- zusätzliche PIN-Eingabe beim Zugang zum Hochsicherheitsbereich (d.h. zu den a.sign CA-Komponenten)
- Möglichkeit der Protokollierung und Rekonstruierbarkeit von Authentifizierungen
- Einbruchs-Alarmmelder
- Video-Überwachungssystem

7.1.3 Stromversorgung

Die verwendete Stromversorgung besitzt folgende Eigenschaften:

- Die Stromversorgung erfolgt im Halblastparallelbetrieb.
- Es werden 2 getrennte USVs inkl. getrennter Batterie mit elektronischem Bypass bei Überschreitung verwendet.
- Bei einem Ausfall der ersten USV übernimmt die zweite USV die gesamte Last.
- Fällt auch die zweite USV aus, so übernimmt das Netz die Versorgung.
- Fällt zusätzlich das Netz aus, so wird eine Notstromversorgung mittels Dieselaggregat aktiviert.

7.1.4 Klimatisierung

Die eingesetzten Räumlichkeiten verfügen über ein Klimatisierungssystem mit einer Leistungsfähigkeit von bis zu 20 kW.

7.1.5 Feuerprävention

In den eingesetzten Räumlichkeiten wird eine TUS-Brandmeldeanlage (tonfrequentes Übertragungssystem) eingesetzt, das in das bestehende Brandmeldesystem integriert ist und daher eine direkte Alarmierung der zuständigen Feuerwehr einschließt. Im Brandfall kann daher von einer Obergrenze von 5 Minuten bis zum Eintreffen der ersten Feuerwehr-Löscheinheiten ausgegangen werden.

7.1.6 Aufbewahrung von Datenmaterial

Zur Aufbewahrung von schützenswertem Datenmaterial wird ein Tresor eingesetzt.

7.1.7 Abfallentsorgung

Die Entsorgung von defekten bzw. nicht mehr benötigten Datenträgern beinhaltet das Löschen der gespeicherten Informationen mittels einer elektromagnetischen Bandlöschmaschine.

7.1.8 Sonstiges

- Die Absicherung des Local Area Networks der CA gegen unautorisierte Zugriffe von außen erfolgt durch den Einsatz von Firewalls.
- Der Zugriff auf die System-Komponenten erfordert die Authentifizierung der Person, die den Zugriff durchführen möchte.
- Es stehen Aufbewahrungsmöglichkeiten für die zur Authentifizierung von CA- und GRA-Bediensteten eingesetzten Hardware-Token (Smartcards o.ä.) zur Verfügung.

7.1.9 Infrastrukturelle Maßnahmen bzgl. a.sign LRAs

Die der CA a.sign Uni zugeordneten LRAs verfügen über Aufbewahrungsmöglichkeiten für die zur Authentifizierung von LRA-Operatoren eingesetzten Hardware-Token (Smartcards o.ä.)

7.2 Organisatorische Sicherheitsmaßnahmen

7.2.1 a.sign CAs

Um den sicheren Betrieb einer a.sign CA zu gewährleisten, werden die kritischen in einer a.sign CA anfallenden Tasks gemäß der unten angeführten Tabelle auf einzelne Klassen von CA-Angestellten aufgeteilt.

Ein Vertreter einer bestimmten Klasse darf dabei keine Aufgaben durchführen, für die ein Vertreter einer anderen Klasse zuständig ist. Zusätzlich kann auch zur Durchführung eines wichtigen Tasks (z.B. Generierung des Privaten CA-Schlüssels) mehr als ein Vertreter der entsprechenden Klasse erforderlich sein.

Task	Klasse der zur Ausführung Berechtigten	Bemerkung
Generierung eines CA-Schlüssels	CAA	mindestens 2 Personen erforderlich
Generieren, Signieren und Veröffentlichen einer CRL	CAA	
Administrieren der CA-Database	CAA	
Erstkonfiguration der eingesetzten Hard- und Software	CASA	
Einrichtung aller notwendigen Accounts	CASA	
Einstellen der Netzwerkkonfigurationen	CASA	
Durchführen von System Backups	CASA	
Durchführen von System Upgrades	CASA	
Durchführen von Backups des Archivs	CASA	
Durchführen von Änderungen bzgl. Domain Name oder IP-Adresse	CASA	
Ausgabe der Zugriffskontrollen bzgl. System-Komponenten und Räumlichkeiten der CA oder LRA (z.B. Smartcards)	SB	
Zuweisen von Passwords für neue Accounts	SB	
Überprüfung der Audit Log Files zur Kontrolle der Aktivitäten der CAAs	SB	
Überprüfung und Management aller angefallener Protokolldaten	SB	
Entsorgung von Datenträgern	SB	
Überprüfung der Signator-Daten mittels der mitgebrachten Dokumente in der LRA	LRAO	
Unterzeichnung des schriftlichen Vertrages in der LRA	LRAO	
Signieren der Enrollment-Daten und Übermittlung an die CA –a.sign Uni	LRAO	
Anstoss „Generieren, Signieren und Veröffetnlichen von Zertifikaten“	LRAO	
Anstoss „Verlängern von Zertifikaten	LRAO	
Anstoss „Generieren, Signieren und Veröffentlichen einer CRL	LRAO	

Tabelle 8 Berechtigungen

CAA ... CA-Administrator

CASA ... CA System-Administrator

SB ... Sicherheitsbeamter

LRAO ... LRA-Operator

7.2.2 a.sign GRAs

Der Zugriff auf die eingesetzten Komponenten ist in GRAs, die einer a.sign CA zugeordnet sind, nur nach einer erfolgreichen Authentifizierung des GRA-Operators möglich.

7.2.3 a.sign LRAs

Der Zugriff auf die eingesetzten Komponenten ist in LRAs, die einer a.sign CA zugeordnet sind, nur nach einer erfolgreichen Authentifizierung des LRA-Operators möglich.

7.2.4 Signatoren

Signatoren sind für den sicheren Umgang mit ihrem Privaten Schlüssel verantwortlich. Dies erfordert den Schutz des Privaten Schlüssels vor Zugriff durch Unbefugte und schließt eine Weitergabe des Privaten Schlüssels aus. Der Zugriff auf den Privaten Schlüssel ist jedenfalls durch eine 8-stellige PIN zu schützen.

7.3 Personelle Sicherheitsmaßnahmen

Es wird sichergestellt, dass das im Rahmen des Zertifizierungsdienstes eingesetzte Personal den Anforderungen der Österreichischen Signaturverordnung (vgl. §10 Abs. 4 und 5) genügt.

7.3.1 a.sign CAs

Für den Betrieb von a.sign CAs werden Personen mit der entsprechenden Vertrauenswürdigkeit, Integrität, Zuverlässigkeit und Fachkunde eingesetzt. Begleitend dazu werden stellenbezogene Schulungsmaßnahmen für das CA-Personal durchgeführt.

7.3.2 a.sign GRAs

Für das Personal, das beim Betrieb der a.sign GRAs eingesetzt wird, gelten zu Abschnitt 7.3.1 analoge Bestimmungen.

7.3.3 a.sign LRAs

In LRAs, die einer a.sign CA unterstellt sind, gelten für LRA-Operatoren folgende Richtlinien:

Erstüberprüfung	Jede a.sign CA führt eine Erstüberprüfung eines möglichen LRA-Operators durch, um dessen Vertrauenswürdigkeit festzustellen. Ergibt die Erstüberprüfung ein negatives Resultat, so darf die überprüfte Person nicht mehr für Aufgaben innerhalb der a.sign Zertifizierungsdienstleistungen eingesetzt werden.
Einschulung	Die Einschulung inkludiert das Ablegen einer LRA-Dienstprüfung, die vom Zertifizierungsdienstanbieter durchzuführen ist.
Akkreditierung	Der LRA-Operator wird von der entsprechenden CA vereidigt. Zusätzlich hat der LRA-Operator in einem schriftlichen Vertrag die Einhaltung der Pflichten eines LRA-Operators (vertrauliche Behandlung der erfassten Daten usw.) zu garantieren.
Fortbildung	Bei wesentlichen Änderungen der verwendeten Systeme haben die LRA-Operatoren Fortbildungskurse zu absolvieren.
Grobes Vergehen gegen die a.sign Richtlinien	Begeht der LRA-Operator ein grobes Vergehen gegen die a.sign Richtlinien, so darf er nicht mehr für Aufgaben innerhalb der a.sign Zertifizierungsdienstleistungen eingesetzt werden.
Dokumentation von Aktionen eines LRA-Operators	Jede a.sign CA dokumentiert jene Aktionen eines LRA-Operators, die eine Beantragung, Erzeugung, Abholung, Verlängerung und den Widerruf eines Zertifikates betreffen.
Signierpflicht	Jeder LRA-Operator hat die übermittelten Zertifikat-Anträge digital zu signieren.

Tabelle 9 Pflichten LRA-Operator

8 Technisches Sicherheitskonzept

8.1 Schlüsselgenerierung und Schlüsselmanagement

8.1.1 Erzeugung des CA-Schlüsselpaares

1. In der a.sign CA wird durch organisatorische Maßnahmen gewährleistet, dass der Private Schlüssel der CA a.sign Uni nicht von einer Person allein generiert wird. Minimumanforderung ist die Generierung nach dem 4-Augen-Prinzip sowie die entsprechende Protokollierung durch den Kontrollbeamten. Durch eine weitere organisatorische Maßnahmen wird sichergestellt, dass der erzeugte Private Schlüssel der CA a.sign Uni in der Signaturerstellungseinheit verbleibt und diese nicht verlässt.

2. Die Erstinstallation der CA und damit die Generierung des CA-a.sign Uni Schlüsselpaares fällt in den Aufgabenbereich der CA-Administratoren.

3. Im Rahmen der Schlüsselerzeugung werden folgende Parameter für den Schlüssel festgelegt:

4. Verschlüsselungsalgorithmus: RSA

5. Schlüssellänge: 1024 bit

6. Der private Schlüssel der CA a.sign Uni wird ausschließlich zur Signatur von Zertifikaten a.sign Uni verwendet.

8.1.2 Distribution des Öffentlichen CA-Schlüssels

Die Verteilung des Öffentlichen Schlüssels der CA a.sign Uni an natürliche Personen erfolgt im Informationsdienst unter http://www.a-trust.at über eine SSLv2-Verbindung.

8.1.3 Erzeugung des Schlüsselpaares eines Signators

1. Die Erzeugung des privaten Schlüssels erfolgt zentral auf einem Prozessorchip. Der Prozessorchip ist einen Kartenkörper eingebettet. Bis zur Personalisierung der Signaturkarte ist der Schlüssel durch eine Transport-PIN gesichert. Die

Liste der vom Zertifizierungsdiensteanbieter verwendeten Smartcards wird im Informationsdienst unter http://www.a-trust.at veröffentlicht.

2. Der Schutz des Privaten Schlüssels erfolgt im Rahmen der Personalisierung der Chipkarte mittels eines 8-stelligen Autorisierungscodes durch den Signator persönlich. Die Eingabe erfolgt zweimal mit Verification mittels eines externen Tastaturblocks. Die Eingabe wird nicht angezeigt.

3. Aufgrund der Struktur und der Sicherheitsmechanismen des Chips wird sichergestellt, dass der private key den Chip nicht verlässt.

4. Der Private Schlüssel ist durch die vom Signator vergebene 8-stellige PIN geschützt.

8.1.4 Einschränkungen bzgl. der Verwendung von Schlüsseln

Die zulässigen Verwendungsmöglichkeiten von Zertifikaten a.sign Uni für CA und Signatoren werden in der *Key Usage Extension* der einzelnen Zertifikate definiert.

a.sign Uni CA-Zertifikate werden ausschließlich für die Erstellung sicherer elektronischer Signaturen von Zertifikaten a.sign Uni verwendet.

a.sign Uni Zertifikate: Die Key Usage Extension im Zertifikat ist so gesetzt, dass laut diesen Angaben nur das Signieren erlaubt ist (non repudiation).

8.2 Schutz des Privaten Schlüssels

8.2.1 Speicherung des Privaten Schlüssels

8.2.1.1 Privater CA-Schlüssel

Bei der Speicherung des Privaten CA-Schlüssels wird ein Kryptografie-Koprozessor eingesetzt, der dem FIPS 140 Level 3-Standard gegen physikalische Angriffe genügt. Dieser Koprozessor registriert automatisch jede Spannungsschwankung (hervorgerufen z.B. durch Anlegen eines Messgeräts), jede übermäßige Temperaturschwankung, übermäßige Erschütterungen sowie Versuche, Informationen aus der Karte mittels Durchleuchten (Röntgenstrahlung) zu gewinnen und verhindert in diesen Fällen durch interne Löschvorgänge unwiderruflich Zugriffe auf die im Koprozessor gespeicherten Informationen.

Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH.
A-1030 Wien, Landstraßer Hauptstraße 5

8.2.1.2 Privater Schlüssel eines Signators

Der Private Schlüssel des Signators wird auf der a.sign Uni Smartcard generiert und in einem Objekt gespeichert. Der Autorisierungscode (die PIN) zum Auslösen des Signaturvorgangs ist nur dem Kunden bekannt. a.trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH empfiehlt dringend im Sinne der Sicherheit keine PIN-Kombinationen wie z. B. Geburtsdatum zu verwenden. Beachten Sie bitte nachfolgend angeführte Informationen zum Autorisierungscode (=PIN).

Zweck des Autorisierungscodes: Der Autorisierungscode ist für die Auslösung des Signaturvorganges notwendig. Die Auslösung des Signaturvorganges ohne Eingabe des Autorisierungscodes ist nicht möglich.

Vergabe des Autorisierungscodes: Der Autorisierungscode besteht aus einer 8-stelligen PIN. Diese wird im Rahmen des Zertifikatsantrags in der lokalen Registrierungsstelle durch den Zertifikatswerber vor Auslösung der Schlüsselgenerierung, mittels eines externen Tastaturblocks generiert. Die Eingabe des Autorisierungscodes erfolgt zweimal mit Verifikation. Die Eingabe des Autorisierungscodes wird aus Sicherheitsgründen nicht angezeigt.

Kenntnis des Autorisierungscodes: Der Autorisierungscode ist nur dem Signator bekannt. Die Weitergabe, das Kopieren, Speichern usw. des Autorisierungscodes ist untersagt.

Eingabe des Autorisierungscodes: Der Autorisierungscode muss vor Auslösung des Signaturvorganges in voller Länge durch den Signator persönlich eingegeben werden. Die Speicherung oder eine Eingabeerleichterung (z.B. Abkürzungen, Aufschreiben, Weitergabe) sind untersagt.

Sperre des Autorisierungscodes: Nach dreimaliger Falscheingabe des Autorisierungscodes wird der Chip automatisch gesperrt. Eine Entsperrung des Chips ist nicht möglich. Der Zugriff resp. die Auslösung des Signaturvorganges ist nicht mehr möglich. Das dazugehörige digitale Zertifikat muss widerrufen werden.

Regelmäßiger Wechsel des Autorisierungscodes: Der Zertifikatsinhaber verpflichtet sich, seinen Autorisierungscode in regelmäßigen Abständen zu ändern.

Signaturprodukte und Chipkartenlesegeräte: Der Signator verwendet zur Erstellung der sicheren elektronischen Signatur, basierend auf einem a.sign Uni Zertifikat, ausschließlich vom Zertifizierungsdiensteanbieter empfohlene Signaturprodukte und Chipkartenlesegeräte.

8.3 8.3 Archivierung der Öffentlichen Schlüssel

Die Archivierung der Öffentlichen Schlüssel der Signatoren erfolgt einerseits in einem X.500-Verzeichnis in unverschlüsselter Form sowie andererseits in lokalen CA-Datenbanken in verschlüsselter Form.

8.4 Gültigkeitsdauer von Zertifikaten für Signatoren und CA-Zertifikaten

Zertifikat	Gültigkeitsdauer
a.sign Uni User Zertifikate	3 Jahre
a.sign Uni CA	30 Jahre

Tabelle 10 Gültigkeitsdauer

8.5 Standards der eingesetzten Soft- und Hardware

8.5.1 Software

Die eingesetzte Software besteht aus 3 Hauptkomponenten:

- Controller
- Certificate Management System
- X.500 Directory

8.5.1.1 Controller

Der Controller unterstützt

- die Secure Sockets Layer Versions 2 (SSLv2) und 3 (SSLv3),
- die Kryptografie-Standards PKCS#7 und PKCS#10,

8.5.1.2 Certificate Management System

Das Certificate Management System unterstützt

- X.509v3-Zertifikate,
- X.509v2-Widerrufslisten (CRLs),
- Schlüssellängen bis 1024 Bits,
- den Hashalgorithmus SHA-1 sowie
- LDAP für die Kommunikation mit dem X.500-Directory.

8.5.1.3 X.500-Directory

Das X.500-Directory unterstützt

- LDAP für die Kommunikation mit der CA und mit anderen System-Komponenten.

8.5.2 Hardware

Der eingesetzte Kryptografie-Koprozessor entspricht dem FIPS 140 Level 3-Sicherheitsstandard gegen physikalische Angriffe und unterstützt die folgenden Kryptografie-Standards:

- DES für Ver- bzw. Entschlüsselungen,
- RSA zum Digitalen Signieren bzw. Überprüfen von Zertifikaten,
- die Hashalgorithmen MD5 und SHA-1,
- ANSI X9.9 und X9.23 sowie
- ISO 9796.

8.5.3 Smartcards für Signatoren

Die im Rahmen des Zertifizierungsdienstes a.sign Uni eingesetzten Smartcards werden von a.trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH zur Verfügung gestellt. Smartcards sind Plastikkarten im Scheckkartenformat mit einem eingebetteten Prozessorchip und mit einem Betriebssystem

ausgestattet sind. Die Smartcards werden für den Zertifizierungsdienst a.sign Uni initialisiert und personalisiert. Die Initialisierung der einzelnen Chips erfolgt im Rahmen der Kartenproduktion durch den Kartenproduzenten.

Die Personalisierung der Smartcard wird in der lokalen Registrierungsstelle in Anwesenheit des Zertifikatswerbers vorgenommen. Der Schutz des privaten Schlüssels erfolgt durch den Signator mittels einer achtstelligen PIN.Die PIN ist ausschließlich dem Signator bekannt. Der Signator hat die Weitergabe der Smartcard und der PIN zu unterlassen. Informationen zur eingesetzten Smartcard werden im Web veröffentlicht.

9 Zertifikats- und CRL-Profil

9.1 Profil der ausgegebenen a.sign Uni Zertifikate

9.1.1 CA-Zertifikat a.sign Uni

a.sign Uni CA-Zertifikate werden entsprechend dem Standard X.509v3 ausgegeben.

9.1.1.1 a.sign Uni User-CA-Zertifikat

Ein Zertifikat einer User-CA a.sign Uni enthält folgende Basisfelder (Basic Certificate Fields):

Attribut	Inhalt	Anmerkung
Version	v3	Das Zertifikat ist ein X.509v3-Zertifikat.
Seriennummer	Seriennummer des Zertifikates	
Public Key	RSA/1024 bit	
Signatur-Algorithmus	SHA 1	Signatur-Algorithmus, der von der ausstellenden Instanz bei der Signatur des Zertifikates verwendet wurde.
Aussteller	CN = a-sign uni OU = a-sign uni OU = www.a-trust.at O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH C = AT	
Gültig von	Beginn der Gültigkeitsdauer des Zertifikates	
Gültig bis	Ende der Gültigkeitsdauer des Zertifikates	
Antragsteller	CN = a-sign uni OU = a-sign uni OU = www.a-trust.at O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH C = AT	
Öffentlicher Schlüssel	Öffentlicher Schlüssel des Zertifikatinhabers	

Tabelle 11 CA-Zertifikatsfelder

Zusätzlich enthalten CA-Zertifikate a.sign Uni einige Standard-Extensions.

9.1.2 a.sign Uni Zertifikate für Signatoren

a.sign Uni Zertifikate für Signatoren werden gemäß dem Standard X.509v3 ausgegeben.

9.1.2.1 a.sign Uni Zertifikat

Ein a.sign Uni User-Zertifikat enthält folgende Basisfelder (Basic Certficate Fields):

Attribut	Inhalt	Anmerkung
Version	v3	Das Zertifikat ist ein X.509v3-Zertifikat.
Seriennummer	Seriennummer des Zertifikates	
Public Key	RSA/1024bit	
Signatur-Algorithmus	SHA1	Signatur-Algorithmus, der von der ausstellenden Instanz bei der Signatur des Zertifikates verwendet wurde.
Aussteller	CN = a-sign uni OU = a-sign uni OU = www.a-trust.at O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH C = AT	
Gültig von	Beginn der Gültigkeitsdauer des Zertifikates	
Gültig bis	Ende der Gültigkeitsdauer des Zertifikates	
Zertifikat-Inhaber	CN = … OU = www.a-trust.at OU = a-sign uni O=A-Trust Ges.f. Sicherheitssysteme im elektr. Datenverkehr GmbH C = AT	CN … Common Name
Öffentlicher Schlüssel	Öffentlicher Schlüssel des Zertifikatinhabers	
QcEuCompliance / Zertifikat laut Signaturgesetz im Land OID:	"AT"	

0.4.0.1.1		
QcEuLimitValue / Transaktionslimit (Währungscode, Betrag, Exponent) OID: 0.4.0.1.2	EUR, 4, 3	EUR = ISO für Euro 4 für 4 Mal 3 für 10 ^ = 4 * 10 ^ 3 = 4.000 EUR
QcSigDeviceId / Seriennummer des Zertifikatsspeichers OID: 1.2.040.0.17.3.1.	zb.: 1469598781541714959	Seriennummer der SmartCard
RenewalOID / Zähler der Verlängerungen OID: 1.2.040.0.17.3.2.	Erlaubte Werte 0, 1, 2	

Tabelle 12 Signatoren-Zertifikatsfelder

Zusätzlich enthalten a.sign Uni User-Zertifikate Standard-Extensions.

9.2 Profil der ausgegebenen CRLs

Es werden X.509 Version 2 CRLs ausgegeben.

9.3 Durchführung von Änderungen des Sicherheits- und Zertifizierungskonzept

9.3.1 Allgemeines

Das Sicherheits- und Zertifizierungskonzept wird von einer Expertengruppe entwickelt, die sich aus den Bereichen Technik, Wirtschaft und Rechtswissenschaften zusammensetzt.

9.3.2 Erforderliche Schritte

- Ein Änderungsvorschlag zum jeweiligen Sicherheits- und Zertifizierungskonzept muss zunächst den Mitgliedern der oben erwähnten Expertengruppe übermittelt werden.

- Nur wenn von den Mitgliedern der Expertengruppe keine Einwände gegen den Änderungsvorschlag eingebracht werden, gilt der Änderungsvorschlag als akzeptiert.

9.4 Veröffentlichung geänderter Sicherheits- und Zertifizierungskonzepte

Jede gemäß Punkt 9.3.2. geänderte Version des Sicherheits- und Zertifizierungskonzepts wird im Rahmen des Informationsdienst veröffentlicht.

10 Anhang

A Definitionen

Antragsteller: siehe → Zertifikatswerber

Aussteller: siehe → Zertifizierungsdiensteanbieter

authentifizieren: beglaubigen, die Echtheit bezeugen

authentisch: echt

Authentizität: Echtheit einer Schrift, Urkunde

Certification Authority (CA): Einheit der Zertifizierungshierarchie, die andere Certification Authorities sowie Signatoren zertifizieren kann

Certification Practice Statement (CPS): verbindliches Dokument, in dem das Vorgehen einer bestimmte Certification Authority bei Zertifizierungen sowie technische und organisatorische Anforderungen an die zugeordneten Einheiten der Zertifizierungshierarchie definiert sind

Certificate Revocation List (CRL): Liste von Zertifikaten, die vor dem Ablauf ihrer Gültigkeitsdauer widerrufen wurden

Common Name (CN): Name von Personen, Organisationen

Digitale Signatur: **Ein eindeutiger Extrakt eines elektronischen Dokumentes wird mit dem Privaten Schlüssel des Signierenden verschlüsselt.** Mit dem dazugehörigen Öffentlichen Schlüssel kann verifiziert werden, dass das elektronische Dokument vom Besitzer des Privaten Schlüssels digital signiert wurde und dass dieses nicht nachträglich verändert wurde.

Distinguished Name (DN): eindeutiger, unverwechselbarer Name

Dritter: Person, die eine Digitale Signatur empfängt bzw. dem Zertifikat eines anderen Signators vertraut

Elektronische Signatur: elektronische Daten, die anderen elektronischen Daten beigefügt oder mit diesen logisch verknüpft werden und die der Feststellung der Identität des Signators dienen (siehe auch → sichere elektronische Signatur)

End-Anwender: siehe → Signator

Globale Registrierungsstelle (GRA): ist einer Certification Authority zugeordnet, überprüft und archiviert Daten, die ihr von Signatoren übermittelt werden.

Kompromittierung des Privaten Schlüssels: Der Private Schlüssel ist zeitweise oder permanent für Unbefugte zugänglich.

Lokale Registrierungsstelle (LRA): führt im Auftrag einer Certification Authority lokal die Überprüfung der Identität eines Zertifikatswerbers durch.

Öffentlicher Schlüssel: Teil des Schlüsselpaares, der zum Verschlüsseln von Nachrichten und Dokumenten sowie zum Prüfen von Digitalen Signaturen dient und weitergegeben werden kann bzw. veröffentlicht wird; ist Bestandteil eines Zertifikates (siehe auch: → Privater Schlüssel)

Policy: Sicherheits- und Zertifizierungskonzept, das von der a.sign Certification Authority für jede Zertifikatsklasse ausgegeben werden

Private Key: siehe → Privater Schlüssel

Privater Schlüssel: Teil des Schlüsselpaares, der zum digitalen Signieren sowie zum Entschlüsseln von Nachrichten und Dokumenten erforderlich ist und geheimgehalten werden muss (siehe auch: → Öffentlicher Schlüssel)

Public Key: siehe → Öffentlicher Schlüssel

Public Key Infrastructure (PKI): siehe → Zertifizierungsinfrastruktur

Qualifiziertes Zertifikat: Zertifikat, das bestimmte, im Signaturgesetz festgelegte Angaben enthält und von einem Zertifizierungsdiensteanbieter ausgestellt wird, der bestimmten, im Signaturgesetz angegebenen Anforderungen genügt

Schlüsselaustausch: Bindung der Identität des Signators an ein neues Schlüsselpaar

Reason Code: Identifier, der den Grund für einen Zertifikats-Widerruf codiert

Secure Multipurpose Internet Mail Extention (S/MIME): Erweiterung des MIME-Formates, die Verschlüsselung und Digitale Signatur von E-Mails unterstützt

Secure Socket Layer (SSL): Protokoll, das einen abhörsicheren und authentischen Datenaustausch ermöglicht

Sichere elektronische Signatur: elektronische Signatur, an die besondere, im Signaturgesetz festgelegte Sicherheitsanforderungen gestellt werden

Signator: Person, die ein Zertifikat besitzt und selbst keine Zertifikate ausstellen darf

Signaturerstellungseinheit: konfigurierte Software- oder Hardwareeinheit zur Verarbeitung der Signaturerstellungsdaten.

Signatur- und Zertifizierungsdienste: Bereitstellung von Signaturprodukten und Signaturverfahren; Ausstellung, Erneuerung und Verwaltung von Zertifikaten; Verzeichnisdienste; Widerrufsdienste; Registrierungsdienste; Zeitstempeldienste; Rechner- und Beratungsdienste im Zusammenhang mit elekronischen Signaturen

Uniform Resource Locator (URL): Namenskonvention, die den Zugriffspfad auf Computer, Verzeichnisse und Daten im Internet eindeutig definiert; die URL beinhaltet auch das verwendete Internet-Protokoll (z.B. HTTP)

Zeitstempel: eine mit einer digitalen Signatur versehene digitale Bescheinigung eines Zertifizierungsdiensteanbieters darüber, dass ihr bestimmte digitale Daten zu einem bestimmten Zeitpunkt vorgelegen haben

Zertifikat: verbindet den eindeutigen Namen eines Subjektes mit einem Öffentlichen Schlüssel durch eine Digitale Signatur; die Spezifikation entspricht dem ITU-T X.509v3 Standard

Zertifikatinhaber: siehe → Signator

Zertifikatsklasse: Kategorisierung der Vertrauenswürdigkeit von Zertifikaten in *Light*, *Strong* und *Uni*

Zertifikatstyp: Kategorisierung des Verwendungszwecks von Zertifikaten in User-, Server- und Developer-Zertifikate

Zertifikatsverzeichnis: Liste aller veröffentlichten Zertifikate

Zertifikatswerber: natürliche Person, die einen Antrag auf Ausstellung eines Zertifikates stellt

Zertifizierungsdienste: siehe → Signatur- und Zertifizierungsdienste

Zertifizierungsdiensteanbieter: natürliche oder juristische Person oder sonstige rechtsfähige Einrichtung, die Zertifikate ausstellt oder andere elektronische Signatur- oder Zertifizierungsdienste erbringt (siehe auch → Signatur- und Zertifizierungsdienste)

Zertifizierungshierarchie: umfasst jene Einheiten, die im Rahmen von Zertifizierungen hierarchisch voneinander abhängen (Zertifizierungsinstanzen, Signatoren); definiert eine integre Zertifikatskette vom Signator zur Wurzel

Zertifizierungsinfrastruktur: Gesamtheit der bei den einzelnen Zertifizierungsprozessen und –dienstleistungen beteiligten Einheiten (Zertifizierungsstellen, Registrierungsstellen, Informationsdienst ...)

Zertifizierungsinstanz: siehe → Zertifizierungsdiensteanbieter

Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH.
A-1030 Wien, Landstraßer Hauptstraße 5

Sicherheits- und Zertifizierungskonzept: verbindliches Dokument, in dem das Vorgehen der Certification Authority a.sign Uni bei Zertifizierungen sowie technische und organisatorische Anforderungen an die Einheiten der Zertifizierungshierarchie definiert sind.

B Abkürzungen

Abkürzung	Bedeutung
CA	Zertifizierungsinstanz (Certification Authority)
CN	Common Name
CPS	Certification Practice Statement
CRL	Certificate Revocation List (Widerrufliste für Zertifikate)
DN	Distinguished Name
FTP	File Transfer Protocol
GRA	Globale Registrierungsstelle (Global Registration Authority)
GUID	Globally Unique Identifier
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol with SSL
ITSEC	Information Technology Security Evaluation Criteria
LRA	Lokale Registrierungsstelle (Local Registration Authority)
MIME	Multipurpose Internet Mail Extensions
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
RSA	Rivest Shamir and Adelman Public Key Cryptographic System
S/MIME	Secure/Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer
URL	Uniform Resource Locator
WWW	World Wide Web