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

Certification Practice Statement a.sign Projects

Version: 2.0.5

Datum: 16.01.2003

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

VORWORT

Die Policy Working Group hat die Aufgabe, das a.sign Certification Practice Statement (CPS) für die Signatur- und Zertifizierungsdienste a.sign Projects User Light, User Strong und User Strong plus des Zertifizierungsdienstanbieters A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH auf der Grundlage der Policies für a.sign Projects (für User Zertifikate Light, User Zertifikate Strong und User Zertifikate Strong plus) zu entwickeln

Hinweis: Zertifikate a.sign Uni (=qualifizierte Zertifikate) werden in eigens dafür vorgesehenen Dokumenten geregelt.

ZUSAMMENFASSUNG

Vorbemerkungen:

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 Certification Practice Statements (CPS) verwiesen.

1. Dieses Certification Practice Statement regelt die Implementierung der angebotenen a.sign Zertifizierungsdienstleistungen (Beantragung, Ausstellung, Abholung, Gebrauch, Verlängerung und Widerrufen eines Zertifikates usw.) durch User Zertifikate Light, Strong und Strong plus.

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

3. Unter der Marke a.sign werden verschiedene User Zertifikate angeboten (Kapitel 1.3.1).

4. Das Schlüsselpaar (bestehend aus Öffentlichem und Privatem Schlüssel) wird vom Signator generiert. Der private Schlüssel ist entsprechend - durch Passwort oder PIN - zu schützen.

5. Für die Beantragung, Ausstellung und Abholung eines User Zertifikates existieren unterschiedliche Verfahren (Kapitel 4.2)

6. Vor dem Gebrauch eines Zertifikates muss der Signator das Zertifikat akzeptieren (Kapitel 4.2.6). Mit diesem Akzeptieren des Zertifikates erklärt sich der Signator mit den Zertifikatinhalten sowie mit den an das Zertifikat geknüpften Bedingungen einverstanden.

7. Jeder Empfänger einer Digitalen Signatur (Dritter) ist dazu verpflichtet, die Digitale Signatur bzw. das zugehörige Zertifikat zu überprüfen, bevor er der Digitalen Signatur bzw. dem Zertifikat vertraut (Kapitel 2.1.5).

8. a.sign Zertifikate können verlängert werden (Kapitel 4.3).

9. In bestimmten Fällen müssen Signatoren oder Certification Authorities (CAs) ein Zertifikat widerrufen (Kapitel 4.5.1). Die zulässigen Verfahren für den Widerruf eines Zertifikates (Kapitel 4.5.3) sowie für die Veröffentlichung widerrufener Zertifikate (Kapitel 4.5.4) werden in diesem a.sign Certification Practice Statement definiert.

10. Dieses Certification Practice Statement regelt zusätzlich Bereiche im Umfeld des eigentlichen Zertifizierungsprozesses, wie beispielsweise Haftungsfragen

(Kapitel 2.2), die rechtliche Bedeutung von Zertifikaten (Kapitel 2.3), Entgelte (Kapitel 2.4), interne Kontrollen (Datenschutz (Kapitel 2.6), Urheberrechte (Kapitel 2.7), Behandlung von Ausnahmesituationen (Kapitel 4.8, 4.9), Sicherheitsmaßnahmen (Kapitel 5 und 6), Profil von a.sign Zertifikaten (Kapitel 7.1) sowie die Administration dieses Certification Practice Statements (Kapitel 8).

Inhaltsverzeichnis

Tabellenverzeichnis

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

1 Einführung

Dieses Kapitel gibt dem Leser einen Überblick über das vorliegende Dokument und beschreibt die Einheiten, die am a.sign Zertifizierungsdiensteanbieter beteiligt sind, sowie die Einsatzmöglichkeiten der ausgestellten Zertifikate. Der Leser erhält in den einzelnen Teilkapiteln u.a. Informationen zu folgenden Fragen:

1.1 Überblick:

- Worin besteht das Ziel dieses Dokumentes?
- Welcher Zusammenhang besteht zwischen dem CPS und den restlichen a.sign Dokumenten?
- Welche Beziehung besteht zwischen Zertifikaten und dem entsprechenden CPS?
- Welche Rolle spielen die Allgemeinen Geschäftsbedingungen des Zertifizierungsdiensteanbieters?

1.2 Identifikation des Certification Practice Statements

- Wie lautet die offizielle Bezeichnung des CPS?
- Wie lautet der Object Identifier des CPS?

1.3 a.sign Zertifizierungsinfrastruktur und Anwendungsbereiche

- Welche unterschiedlichen Registrierungsverfahren gibt es?
- Welche Anwendungsbereiche von Zertifikaten gibt es?
- Welche Einheiten bilden die a.sign Zertifizierungsinfrastruktur?
- Wie sieht der hierarchische Aufbau der Zertifizierungsinfrastruktur aus?

1.4 Kontaktinformation

- Wie kann man den Zertifizierungsdiensteanbieter kontaktieren?

1.1 Überblick

1.1.1 Ziel dieses Dokumentes

Das Ziel des vorliegenden a.sign Certification Practice Statements (CPS) besteht darin, die Umsetzung der Ausgabe, Administration und Anwendung von a.sign Zertifikaten derart festzulegen, dass eine sichere und zuverlässige Durchführung der angebotenen a.sign Zertifizierungsdienstleistungen sowie der Anwendung der ausgegebenen Zertifikate gewährleistet ist.

1.1.2 Verhältnis des a.sign CPS zu den weiteren a.sign Projects Dokumenten

Die Dokumente des a.sign Zertifizierungsdiensteanbieters für die User Zertifikate Light, User Zertifikate Strong und User Zertifikate Strong Plus bilden aufgrund ihrer Funktionen eine 3-stufige Hierarchie (siehe nachstehende Abbildung):

- Die a.sign Policies Project (Light, Strong und Strong Plus) enthält die globalen Richtlinien, die von den Service-Betreibern und Signatoren einzuhalten sind. Jede Policy bezieht sich dabei auf ein bestimmtes User Zertifikat (Light und Strong und Strong plus) und ist öffentlich zugänglich.

- Das Certification Practice Statements (CPS) enthält Angaben darüber, wie die in den a.sign Policies Projects Light, Strong und Strong plus enthaltenen globalen Richtlinien von der jeweiligen CA umgesetzt werden. Da das CPS den Signatoren und Dritten die Einschätzung der Qualität der ausgegebenen Zertifikate erleichtert, wird das CPS ebenfalls veröffentlicht.

- Das vorliegende Dokument (a.sign CPS Projects) enthält die Umsetzung der a.sign Policies.

- 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 CPS

Jedes a.sign Zertifikat enthält Verweise auf die entsprechende a.sign Policy Projects sowie auf das CPS der CA, sodass dem Anwender des Zertifikats die Möglichkeit

eingeräumt wird, sich darüber zu informieren, welche Richtlinien bzw. Realisationen dieser Richtlinien dem Zertifikat zugrunde liegen und ob das Zertifikat den Erfordernissen des geplanten Verwendungszwecks genügt.

Bemerkung: Derzeit sind die Verweise indirekt durch Angabe des-Domain-Name im Zertifikat realisiert.

1.1.4 Beziehung zwischen den AGB und dem a.sign CPS Projects

Das a.sign CPS Projects stellt eine Erweiterung der Allgemeinen Geschäftsbedingungen (AGB) der A-Trust GmbH dar. Informationen über diese Allgemeinen Geschäftsbedingungen finden Sie auf folgender Webseite:
http://www.a-trust.at.

1.2 Identifikation des Certification Practice Statement Projects

Name des CPS: a.sign Certification Practice Statement für a.sign Projects / Version 2.0.5.

1.3 a.sign Zertifizierungsinfrastruktur und Anwendungsbereiche

1.3.1 Klassen von Zertifikaten für Signatoren

a.sign bietet User Zertifikate verschiedener Klassen an. Der wesentliche Unterschied zwischen den einzelnen Zertifikatsklassen liegt in den angewandten Registrierungsverfahren.

Klasse	Definition	Typen
Light	automatische, indirekte Überprüfung der E-Mail-Adresse des Signators	User
Strong	persönliche Überprüfung der im Zertifikat abgebildeten Zertifikatswerber-Daten	User
Strong Plus	persönliche Überprüfung der im Zertifikat abgebildeten Signator-	User

Klasse	Definition	Typen
	Daten; das Schlüsselpaar des Signators wird auf einer Smartcard bzw. einem sicheren Token gespeichert	
Uni	Persönliche Überprüfung der im Zertifikat abgebildeten Signator-Daten, das Schlüsselpaar des Signators muss auf einer Smartcard bzw. einem sicheren Token gespeichert sein	User

Tabelle 1 Zertifikatsklassen

1.3.2 Einheiten der a.sign Zertifizierungsinfrastruktur

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

1.3.2.1 CA Projects

Die CA Projects stellt Zertifikate für Signatoren aus und ist für das Management von Zertifikaten für Signatoren verantwortlich.

Das a.sign CPS legt die Richtlinien der a.sign CA Projects fest.

1.3.2.2 GRAs

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

1.3.2.3 LRAs

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

1.3.2.4 Signatoren

Signatoren von a.sign Zertifikaten sind natürliche Personen.

1.3.2.5 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 a.sign Zertifizierungsdiensteanbieter

Kontaktinformationen bez. des a.sign Zertifizierungsdiensteanbieters finden Sie in folgender Tabelle:

Name:	A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH
Adresse:	A-1030 Wien Landstraßer Hauptstraße 5
Telefon:	0800/501 555
Web:	http://www.a-trust.at

Tabelle 2 Kontaktinformation

1.4.2 a.trust Web-Schnittstellen

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

A-Trust Web

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 Richtlinien

Tabelle 3 a.trust Web-Schnittstellen

Informationsdienst:

Die Abfrage der User Zertifikate ist über

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

möglich.

Die User CRL kann über

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

abgefragt werden.

2 Allgemeine Richtlinien

In diesem Kapitel wird dem Leser ein Überblick über die allgemeinen Grundlagen der angebotenen Signatur- und Zertifizierungsdienste gegeben. Die einzelnen Teilkapitel enthalten u. a. Informationen zu folgenden Fragen:

2.1 Pflichten

- Welche Verpflichtungen haben die einzelnen Einheiten der Zertifizierungsinfrastruktur (GRAs, LRAs, Signatoren, Dritte, Informationsdienst)?

2.2 Haftung

- Für welche Schäden haften die a.sign CA, GRAs und LRAs?
- Für welche Schäden haften die angegebenen Einheiten nicht?
- Welche Einschränkungen bzgl. der Haftung und welche Limits für Schadenersatzansprüche bestehen?
- Welche Gründe für den Ausschluss einer Haftung sind zu beachten?

2.3 Rechtliche Hinweise

- Auf welchen rechtlichen Grundlagen beruhen die a.sign Signatur- und Zertifizierungsdienste?
- Welche rechtliche Bedeutung haben a.sign Zertifikate?

2.4 Entgelte

- Wo kann man sich über die Höhe der Entgelte für die angebotenen Dienstleistungen informieren?

2.5 Veröffentlichungen

- Welche Informationen werden vom Zertifizierungsdienstеanbieter veröffentlicht?
- In welchen Abständen werden diese Veröffentlichungen durchgeführt?
- Wer führt diese Veröffentlichungen durch? Wie werden diese Veröffentlichungen duchgeführt?

2.6 Datenschutz

- Welche Daten und Informationen sind als vertraulich anzusehen?
- Welche Daten und Informationen werden veröffentlicht?

2.7 Urheber- und Eigentumsrechte

- Wer besitzt die Urheber- und Eigentumsrechte für Zertifikate, Zertifizierungs-richtlinien, Namen und Schlüssel?

2.1 Pflichten

2.1.1 Verpflichtungen der a.sign CA Projects

2.1.1.1 Allgemeine Verpflichtungen

Die a.sign CA Projects hält die Richtlinien die Richtlinien dieses Dokumentes (a.sign CPS Projects) ein. Dies bedeutet insbesondere, dass die CA

- die in den entsprechenden Policies Projects Light, Strong und Strong plus sowie in diesem CPS spezifizierten Identifikations- und Authentifikations-Mechanismen sicherstellt,
- Zertifikate für Signatoren gemäß der entsprechenden Policy Projects Light, Strong und Strong plus sowie gemäß dieses CPS ausstellt,
- Zertifikate für Signatoren gegebenenfalls widerruft,
- den unter Punkt 2.1.1.5 angeführten 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 a.sign CA Projects sorgt durch geeignete organisatorische, infrastrukturelle, personelle und sicherheitstechnische Maßnahmen für den Schutz des Privaten Schlüssels der CA.

2.1.1.3 Verwendung des Privaten Schlüssels der CA

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

2.1.1.4 Implementierung eines Sicherheitskonzeptes

Entsprechend den Abschitten 5 und 6 dieses CPS wird von der a.sign CA Projects ein Sicherheitskonzept entwickelt und implementiert.

2.1.1.5 Publikation / Information

Ausgestellte Zertifikate werden entsprechend den a.sign Richtlinien veröffentlicht (siehe Abschnitt 2.5.1.2). Zertifikatswerber werden von einer erfolgten Ausstellung des Zertifikates in Kenntnis gesetzt.

Widerrufene Zertifikate werden entsprechend der a.sign Richtlinien in Form von CRLs veröffentlicht (siehe Abschnitt 2.5.1.3). Zertifikatinhaber werden von einem erfolgten Widerruf ihres Zertifikates in Kenntnis gesetzt.

Die a.sign CA Projects unterrichtet den Zertifikatswerber über den Umgang mit Zertifikaten, den Umgang mit seinem Privaten Schlüssel, den Schutz seines Privaten Schlüssels und die Prüfung von Digitalen Signaturen.

2.1.2 Verpflichtungen von a.sign GRAs

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

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

2.1.3 Verpflichtungen von a.sign LRAs

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

Die a.sign LRAs halten die von der a.sign CA Projects 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 von der a.sign CA Projects in ihrem CPS festgelegten Richtlinien einzuhalten.

2.1.4.2 Schutz des Privaten Schlüssels

Signatoren sind verpflichtet,

- den Privaten Schlüssel zu schützen, d.h. den Zugriff anderer Personen auf den Privaten Schlüssel zu unterbinden sowie eine Weitergabe des Privaten Schlüssels zu unterlassen, und
- ausgestellte Zertifikate zu widerrufen, falls die Notwendigkeit dazu gegeben ist (siehe Abschnitt 4.5.1).

2.1.4.3 Einschränkungen bezüglich der Anwendung Privater Schlüssel bzw. ausgestellter Zertifikate

Signatoren ist es untersagt, selbst Zertifikate auszustellen.

a.sign User Zertifikate dürfen nur für den in der im a.sign CPS Projects festgelegten Zweck eingesetzt werden. Für a.sign Zertifikate gilt jene Version der a.sign Policy Projects bzw. des a.sign CPS Projects, die zum Zeitpunkt der Ausstellung des Zertifikates gültig war.

2.1.5 Verpflichtungen Dritter

Bevor ein Zertifikat durch Dritte akzeptiert wird, sind diese dazu verpflichtet,

- die Digitale Signatur des Zertifikates zu überprüfen,
- zu überprüfen, ob das Zertifikat abgelaufen ist,
- zu überprüfen, ob das Zertifikat widerrufen wurde,

- die Klasse des User Zertifikats Projects zu identifizieren und
- zu überprüfen, ob das Zertifikat für den entsprechenden Zweck eingesetzt werden darf.

2.1.6 Verpflichtungen des a.sign Informationsdienstes

Der a.sign Informationsdienst veröffentlicht im Auftrag der a.sign CA Projects 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 den Zertifizierungsdienstleistungen können dem nachfolgenden Kapitel 2.3 („Rechtliche Hinweise“) entnommen werden.

2.3 Rechtliche Hinweise

Beim Vorgang der Beantragung eines a.sign Zertifikates im Web hat der Signator explizit (durch Anklicken einer Checkbox) einer Einverständniserklärung zuzustimmen. Diese Einverständnis-erklärung enthält alle relevanten rechtlichen Hinweise im Zusammenhang mit a.sign Zertifikaten.

Zur Rechtswirkung der elektronischen Signatur basierend auf einem a.sign Projects User Zertifikat Light, Strong und Strong plus:

Gemäß dem Österreichischen Signaturgesetz (SigG) können im Rechts- und Geschäftsverkehr Signaturverfahren mit unterschiedlichen Sicherheitsstufen und unterschiedlichen Zertifikatsklassen verwendet werden. Die a.sign User Zertifikate Light, Strong und Strong Plus entsprechen nicht den qualifizierten Zertifikaten des Österreichischen Signaturgesetzes. Das bedeutet, dass die elektronische Signatur, basierend auf den a.sign User Zertifikat Light, Strong und Strong Plus zwar als Beweismittel verwendet werden können, nicht aber die Rechtswirkungen der eigenhändigen Unterschrift (=Schriftlichkeit) entfalten.

1. Dokumente, die mit den a.sign User Zertifikaten Light, Strong und Strong Plus signiert sind, können rechtliche Wirksamkeit entfalten und als Beweismittel verwendet werden.

2. Derart signierte Dokumente unterliegen der freien Beweiswürdigung

Daraus folgt, dass wenn man ein derart signiertes Dokument als Beweis verwenden möchte, es auch zugelassen werden muss, und nicht als "nullum" abgetan werden darf. (Nichtdiskriminierungsklausel gem. § 3(2) SigG) Wie es allerdings gewertet wird und welche tatsächliche Beweiskraft der Richter dem Dokument zukommen lässt, bleibt seiner freien Beweiswürdigung überlassen.

2.4 Entgelte

Die Entgelte für die angebotenen Dienstleistungen werden von der A-Trust GmbH festgelegt. Die aktuellen Entgelte sind dem Informationsdienst der A-Trust GmbH zu entnehmen.

Folgende Services der a.sign CA Projects sind kostenlos:

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

2.5 Veröffentlichungen

2.5.1 Veröffentlichte Inhalte

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

2.5.1.1 Richtlinien für die a.sign CA Projects

Das a.sign CPS Projects wird in der aktuellen und allen vorangegangenen Versionen durch den a.sign Informationsdienst via Web veröffentlicht.

2.5.1.2 Zertifikatsverzeichnisse

Die von der a.sign CA Projects 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 widerrufen.
Expired	Die Gültigkeit des Zertifikates ist abgelaufen.

Tabelle 4 Zertifikatsstatus

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.

Bemerkung: Derzeit ist das Angeben des Zeitpunktes eines Widerrufs nicht implementiert.

2.5.1.3 Widerrufslisten (CRLs)

Widerrufe von Zertifikaten werden mittels signierter CRLs vom Verzeichnisdienst veröffentlicht.

Widerrufene Zertifikate werden solange in den CRLs geführt, bis die ursprüngliche Gültigkeitsdauer des Zertifikates überschritten ist.

CRLs für User Zertifikate Projects Light, Strong und Strong plus werden bei jedem durchgeführten Zertifikat-Widerruf aktualisiert.

Zertifikatinhaber werden über einen erfolgten Widerruf informiert.

2.5.1.4 Unterrichtung von Signatoren

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

Dies erfolgt bei den User Zertifikate Light, Strong und Strong plus mittels folgender Verfahren:

Zertifikatsklasse	Verfahren
Light	online via Web durch den Informationsdienst
Strong + Strong plus	online via Web durch den Informationsdienst sowie persönlich in der LRA

Tabelle 5 Unterrichtung von Signatoren

2.5.2 Durchführung von Veröffentlichungen

Die a.sign CA Projects beauftragt 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 und
- Protokolldaten, die beim Beantragen, Verlängern und Widerrufen von Zertifikaten usw. archiviert wurden.

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 a.sign CA Projects zu.

2.6.2 Zu veröffentlichende Daten

2.6.2.1 Typen von zu veröffentlichenden Daten

Als zu veröffentlichende Daten gelten

- alle Zertifikatinhalte sowie
- CRLs.

2.6.2.2 Behandlung von zu veröffentlichenden Daten

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

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

2.7 Urheber- und Eigentumsrechte

Objekt	Urheberrecht / Eigentumsrecht	Bemerkungen
a.sign Policies Projects	Das Urheber- und Eigentumsrecht für diese Dokumente liegt ausschließlich beim Zertifizierungsdiensteanbieter.	Diese Dokumente bzw. Teile aus diesen Dokumenten dürfen ohne Zustimmung des Zertifizierungsdiensteanbieters nicht kopiert oder veröffentlicht werden.
Certification Practice Statement	Das Urheber- und Eigentumsrecht eines CPS liegt beim Zertifizierungsdiensteanbieter .	Diese Dokumente bzw. Teile aus diesen Dokumenten dürfen ohne Zustimmung des entsprechenden Zertifizierungsdiensteanbieters nicht kopiert oder veröffentlicht werden.
Zertifikat	Ein Zertifikat ist das Eigentum der aussstellenden CA Projcects.	Damit soll verhindert werden, dass von externen Organisationen Zertifikatsverzeichnisse für gewerbliche Zwecke erstellt werden können. Um den Gebrauch von Zertifikaten kundenfreundlicher gestalten zu können, wird folgende Ausnahme zu dieser Bestimmung vorgesehen: Die Erstellung von Kopien ist gestattet, falls diese zum Prüfen von Signaturen eingesetzt werden (z.B. Download von Wurzelzertifikaten).

Privater CA-Schlüssel	Der private Schlüssel der CA Projects ist das Eigentum der CA.	
Öffentlicher CA-Schlüssel	Der öffentliche Schlüssel der CA Projects ist das Eigentum der CA.	
Privater Schlüssel (Signator)	Jeder Private Schlüssel eines Signators ist das Eigentum des Signators.	
Öffentlicher Schlüssel (Signator)	Jeder Öffentliche Schlüssel eines Signators ist das Eigentum des Signators.	

Tabelle 6 Urheber- und Eigentumsrechte

3 Identifizierung, Authentifizierung

In diesem Kapitel wird dem Leser ein Überblick darüber gegeben, anhand welcher Merkmale Einheiten der Zertifizierungsinfrastruktur identifiziert werden und welche Authentifizierungsverfahren zulässig sind. Die einzelnen Teilkapitel enthalten u.a. Informationen zu folgenden Fragen:

3.1 Erstregistrierung

- Durch welche Namensstruktur wird die a.sign CA Projects festgelegt?
- Welche Identifikationsmerkmale von Signatoren enthalten die a.sign Zertifikate?
- Welche Ausweise sind bei der persönlichen Registrierung eines Signators zugelassen?
- Welche Daten eines Signators werden zusätzlich für die interne Verarbeitung erfasst?
- Welche Richtlinien bestehen bezüglich der Eindeutigkeit von Namen?
- Wie hat der Signator den Nachweis über den Besitz des Privaten Schlüssels zu erbringen?
- Wie wird die Identität des Signators bei User-Zertifikaten überprüft?

3.2 Verlängerung der Gültigkeit von Zertifikaten für Signatoren

- Welche Identifikations- und Authentifikationsverfahren werden bei der Verlängerung der Gültigkeit von a.sign Zertifikaten eingesetzt?

3.3 Widerruf von Zertifikaten für Signatoren

- Welche Identifikations- und Authentifikationsverfahren werden beim Widerruf von a.sign Zertifikaten eingesetzt?

3.1 Erstregistrierung

3.1.1 Identifikationsmerkmale

3.1.1.1 a.sign CA Projects

Der Name für die a.sign CA Projects wird durch folgende Namensstruktur eindeutig definiert:

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

3.1.1.2 Signatoren

Ein a.sign User Zertifikat der einzelnen Klassen enthält folgende persönliche Identifikationsmerkmale des Signators:

a.sign Projects - User-Zertifikat Light	
Attribut	**Anmerkung**
Vorname	
Nachname	
E-Mail-Adresse	
a.sign Projects - User –Zertifikat Strong und User Zertifikat Strong Plus	
Attribut	**Anmerkung**
Vorname	
Nachname	
E-Mail-Adresse	

Tabelle 7 Identifikationsmerkmale des Signators

3.1.1.3 Zulässige amtliche Lichtbildausweise

Die für eine persönliche Registrierung eines Signators zugelassenen Ausweise sind im Abschnitt 4.2.3 spezifiziert.

3.1.1.4 Zusätzlich erfasste Daten für interne Ablage

Die zusätzlich für die interne Ablage erfassten Daten können dem Abschnitt 4.2.2 (Enrollment-Daten) entnommen werden.

3.1.2 Eindeutigkeit der Identifikationsmerkmale

Die in a.sign User Zertifikaten angeführten Identifikationsmerkmale enthalten keinen eindeutigen Identifier (Sozialversicherungsnummer o.ä.), d.h. der Zertifikats-Inhaber kann aufgrund dieser Merkmale nicht eindeutig identifiziert werden.

3.1.3 Identitätsüberprüfung bei User-Zertifikaten

3.1.3.1 User-Zertifikate Light

- Für die Registrierung ist kein persönliches Erscheinen des Zertifikatswerbers bei der Registrierungsstelle erforderlich.
- Durch das Registrierungsverfahren wird die E-Mail-Adresse des Zertifikatswerbers indirekt überprüft.

3.1.3.2 User-Zertifikate Strong und Strong plus

- Für die Registrierung ist das persönliche Erscheinen des Zertifikatswerbers bei der Registrierungsstelle sowie das Vorlegen eines amtlich anerkannten Ausweisdokumentes (siehe Abschnitt 4.2.3) erforderlich.
- Durch das Registrierungsverfahren wird der Name des Zertifikatswerbers direkt überprüft.

3.2 Verlängerung der Gültigkeit von Zertifikaten für Signatoren

Das Verfahren zur Identifizierung bzw. Authentifizierung bei der Verlängerung der Gültigkeit eines Zertifikates ist zu jenem bei der Erstregistrierung identisch.

Bemerkung: Derzeit ist das Verlängern von Zertifikaten nicht implementiert.

3.3 Widerruf von Zertifikaten für Signatoren

Um eine rasche Abwicklung des Widerrufs eines Zertifikates zu ermöglichen, akzeptieren die a.sign CA Projects bzw. die ihr unterstellten LRAs folgende Identifikations- bzw. Authentifikationsmechanismen:

Mechanismus	Anwendbarkeit
Widerruf via Web	Zertifikate der Klassen Light, Strong und Strong plus
Widerruf via Telefon	Zertifikate Strong und Strong Plus

Tabelle 8 Widerruf

4 Verfahrensanforderungen

Dieses Kapitel gibt dem Leser einen Überblick über jene Bestimmungen und Anforderungen, die sich für die Einheiten der Zertifizierungsinfrastruktur bei den einzelnen Verfahren im Rahmen der Zertifizierungsdienstleistungen ergeben. Die Teilkapitel enthalten u.a. Informationen zu folgenden Fragen:

4.1 Zertifizierung der a.sign CA Projects

- Wie wird die a.sign CA Projects zertifiziert?

4.2 Zertifizierung von Signatoren

- Welche allgemeinen Eigenschaften besitzen die Verfahren zur Zertifizierung von Signatoren?
- Welche Signator-Daten werden beim Enrollment erfasst?
- Welche Ausweise und Dokumente werden beim Zertifizierungsprozess anerkannt?
- Welche Payment-Daten sind erforderlich?
- Wie sind die Zertifizierungsverfahren spezifiziert?
- Welche Bedeutung hat das Abschicken eines Zertifikatantrages bzw. das Abholen eines Zertifikates im Hinblick auf das Akzeptieren der Bestimmungen des a.sign Zertifizierungsdiensteanbieters und das Akzeptieren der Zertifikats-inhalte?

4.3 Verlängerung der Gültigkeit von Zertifikaten für Signatoren

- Wie verlängert man die Gültigkeit eines a.sign Zertifikates?

4.4 Überprüfung der Gültigkeit von Zertifikaten

- Wie überprüft man die Gültigkeit eines a.sign Zertifikates?

4.5 Widerruf von Zertifikaten

- Wann ist ein Zertifikat zu widerrufen?
- Wer ist dazu berechtigt, ein Zertifikat zu widerrufen?
- Wie sind die Verfahren zum Widerrufen von Zertifikaten der einzelnen Zertifikatsklassen definiert?

- Wie werden widerrufene Zertifikate veröffentlicht?

4.6 Schlüsselaustausch bei einem Signator

- Wie kann der Signator einen Schlüsselaustausch durchführen?

4.7 Archivierung

- Warum werden Informationen über wichtige Ereignisse und Aktionen archiviert?
- Welche Daten werden archiviert?
- Wie lange werden die archivierten Daten aufbewahrt?
- Wie werden die archivierten Daten vor Einsichtnahme, Manipulation und Löschen geschützt?
- Wie werden Sicherungen der archivierten Daten durchgeführt?
- Wo werden die archivierten Daten aufbewahrt?
- Wer besitzt Zugriffsrechte auf archivierte Daten?

4.8 Ausnahmesituationen bezüglich Privater Schlüssel einer a.sign CA

- Welche Maßnahmen werden beim Verlust eines Privaten CA-Schlüssels (ohne Kompromittierung) durchgeführt?
- Welche Maßnahmen werden beim Austausch des Privaten CA-Schlüssels durchgeführt?
- Welche Maßnahmen werden bei der Kompromittierung eines Privaten CA-Schlüssels durchgeführt?
- Welche Maßnahmen werden bei der Einstellung einer a.sign CA durchgeführt?

4.1 Zertifizierung der a.sign CA Projects

Die Zertifizierung der a.sign CA Projects erfordert

- die Genehmigung des von der a.sign CA Projects vorgelegten CPS,
- die Generierung des CA-Schlüsselpaares durch die CA selbst sowie

- die Unterzeichnung eines schriftlichen Vertrages, der die Einhaltung der definierten Richtlinien, insbesondere der definierten Sicherheitsbestimmungen garantiert.

4.2 Zertifizierung von Signatoren

4.2.1 Allgemeine Eigenschaften der Verfahren

	User Zertifikate Light	**User Zertifkate „Strong“**	**User Zertifikate „Strong Plus“**
Registrierung der persönlichen Daten des Zertifikatswerbers	E-Mail-Adresse (indirekt)	Name (direkt) E-Mail-Adresse (indirekt)	Name (direkt) E-Mail-Adresse (indirekt)
Management des Privaten Schlüssels des Signators	Der Private Schlüssel wird vom Signator selbst erzeugt und ist durch eine PIN oder ein persönliches Passwort zu schützen.	Der Private Schlüssel wird vom Signator selbst erzeugt und ist durch eine PIN oder ein persönliches Passwort zu schützen.	Der private Schlüssel wird in der lokalen Registrierungsstelle unter Anwesenheit des Zertifikats-werbers generiert und ist durch eine PIN zu schützen
Zertifizierung	Die Zertifizierung erfolgt online und automatisch.	Die Zertifizierung erfolgt offline. Der Zertifikats-Antrag muss vom LRA-Operator freigegeben werden.	Die Zertifizierung erfolgt offline. Der Zertifikats-Antrag muss vom LRA-Operator freigegeben werden
Zertifikatsausgabe	Die Zertifikat-Ausgabe erfordert die Kenntnis eines Codes und des Persönlichen Passwortes.	Die Zertifikat-Ausgabe erfordert die Kenntnis eines Codes und des Persönlichen Passwortes.	Die Zertifikat-Ausgabe erfolgt in der lokalen Registrierungsstelle

Tabelle 9 Verfahren des Zertifizierungsprozesses

4.2.2 Enrollment-Daten

4.2.2.1 User-Zertifikate Light

Information	v/o	ZI	Anmerkung
Beim Enrollment-Formular ist einzugeben:			
Vorname	V	ja	Die CA a.sign Projects behält sich vor, fallweise oder permanent zusätzliche, in dieser Tabelle nicht enthaltene Daten beim Enrollment zu erfassen.
Nachname	V	ja	
E-Mail-Adresse	V	ja	
Persönliches Passwort	V	nein	

Tabelle 10 Enrollment-Daten Strong

v/o ... verpflichtend / optional anzugeben

ZI ... Ist diese Information Zertifikat-Inhalt ?

4.2.2.2 User-Zertifikate Strong Plus

Information	v/o	ZI	Anmerkung
Beim Enrollment-Formular ist einzugeben:			
Vorname	v	ja	Die CA a.sign Projects behält sich vor, fallweise oder permanent zusätzliche, in dieser Tabelle nicht enthaltene Daten beim Enrollment zu erfassen.
Nachname	v	ja	
E-Mail-Adresse	v	ja	
Akad. Titel (falls vorhanden)	v/o	nein	
Geburtsdatum	v	nein	
Geburtsort	v	nein	
Geschlecht	v	nein	
Weitere Daten des Zertifikatswerbers: Firmen- oder Wohnadresse (Straße, Postleitzahl, Ort, Land) Telefonnummer Faxnummer	 v o o	 nein nein nein	
Weitere (rechtlich erhebliche) Angaben	o	ja	
Typ des verwendeten Ausweises (Reisepass, Führerschein oder Personalausweis)	v	nein	
Ausweisnummer	v	nein	
Persönliches Passwort	v	nein	
Schlüssel-Länge	v	ja	
Der Zertifikatswerber hat zur LRA mitzubringen:			
Bestätigung über die Identität des Zertifikatswerbers	v	nein	Reisepass, Führerschein oder Personalausweis

Tabelle 11 Enrollment-Daten Strong Plus

v/o ... verpflichtend / optional anzugeben

ZI ... Ist diese Zertifikat-Inhalt?

4.2.3 Zugelassene Ausweise und Dokumente

Der Nachweis der im vorigen Abschnitt (Kapitel 4.2.2) spezifizierten Informationen ist nur mit den in der unten angegebenen Tabelle angeführten Ausweisen und Dokumenten zulässig:

Überprüfte Einheit		Zugelassener Ausweis, zugelassenes Dokument
Signator	In- und Ausland	Reisepass Führerschein (ausgestellt von einer österreichischen Behörde) oder Personalausweis (ausgestellt von einer österreichischen Behörde)
Firma	Inland	Gewerbeschein, Firmenbuchauszug
	Ausland (EU-Land)	Firmenbuchauszug
Verein		Amtsbestätigung, ausgestellt von Bundespolizeidirektion bzw. Bezirkshauptmannschaft
Andere Organisationsformen (Botschaft, Stiftung usw.)		keine Vorgaben

Tabelle 12 Zugelassene Ausweise und Dokumente

4.2.4 Payment-Daten

Bei allen a.sign Zertifikaten müssen beim Enrollment zusätzlich folgende Payment-Informationen angegeben werden:

Information	v/o	ZI
Kreditkartentyp bzw. Prepaid-Modus	v	nein
Kreditkartennummer bzw. Prepaid-Code	v	nein
Ablaufdatum der Kreditkarte	v	nein

Tabelle 13 Payment-Informationen

v/o ... verpflichtend / optional anzugeben

ZI ... Ist diese Information im Zertifikat enthalten ?

4.2.5 Spezifikation der einzelnen Verfahren

4.2.5.1 User-Zertifikate Light

Schritt	Aktion	Input	Output	Ort
1	Zertifikat-Antrag: Ausfüllen der Enrollment-Page im Web Generierung des Schlüsselpaares durch die Client-Software des Signators Generierung eines PKCS#10-Requests durch die Client-Software des Signators, Übermittlung des Requests an die CA Projects über eine SSL-Verbindung im Web	Daten des Signators	Schlüssel-paar, PKCS#10-Request	Terminal des Signators
2	Zertifikat-Ausstellung: online-Generierung des Zertifikates in der CA Projects Zertifikat wird von der CA zum Abholen freigegeben	PKCS#10-Request	Zertifikat des Signators	ausstellende CA Projects
3	Abholen und Akzeptieren des Zertifikates: CA Projects informiert Zertifikatswerber via E-Mail von der abgeschlossenen Generierung des Zertifikates sowie über Details zum Abholen des Zertifikates (Abhol-Code usw.) Abholung des Zertifikates durch den Signator über eine SSL-Verbindung im Web (erfordert die Kenntnis des Abhol-Codes) automatische Installation des Zertifikates in der Client-Software des Signators Überprüfung, ob die Installation des Zertifikates fehlerfrei ausgeführt wurde	Informations-E-Mail an den Signator	in der Client-Software des Signators installiertes Zertifikat	ausstellende CA - Projects, Terminal des Signators

Tabelle 14 Verfahren bei User Light Zertifikaten

4.2.5.2 User-Zertifikate Strong

User Zertifikate der Klasse Strong werden in zwei Varianten angeboten:

4.2.5.2.1 User Zertifikat Strong (Softwarezertifikat)

Schritt	Aktion	Input	Output	Ort
1	Zertifikat-Antrag: Ausfüllen der Enrollment-Page im a.sign Web Generierung des Schlüsselpaares durch die Client-Software des Signators Generierung eines PKCS#10-	Daten des Signators	Schlüssel-paar	Terminal des Signators

Schritt	Aktion	Input	Output	Ort
	Requests durch die Client-Software des Signators, Übermittlung des Requests an die CA über SSL-Verbindung im Web			
2	Authentifizierung des Signators und Überprüfung der Signator-Daten in der LRA: Signator erhält von der CA eine Informations-E-Mail (Inhalt: Aufforderung, eine LRA aufzusuchen, sowie interne Antragsnummer) Signator nennt dem LRA-Operator die interne Antragsnummer Überprüfung der Inhalte der mitgebrachten Dokumente des Signators Unterzeichnung eines schriftlichen Vertrages durch LRA-Operator Übermittlung eines signierten elektronischen Zertifikat-Antrages an die CA	vom Signator mitge-brachte Dokumente	schriftlicher Vertrag, signierter elektron. Antrag, Freigabe des Zertifikat-Antrages	LRA
3	Zertifikat-Ausstellung: Generierung des Zertifikates in der CA nach erfolgter Freigabe des Zertifikat-Antrages durch den LRA-Operator Zertifikat wird von der CA zum Abholen freigegeben	PKCS#10-Request, Freigabe des Zertifikat-Antrages	Zertifikat des Signators	ausstellende CA
4	Abholen und Akzeptieren des Zertifikates: CA informiert Zertifikatswerber via E-Mail von der abgeschlossenen Generierung des Zertifikates sowie über Details zum Abholen des Zertifikates (Abhol-Code) Abholung des Zertifikates durch den Signator über eine SSL-Verbindung im Web (erfordert die Kenntnis des Abhol-Codes) automatische Installation des Zertifikates in der Client-Software des Signators Überprüfung, ob die Installation des Zertifikates fehlerfrei ausgeführt wurde	Informations-E-Mail an den Signator	in der Client-Software des Signators installiertes Zertifikat	ausstellende CA, Terminal des Signators

Tabelle 15 Verfahren bei User Strong Zertifikat

4.2.5.2.2 User-Zertifikate Strong Plus (in Verbindung mit Chipkarte)

Schritt	Aktion	Input	Output	Ort
1	Zertifikat-Antrag erfolgt in der lokalen Registrierungsstelle	Daten des Zertifikats-werbers	Zertifikats-antrag	Lokale Registrierungsstelle
2	Authentifizierung des Signators und Überprüfung der Signator-Daten in der LRA: Überprüfung des Zertifikatswerbers und der im Zertifikatsantrag enthaltenen Daten anhand des amtlichen Lichtbildausweises	vom Signator mitge-brachte Dokumente	Schriftlicher Vertrag, signierter elektron. Antrag, Schlüssel-paar,	LRA

Schritt	Aktion	Input	Output	Ort
	Unterzeichnung eines schriftlichen Vertrages durch LRA-Operator und Signator Eingabe der Benutzer-PIN durch den Signator Generierung des Schlüsselpaares auf der Chipkarte Übermittlung eines signierten elektronischen Zertifikat-Antrages an die CA		Freigabe des Zertifikat-Antrages	
3	Zertifikat-Ausstellung: Generierung des Zertifikates in der CA nach erfolgter Freigabe des Zertifikat-Antrages durch den LRA - Operator Zertifikat wird von der CA zum Abholen freigegeben	Freigabe des Zertifikatsantrages	Zertifikat des Signators	ausstellende CA
4	Abholung des Zertifikates über SSL automatische Speicherung des Zertifikates auf der Chipkarte des Signators Übergabe der Chipkarte an den Signator			Lokale Registrierungsstelle

Tabelle 16 Verfahren bei User Strong Plus Zertifikat

4.2.6 Akzeptieren von Zertifikaten

4.2.6.1 Abschicken des Zertifikatantrages

Der Vorgang des Abschickens des Zertifikatantrages durch den Signator beinhaltet das Akzeptieren der im Antragsformular enthaltenen Einverständniserklärung und hat daher folgende Bedeutung:

- Der Signator nimmt zur Kenntnis, dass die a.sign Dienstleistungen im a.sign CPS der CA Projects, in den a.sign Policies Projects sowie in den Allgemeinen Geschäftsbedingungen der A-Trust GMBH geregelt werden.

- Der Signator akzeptiert alle im a.sign CPS der CA Projects, in den a.sign Policies Projects sowie in den Allgemeinen Geschäftsbedingungen der A-Trust GmbH enthaltenen Bestimmungen. Insbesondere akzeptiert der Signator die im CPS der CA Projects enthaltenen Verpflichtungen von Signatoren.

4.2.6.2 Abholen des beantragten Zertifikates

Nach der Generierung seines Zertifikates bekommt der Signator eine E-Mail, die Angaben über

- die im Zertifikat enthaltenen Inhalte sowie

- den zulässigen Verwendungszweck des Zertifikates

enthält. Der Vorgang des Abholens dieses beantragten Zertifikates durch den Signator hat implizit folgende Bedeutung:

- Der Signator bestätigt die Richtigkeit aller in diesem Zertifikat enthaltenen persönlichen Daten.
- Der Signator akzeptiert alle in diesem Zertifikat enthaltenen Daten.

Hinweis: Bei User Zertifikaten Strong Plus impliziert das Unterschreiben des Zertifikatsantrages die Richtigkeit der im Zertifikat enthaltenen persönlichen Angaben und das Akzeptieren aller im Zertifikat enthaltenen Daten.

Bemerkung: Derzeit sind die Zertifikatinhalte und der zulässige Verwendungszweck nicht in den übermittelten E-Mails enthalten.

4.3 Verlängerung der Gültigkeit von Zertifikaten für Signatoren

Bei der online-Verlängerung der Gültigkeit eines a.sign Zertifikates für Signatoren wird vom Signator kein neues Schlüsselpaar generiert, sondern der Öffentliche Schlüssel des Zertifikatinhabers von der entsprechenden Zertifizierungsinstanz erneut zertifiziert. Im Gegensatz zur Beantragung eines neuen Zertifikates kann der Zertifikatinhaber daher seinen Privaten Schlüssel weiterhin verwenden. Die Daten des Signators, die im Zertifikat enthalten sind, dürfen sich aber nicht geändert haben.

Eine Verlängerung von widerrufenen Zertifikaten ist ausgeschlossen.

Die Gültigkeitsdauer von Zertifikaten ist in Abschnitt 6.4 angeführt.

Bemerkung: Derzeit ist das Verlängern von Zertifikaten nicht implementiert.

4.4 Überprüfung der Gültigkeit von Zertifikaten

Die a.sign CA Projects 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/.

4.5 Widerruf von Zertifikaten

Der Widerruf von Zertifikaten ist rund um die Uhr möglich.

Ein Widerruf enthält den Zeitpunkt, von dem an er gilt. Ein rückwirkender Widerruf von Zertifikaten ist nicht möglich.

4.5.1 Gründe für den Widerruf eines Zertifikates

Der Widerruf eines Zertifikates 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.

Die a.sign CA Projects ist berechtigt, ein Zertifikat für Signatoren zu widerrufen, falls sich der Zertifikatinhaber nicht an die mit dem Zertifikat verknüpften Bestimmungen hält. Hinweis: Der Zertifikatsinhaber wird – soweit möglich – vor der Durchführung des Widerrufs des Zertifikats benachrichtigt.

4.5.2 Zum Widerruf Berechtigte

Der Widerruf eines Zertifikates kann jederzeit und ohne Angabe von Gründen durch a.sign CA Projects bzw. den Zertifikatinhaber erfolgen.

4.5.3 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 Projects 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.
- Im Fall des Todes des Zertifikatsinhabers kann das Zertifikat durch den Erben – mit Nachweis der Todesurkunde – widerrufen werden.
- Im Falle der Entmündigung ist der Widerruf durch den gerichtlich bestellten Vormund unter Nachweis der Vertretungsvollmacht vorzunehmen.

4.5.3.1 Widerruf eines Zertifikates via Web

Die Durchführung eines Zertifikat-Widerrufes via Web ist für Zertifikate der Klasse Light, Strong und Strong plus möglich.

Schritt	Aktion	Input	Output	Location
1	Durch Eingabe der erforderlichen persönlichen Daten (siehe unten) wird ein Antrag auf Widerruf abgesetzt. Folgende persönliche Daten sind einzugeben: Light: Vorname, Nachname, Pers. Passwort, Reason Code (optional) Strong und Strong plus: Vorname, Nachname, Geburtsort, Geburtsdatum, Pers. Passwort, Reason Code (optional)	persönliche Signator-Daten	Antrag auf Widerruf	Terminal des Signators, ausstellende CA
2a	Ist die Zuordnung erfolgreich, d.h. gibt es eine Übereinstimmung bzgl. der übermittelten persönlichen Daten, so wird das entsprechende Zertifikat revoziert. (Bemerkung: Sollten mit den angegebenen persönlichen Daten mehrere Zertifikate referenziert werden, so werden diese dem Zertifikatswerber zur Selektion angeboten.)	erfolgreiche Übereinstimmung	Zertifikat-Widerruf, Informations-E-Mail an den Signator	Terminal des Signators, ausstellende CA

Schritt	Aktion	Input	Output	Location
2b	Schlägt die Zuordnung fehl, so wird das entsprechende Zertifikat nicht revoziert.	fehlende Übereinstimmung	Informations-E-Mail an den Signator	Terminal des Signators, ausstellende CA

Tabelle 17 Widerruf eines Zertifikates via Web

4.5.3.2 Widerruf eines Zertifikates via Telefon

Die Durchführung eines Zertifikat-Widerrufes via Telefon ist für Zertifikate Strong und Strong plus möglich.

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: Strong und Strong Plus: Vorname, Nachname, Geburtsort, Geburtsdatum, Pers. Passwort, Reason Code (optional)	persönliche Signator-Daten		Aufstellungsort des vom Zertifikatswerber verwendeten Telefons, ausstellende CA
2a	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. (Bemerkung: Sollten mit den angegebenen persönlichen Daten mehrere Zertifikate referenziert werden, so werden diese dem Zertifikatswerber zur Selektion angeboten.)	erfolgreiche Übereinstimmung	Zertifikat-Widerruf, Informations-E-Mail an den Signator	Aufstellungsort des vom Zertifikatswerber verwendeten Telefons, ausstellende CA

Schritt	Aktion	Input	Output	Location
2b	Ist die Zuordnung nicht möglich, so wird dem Signator das Fehlschlagen des Revozierungsantrages mitgeteilt. Es obliegt dem CA-Operator zu entscheiden, ob weitere Versuche zum Revozieren unternommen werden (z.B. bei Problemen mit der Schreibweise von Doppelnamen, mehreren Vornamen etc.). Mehrere Versuche bezüglich Variationen in diesen Fällen sollten möglich sein.	fehlende Übereinstimmung	Mitteilung an den Zertifikat-Inhaber	Aufstellungsort des vom Zertifikatswerber verwendeten Telefons, ausstellende CA

Tabelle 18 Widerruf eines Zertifikates via Telefon

Bemerkung: Derzeit ist das Widerrufen von Zertifikaten via Telefon nicht implementiert.

4.5.4 Veröffentlichung widerrufener Zertifikate

Widerrufe von Zertifikaten werden in Form von CRLs unter Einhaltung der in Abschnitt 2.5.1.3 angeführten Bestimmungen veröffentlicht.

4.6 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 (siehe Abschnitt 4.2).

4.7 Archivierung

4.7.1 Zielsetzung

In diesem Kapitel wird beschrieben,

- wie der Bereich Archivierung geregelt wird und

- wozu die Archivierung von Daten über eingetretene Ereignisse durchgeführt wird.

Die a.sign CA Projects 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 a.sign Certification Practice Statement angeführten Zertifizierungsrichtlinien und Sicherheitsmaßnahmen dokumentieren zu können.

4.7.2 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
  - usw.
- Management des Privaten CA-Schlüssels
  - Protokollierung jedes Einsatzes des Privaten CA-Schlüssels
- CA-Management
  - Anlegen der 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 CA Projects arbeitet.

4.7.3 Archivierungsdauer

Abhängig von der Zertifikatsklasse des Zertifikates, auf das sich das aufgezeichnete Ereignis bezieht, werden die Aufzeichnungen über folgende Zeiträume aufbewahrt:

Zertifikatsklasse	Aufbewahrungsdauer
Light	7 Jahre
Strong + Strong plus	15 Jahre

Tabelle 19 Archivierungsdauer

Die Archivierungsdauer von Daten, die sich auf Zertifikate aller Klassen beziehen, wird auf 15 Jahre festgelegt.

4.7.4 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.

4.7.5 Datensicherung

Der Systemadministrator der a.sign CA Projects (siehe Kapitel 5.2) erstellt täglich eine Sicherung des Archivs.

4.7.6 Aufbewahrungsort der Aufzeichnungen

Die angefallenen Daten werden intern in geeigneter Form aufbewahrt. Zusätzlich werden die in Abschnitt 4.7.5 angesprochenen Datensicherungen an einen externen Ort gebracht und dort in geeigneter Weise aufbewahrt.

4.7.7 Zugriff auf Aufzeichnungen

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

4.8 Ausnahmesituationen bezüglich Privater Schlüssel der a.sign CA Projects

4.8.1 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 a.sign CA Projects mit einem neuen CA-Schlüssel den Betrieb fort, so geht sie analog zu Abschnitt 4.8.2 (Austausch eines Privaten CA-Schlüssels) vor.
- Stellt die a.sign CA Projects hingegen ihren Betrieb ein, so geht sie analog zu Abschnitt 4.9 (Einstellen des Betriebes einer CA) vor.

4.8.2 Austausch eines Privaten CA-Schlüssels

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

- Die a.sign CAProjects generiert ein neues Schlüsselpaar. Dieser Punkt 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.

4.8.3 Kompromittierung des Privaten CA-Schlüssels

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

- Informierung jedes Inhabers eines gültigen, von der CA Projects mit dem kompromittierten Schlüssel signierten Zertifikates
- Revozieren des CA-Zertifikates

- Generieren eines neuen Schlüsselpaares und Ausstellung eines neuen CA-Zertifikates
- 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 weitergeführt, um authentische CRLs veröffentlichen zu können.
- Jedem Signator wird von der a.sign CA Projects ein neues Zertifikat ausgestellt.

4.9 Einstellen des Betriebes einer a.sign CA

Bei der dauerhaften Einstellung des Betriebes der a.sign CA Projects werden folgende Maßnahmen durchgeführt:

- Jeder Inhaber eines gültigen, von der CA Projects ausgestellten Zertifikates werden spätestens 3 Monate vor der geplanten Einstellung der CA Projects informiert.
- Die geplante Einstellung der CA Projects wird bereits 3 Monate vorher in geeigneter öffentlicher Form bekanntgegeben.
- Zum Zeitpunkt der Terminierung der CA Projects werden alle zu diesem Zeitpunkt noch gültigen, d.h. weder revozierten noch abgelaufenen Zertifikate für Signatoren von der CA widerrufen.
- Alle von den im vorigen Punkt spezifizierten Widerrufen betroffenen Zertifikats-inhaber werden vom Widerruf ihres Zertifikates informiert.
- Der Zertifizierungsdiensteanbieter sorgt dafür, dass die CRLs bzgl. der terminierten CA Projects auch nach der Terminierung öffentlich und authentisch zur Verfügung stehen.
- Der Zertifizierungsdiensteanbieter sorgt für die Sicherung aller relevanten, von der betroffenen a.sign CA Projects gespeicherten Daten (Zertifikate, CRLs, Audit Log Files usw.).

5 Infrastrukturelles, organisatorisches und personelles Sicherheitskonzept

Dieses Kapitel beschreibt alle Sicherheitsanforderungen an die a.sign CA Projects, GRAs, LRAs und Signatoren (ausgenommen technische Sicherheitsanforderungen). Damit soll eine zuverlässige und vertrauenswürdige Abwicklung von Schlüsselgenerierung, Authentifizierung, Zertifikat-Ausstellung, Zertifikat-Widerruf sowie Audit- und Archivierungsvorgängen gewährleistet und vor allem Missbrauch von Privaten Schlüsseln verhindert werden. Die Teilkapitel enthalten u.a. Informationen zu folgenden Fragen:

5.1 Infrastrukturelle Sicherheitsmaßnahmen

- Wo befinden sich die einzelnen Komponenten des Zertifizierungssystems?
- Welche Zugangskontrollen werden eingesetzt?
- Wie wird eine zuverlässige Stromversorgung gewährleistet?
- Wie wird eine zuverlässige Klimatisierung gewährleistet?
- Wie wird eine zuverlässige Feuerprävention gewährleistet?
- Welche Möglichkeiten zur Aufbewahrung von Datenmaterial stehen zur Verfügung?
- Wie ist die Abfallentsorgung geregelt?

5.2 Organisatorische Sicherheitsmaßnahmen

- Welche organisatorischen Sicherheitsmaßnahmen (Vieraugenprinzip, Aufgabenverteilung usw.) werden eingesetzt?

5.3 Personelle Sicherheitsmaßnahmen

- Wie erfolgt die Auswahl und Überprüfung von Personal für vertrauliche Aufgaben?
- Welche stellenbezogenen Einschulungsmaßnahmen werden getroffen? Welche begleitenden, aufgabenspezifischen Schulungen werden durchgeführt?
- Mit welchen Sanktionen hat das Personal bei Verstößen gegen die Vorschriften zu rechnen?

Die a.sign CA Projects definiert im vorliegenden CPS ein Sicherheitskonzept, das die in den Abschnitten 5 und 6 behandelten Aspekte abdeckt und als Grundlage für Audits herangezogen wird.

5.1 Infrastrukturelle Sicherheitsmaßnahmen

In diesem Kapitel werden die eingesetzten infrastrukturellen Sicherheitsmaßnahmen der a.sign CA Projects und GRAs (Kapitel 5.1.1 – 5.1.8) sowie LRAs (Kapitel 5.1.9) angeführt.

5.1.1 Verwendete Räumlichkeiten

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

5.1.2 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

5.1.3 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.

5.1.4 Klimatisierung

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

5.1.5 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.

5.1.6 Aufbewahrung von Datenmaterial

Zur Aufbewahrung von schützenswertem Datenmaterial wird ein Tresor eingesetzt.

5.1.7 Abfallentsorgung

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

5.1.8 Sonstiges

- Die Absicherung des Local Area Networks der CA gegen unautorisierte Zugriffe von außen erfolgt durch den Einsatz von Firewalls.
- Die Kommunikation zwischen den Komponenten der CA und den restlichen System-Komponenten erfolgt ausschließlich gesichert.
- 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.

5.1.9 Infrastrukturelle Maßnahmen bez. a.sign LRAs

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

5.2 Organisatorische Sicherheitsmaßnahmen

5.2.1 a.sign CA Projects

Um den sicheren Betrieb der a.sign CA zu gewährleisten, werden die kritischen 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	

Task	Klasse der zur Ausführung Berechtigten	Bemerkung
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 GRA	LRAO	

Tabelle 20 Berechtigungen

CAA ... CA-Administrator

CASA ... CA System-Administrator

SB ... Sicherheitsbeamter

LRAO ... LRA-Operator

5.2.2 a.sign GRAs

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

5.2.3 a.sign LRAs

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

5.2.4 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 zumindest durch ein Passwort bzw. eine PIN zu schützen.

5.3 Personelle Sicherheitsmaßnahmen

5.3.1 a.sign CA Projects

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

5.3.2 a.sign GRAs

Für das Personal, das beim Betrieb der a.sign GRAs eingesetzt wird, gelten zu Abschnitt 5.3.1 analoge Bestimmungen.

5.3.3 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 Zertifizierungsdiensteanbieter 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 21 LRA-Operatoren

6 Technisches Sicherheitskonzept

Dieses Kapitel beschreibt alle technischen Sicherheitsanforderungen an die CA, GRAs, LRAs, Signatoren und den Informationsdienst. Die Maßnahmen gewährleisten den zuverlässigen Schutz der Privaten CA-Schlüssel und Aktivierungsdaten und ermöglichen eine sichere Durchführung der Schlüsselgenerierung, der Signator-Authentifizierung, des Zertifikat-Managements sowie der anfallenden Auditierungs- und Archivierungsaufgaben. Die Teilkapitel enthalten u. a. Informationen zu folgenden Fragen:

6.1 Schlüsselgenerierung und Schlüsselmanagement

- Wie wird das CA-Schlüsselpaar generiert?
- Wie wird der Öffentliche CA-Schlüssel verteilt?
- Sind Schlüssel eines Signators eindeutig?
- Existieren Einschränkungen für die Schlüsselverwendung?

6.2 Schutz des Privaten CA-Schlüssels

- Wie wird der Private Schlüssel der CA und Signatoren gespeichert?
- Wie werden Sicherheitskopien des Privaten Schlüssels angelegt?

6.3 Archivierung öffentlicher Schlüssel

- Wie werden der Öffentliche Schlüssel eines Signators archiviert?

6.4 Gültigkeitsdauer von Zertifikaten

- Wie lange sind Zertifikate für die CA und Signatoren gültig?

6.5 Standards der eingesetzten Soft- und Hardware

- Welchen Sicherheitsstandards genügt die eingesetzte Soft- und Hardware?

6.1 Schlüsselgenerierung und Schlüsselmanagement

6.1.1 Erzeugung des CA-Schlüsselpaares

- Die a.sign CA Projects hat technisch zu gewährleisten, dass der Private CA-Schlüssel nicht von einer Person allein generiert werden kann.
- Die Erstinstallation der CA Project und damit die Generierung des a.sign CA-Schlüsselpaares fällt in den Aufgabenbereich der CA-Administratoren.

6.1.2 Distribution des Öffentlichen CA-Schlüssels

Die Verteilung des Öffentlichen CA-Schlüssels an die Inhaber von a.sign Zertifikaten erfolgt via Web.

6.1.3 Eindeutigkeit von Schlüsseln eines Signators

Da Signatoren ihre Schlüssel selbst erzeugen, ist die Eindeutigkeit der Schlüssel für Signatoren von den dabei eingesetzten Browsern durch die Erzeugung und Verwendung von GUIDs (Globally Unique Identifiers) sichergestellt.

6.1.4 Einschränkungen bzgl. der Verwendung von Schlüsseln

Die zulässigen Verwendungsmöglichkeiten von Zertifikaten für die CA Projects und Signatoren werden in der Key Usage Extension der einzelnen Zertifikate definiert.

6.2 Schutz des Privaten Schlüssels

6.2.1 Speicherung des Privaten Schlüssels

6.2.1.1 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.

6.2.1.2 Privater Schlüssel eines Signators

Die Generierung und Speicherung eines Privaten Schlüssels des Signators ist auf einer Harddisk des verwendeten PCs , Smartcards sowie auf Floppy-Disks zulässig.

6.3 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.

6.4 Gültigkeitsdauer von Zertifikaten

6.4.1 Aussteller-Zertifikate

Zertifikat	Gültigkeitsdauer
a.sign Projects CA	30 Jahre

Tabelle 22 Gültigkeitsdauer der CA-Zertifikate

6.4.2 Zertifikate für Signatoren

Zertifikat	Gültigkeitsdauer
a.sign User Light	1 Jahr (mind) (verlängerbar bis zu einer Gesamtdauer von 5 Jahren ab Erstausstellung)
a.sign User Strong und Strong plus	1 Jahr (mind) (verlängerbar bis zu einer Gesamtdauer von 3 Jahren ab Erstausstellung)

Tabelle 23 Gültigkeitsdauer der Zertifikate für Signatoren

Bemerkung: Derzeit ist das Verlängern von Zertifikaten nicht implementiert.

6.5 Standards der eingesetzten Soft- und Hardware

6.5.1 Software

Die eingesetzte Software besteht aus 3 Hauptkomponenten:

- Controller
- Certificate Management System
- X.500 Directory

6.5.1.1 Controller

Der Controller unterstützt

- die Secure Sockets Layer Versions 2 (SSLv2) und 3 (SSLv3),
- die Kryptografie-Standards PKCS#7 und PKCS#10,
- Requests für User-Zertifikate bzgl. Microsoft Internet Explorer, Netscape Navigator und Netscape Communicator.

6.5.1.2 Certificate Management System

Das Certificate Management System unterstützt

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

6.5.1.3 X.500-Directory

Das X.500-Directory unterstützt

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

6.5.2 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 SHA-1,
- ANSI X9.9 und X9.23 sowie
- ISO 9796.

7 Zertifikats- und CRL-Profil

In diesem Kapitel wird das Format der ausgegebenen Zertifikate und CRLs definiert. In den einzelnen Teilkapiteln werden u. a. folgende Fragen beantwortet:

7.1 Profil der ausgegebenen Zertifikate

- Welchem Standard entsprechen die Zertifikate für CAs und Signatoren?
- Welche Basic Certificate Fields werden verwendet?

7.2 Profil der ausgegebenen CRLs

- Welchem Standard entsprechen die verwendeten CRLs?

7.1 Profil der ausgegebenen Zertifikate

7.1.1 a.sign CA-Zertifikat Projects

a.sign CA-Zertifikate sind X.509-Zertifikate (Version 3), d. h. a.sign CA-Zertifikate genügen den Spezifikationen der ITU-T Rec. X.509 | ISO/IEC 9594-8.

7.1.1.1 User-CA-Zertifikate

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

Attribut	Inhalt	Anmerkung
Version	v3	Das Zertifikat ist ein X.509v3-Zertifikat.
Seriennummer	Seriennummer des Zertifikates	
Signatur-Algorithmus	SHA 1	Signatur-Algorithmus, der von der ausstellenden Instanz bei der Signatur des Zertifikates verwendet wurde.

Aussteller	OU = www.a-trust.at OU = a.sign Projects O = A-Trust Ges.f. Sicherheitssysteme im elektronische Daten-verkehr GmbH C = AT	
Gültig von	Beginn der Gültigkeitsdauer des Zertifikates	
Gültig bis	Ende der Gültigkeitsdauer des Zertifikates	
Zertifikatsinhaber	OU = www.a-trust.at OU = a.sign User Light / a.sign User Strong /a.sign Strong plus O = A-Trust Ges.f.Sicherheitssysteme im elektronischen Daten-verkehr GmbH C = AT	Der Wert des zweiten OU-Eintrages hängt davon ab, ob es sich um die User-CA der Klasse Light, Strong oder Strong plus handelt.
Öffentlicher Schlüssel	RSA/1024 bit	Öffentlicher Schlüssel des Zertifikatsinhabers

Tabelle 24 Profil CA-Zertifikat

Zusätzlich enthält das a.sign User CA-Zertifikat Projects einige Standard-Extensions.

7.1.2 a.sign Zertifikate für Signatoren

a.sign Zertifikate für Signatoren sind X.509-Zertifikate (Version 3), d.h. a.sign Zertifikate für Signatoren genügen den Spezifikationen der ITU-T Rec. X.509 | ISO/IEC 9594-8.

7.1.2.1 a.sign User Light Zertifikat

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

Attribut	Inhalt	Anmerkung
Version	v3	Das Zertifikat ist ein X.509v3-Zertifikat.
Seriennummer	Seriennummer des Zertifikates	
Signatur-Algorithmus	SHA 1	Signatur-Algorithmus, der von der ausstellenden Instanz bei der Signatur des Zertifikates verwendet wurde.
Aussteller	OU = www.a-trust.at OU = a.sign Projects O = A-Trust Ges.f.Sicherheitssysteme im elektronischen Daten-verkehr GmbH C = AT	
Gültig von	Beginn der Gültigkeitsdauer des Zertifikates	
Gültig bis	Ende der Gültigkeitsdauer des Zertifikates	
Zertifikatsinhaber	E = … CN = … SN = … OU = www.a-trust.at OU = a.sign User Light O =A-Trust Ges.f.Sicherheitssysteme im elektronischen Datenverkehr GmbH C = AT	E … E-Mail-Adresse CN … Common Name SN … Serial Number Option bei Projektgeschäft OU ... nach Vereinbarung OU ... nach Vereinbarung O .... nach Vereinbarung C ... nach Vereinbarung
Öffentlicher Schlüssel	RSA/512, 786, 1024 bit und höher	Öffentlicher Schlüssel des Zertifikatsinhabers

Tabelle 25 Profil User Light Zertifikat

Zusätzlich enthalten a.sign User-Zertifikate Light einige Standard-Extensions.

7.1.2.2 User-Zertifikat Strong und Strong plus

Ein User-Zertifikat Strong und Strong plus enthält folgende Basisfelder (Basic Certficate Fields):

Attribut	Inhalt	Anmerkung
Version	v3	Das Zertifikat ist ein X.509v3-Zertifikat.
Seriennummer	Seriennummer des Zertifikates	
Signatur-Algorithmus	SHA1	Signatur-Algorithmus, der von der ausstellenden Instanz bei der Signatur des Zertifikates verwendet wurde.
Aussteller	OU =www.a-trust.at OU = a.sign Projects O = A-Trust Ges.f.Sicherheitssysteme im elektronischen Datenverkehr GmbH C = AT	
Gültig von	Beginn der Gültigkeitsdauer des Zertifikates	
Gültig bis	Ende der Gültigkeitsdauer des Zertifikates	
Zertifikatsinhaber	E = … CN = … SN = … OU = www.a-trust.at OU = a.sign User Strong O =A-Trust Ges.f. Sicherheitssysteme im elektronischen Datenverkehr GmbH C = AT	E … E-Mail-Adresse CN … Common Name SN … Serial Number Optional: Strong Plus OU ... nach Vereinbarung OU ... nach Vereinbarung O .... nach Vereinbarung C ... nach Vereinbarung
Öffentlicher Schlüssel	RSA/512, 786, 1024 bit und höher	Öffentlicher Schlüssel des Zertifikatsinhabers

Tabelle 26 Profil User Strong und Strong plus Zertifikat

Zusätzlich enthalten a.sign User-Zertifikate Strong und Strong plus einige Standard-Extensions.

7.2 Profil der ausgegebenen CRLs

Es werden X.509 Version 2 CRLs ausgegeben.

8 Administration des CPS Projects

Dieses Kapitel enthält die Richtlinien zur Durchführung von Änderungen am a.sign Certification Practice Statement. Die Teilkapitel enthalten u. a. Informationen zu folgenden Fragen:

8.1 Durchführung von Änderungen am a.sign CPS

- Wer entwickelt das a.sign Certification Practice Statement?
- Wie werden Änderungen am a.sign Certification Practice Statement durchgeführt?

8.2 Veröffentlichung geänderter a.sign CPSs

- Wie ist die Veröffentlichung geänderter a.sign Certification Practice Statements geregelt?

8.1 Durchführung von Änderungen am a.sign CPS Projects

8.1.1 Allgemeines

Das a.sign Certification Practice Statement Projects (CPS) wird von einer a.sign Expertengruppe entwickelt, die sich aus den Bereichen Technik, Wirtschaft und Rechtswissenschaften zusammensetzt.

8.1.2 Erforderliche Schritte

- Ein Änderungsvorschlag zum jeweiligen CPS Projects muss zunächst den Mitgliedern der oben erwähnten Expertengruppe übermittelt werden.
- Werden von den Mitgliedern der Expertengruppe keine Einwände gegen den Änderungsvorschlag vorgebracht, gilt der Änderungsvorschlag als akzeptiert.

8.2 Veröffentlichung geänderter a.sign CPS Projects

Regelung der Veröffentlichung eines geänderten a.sign CPS:

Jede neue Version des a.sign CPS wird vom Informationsdienst veröffentlicht.

9 Anhang

Der Anhang stellt dem Leser folgende Informationen zur Verfügung:

- Definitionen für Schlagwörter und Fachbegriffe aus dem Bereich Zertifizierung Was bedeuten die am häufigsten verwendeten Fachbegriffe?
- Liste der verwendeten Abkürzungen

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

Globally Unique Identifier (GUIDs): weltweit eindeutige Identifier; werden vom Internet Explorer sowie vom Netscape Navigator / Communicator unterstützt und bei der Generierung des Privaten Schlüssels benötigt

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: Zertifizierungsrichtlinien, die von der a.sign Primary Certification Authority für jede Zertifikatsklasse ausgegeben werden

Primary Certification Authority (PCA): Certification Authority, die nur andere Certification Authorities zertifiziert; diese zertifizierten Certification Authorities müssen die Richtlinien der entsprechenden a.sign Policy einhalten

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)

Virtual Private Network (VPN): siehe → Virtuelles Privates Netzwerk

Virtuelles Privates Netzwerk: eine private Netzwerkinfrastruktur, die sich der öffentlichen Telekommunikationsinfrastruktur bedient, dabei aber Vertraulichkeit durch Sicherheitsmaßnahmen ,wie z. B. der Verschlüsselung, garantiert.

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 Strong plus und Premium.

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

Zertifikatsverzeichnis: Liste aller veröffentlichten Zertifikate

Zertifikatswerber: Person, die ein Zertifikat beantragt

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 (a.sign Primary Certification Authority)

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

Zertifizierungsinstanz: siehe → Zertifizierungsdiensteanbieter

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
IPSEC	Internet Protocol Securtiy
ITSEC	Information Technology Security Evaluation Criteria
LRA	Lokale Registrierungsstelle (Local Registration Authority)
MIME	Multipurpose Internet Mail Extensions
PCA	Primary Certification Authority
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
VPN	Virtual Private Network
WWW	World Wide Web