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

Certificate Policy a.sign Projects für User Light Zertifikate

Version: 1.1.5

Datum: 01.10.2002

Inhaltsverzeichnis

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

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

Tabellenverzeichnis

1 Einführung

Dieses Kapitel gibt dem Leser einen Überblick über das vorliegende Dokument und beschreibt die Einheiten, die an den Signatur- und Zertifizierungsdiensten beteiligt sind, sowie die Einsatzmöglichkeiten für die ausgestellten Zertifikate.

1.1 Überblick

Das Ziel des vorliegenden Dokuments besteht darin, die Richtlinien bezüglich Light Zertifikaten derart festzulegen, dass die Voraussetzungen für eine sichere und zuverlässige Abwicklung der angebotenen Signatur- und Zertifizierungsdienste gewährleistet sind.

Jedes User Zertifikat enthält einen Verweis auf die Policy für a.sign Projects – Light Zertifikate, sodass dem Benutzer des Zertifikates die Möglichkeit eingeräumt wird, sich darüber zu informieren, ob das Zertifikat den Erfordernissen des geplanten Verwendungszwecks genügt.

1.2 Identifikation der Policy

Name der Policy: Certificate Policy für a.sign User Light Zertifikate (Version 1.1.5)
Object Identifier: **1.2.040.017.1.6.1.**

1.3 a.sign Zertifizierungsinfrastruktur und Anwendungsbereiche

1.3.1 a.sign Zertifizierungsinfrastruktur

1.3.1.1 a.sign User Light

User Zertifikate a.sign User Light werden entsprechend der a.sign Zertifizierungsrichtlinien (d. h. des Certification Practice Statements für a.sign Projects (CPS)) für Signatoren ausgegeben).

1.3.1.2 Signatoren

Als Signatoren (Inhaber von a.sign User Light Zertifikaten) sind ausschließlich Zertifizierungsdiensteanbieter und natürliche Personen zulässig.

1.3.1.3 a.sign Informationsdienst

Der a.sign Informationsdienst stellt Zertifikatsverzeichnisse, Widerrufslisten (CRLs), die a.sign Richtlinien (a.sign Policies, Certification Practice Statements (CPSs) aller CAs) sowie andere relevante Informationen bezüglich der Signatur- und Zertifizierungsdienste online und öffentlich zugänglich zur Verfügung.

Der a.sign Informationsdienst ist unter folgender Webadresse zugänglich: http://www.a-trust.at/.

1.3.2 Anwendung von a.sign User Light Zertifikaten

User Zertifikate, die im Rahmen der a.sign Zertifizierungsinfrastruktur ausgegeben werden, können in unterschiedliche Varianten (Light, Strong und Uni) eingeteilt werden. Die Variante gibt dabei die verwendete Variante bei der Registrierung an.

Das Anwendungsgebiet dieser Zertifikate umfasst den elektronischen Datenaustausch via E-Mail (digitale Signatur, Verschlüsselung) sowie die Authentifizierung des Signators (an Web-Servern o.ä.).

Weitere Informationen über die a.sign Signatur- und Zertifizierungsdienste sind unter folgender Webadresse zugänglich: http://www.a-trust.at.

1.4 Kontaktierungsmöglichkeiten

1.4.1 Kontaktinformation zum a.trust Zertifizierungsdiensteanbieter

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 1 Kontaktinformation

1.4.2 a.trust Web-Schnittstellen

Unter der Webadresse http://www.a-trust.at werden Informationen zu folgenden Themen angeboten:

a.trust- Web

Allgemeine Information	*Zertifizierungsdienst*	*Informationsdienst*
Informationen über a.sign Produkte digitale Signatur Anwendung von Zertifikaten Support	Zertifizierung Verlängerung eines Zertifikates Widerruf eines Zertifikates	a.sign Verzeichnisdienst a.sign Widerrufslisten a.sign Richtlinien

Tabelle 2 Web-Schnittstellen

2 Allgemeine Richtlinien

In diesem Kapitel wird dem Leser ein Überblick über die allgemeinen Grundlagen der a.sign Signatur- und Zertifizierungsdienste (Pflichten der beteiligten Einheiten, Haftung, rechtliche Aspekte, Entgelte, Veröffentlichungen, Kontrollen, Datenschutz usw.) gegeben.

2.1 Pflichten

2.1.1 Verpflichtungen der a.sign Projects CA

2.1.1.1 Allgemeine Verpflichtungen

Die a.sign Projects CA hat für die Einhaltung und Umsetzung der a.sign Projects Policies für User Light, User Strong und User Strong plus sowie der CPSs der untergeordneten CA durch die entsprechenden Einheiten der a.sign Zertifizierungs-infrastruktur zu sorgen.

2.1.1.2 Privater Schlüssel der a.sign Projects CA

Die a.sign Projects CA hat durch geeignete organisatorische, infrastrukturelle, personelle und sicherheitstechnische Maßnahmen für den Schutz ihres privaten Schlüssels (Signaturschlüssels) zu sorgen.

2.1.1.3 Definition eines Sicherheitskonzeptes

Entsprechend den Kapiteln 5 und 6 der a.sign Policy Projects für User Light ist vom Zertifizierungsdiensteanbieter ein Sicherheitskonzept zu entwickeln und zu dokumentieren.

2.1.1.4 Allgemeine Verpflichtungen

Die a.sign Projects CA ist ist dazu verpflichtet, die a.sign Policy Projects für User Light und das definierte CPS umzusetzen und einzuhalten. Dies erfordert ins besondere, dass die CA

- die Einhaltung der in diesen Richtlinien spezifizierten Identifikations- und Authentifikationsmechanismen sicherzustellen hat,

- Zertifikate für Signatoren gemäß dieser Richtlinien auszustellen hat und
- Zertifikate für Signatoren gegebenenfalls zu widerrufen hat.

2.1.1.5 Veröffentlichungen, Informationen für Signatoren

Ausgestellte Zertifikate für Signatoren sind entsprechend den a.sign Richtlinien (d.h. der a.sign Policy Projects für User Light bzw. des Certification Practice Statements Projects (CPS)) zu veröffentlichen (siehe Kapitel 2.5.3). Zertifikatswerber sind von einer erfolgten Ausstellung des Zertifikates in Kenntnis zu setzen.

Widerrufene Zertifikate für Signatoren sind entsprechend den a.sign Richtlinien in Form von Certificate Revocation Lists (CRLs, deutsch: Widerrufslisten) zu veröffentlichen (siehe Kapitel 2.5.4). Signatoren sind von einem erfolgten Widerruf ihres Zertifikates in Kenntnis zu setzen.

Die CA, die ein Zertifikat für einen Signator ausstellt, ist verpflichtet, den Zertifikatswerber über den Umgang mit Zertifikaten, den Umgang mit seinem privaten Schlüssel, den Schutz seines privaten Schlüssels, die Prüfung von digitalen Signaturen sowie weitere Themen zu unterrichten (siehe auch Kapitel 2.5.5).

2.1.2 Verpflichtungen von Signatoren

2.1.2.1 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 Richtlinien der a.sign Projects CA einzuhalten.

2.1.2.2 Schutz des privaten Schlüssels

Signatoren sind verpflichtet, den privaten Schlüssel zu schützen, d.h.

- ihn in geeigneter Weise (d.h. zumindest durch ein Passwort oder eine PIN gesichert) zu verwahren,
- die Weitergabe zu unterlassen und
- den Zugriff auf den privaten Schlüssel soweit zumutbar zu verhindern.

2.1.2.3 Widerruf von Zertifikaten für Signatoren

Signatoren sind dazu verpflichtet, die für sie ausgestellten Zertifikate zu widerrufen, falls

- der zugehörige private Schlüssel verloren geht,
- der Verdacht besteht, dass der zugehörige private Schlüssel kompromittiert wurde oder
- sich die im Zertifikat angeführten Daten geändert haben.

2.1.2.4 Anwendung privater Schlüssel bzw. ausgestellter Zertifikate

Natürlichen Personen ist es im Gegensatz zu Zertifizierungsdiensteanbietern untersagt, selbst Zertifikate auszustellen.

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

2.1.3 Verpflichtungen Dritter

Bevor ein a.sign User Light 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 Variante des Zertifikates zu identifizieren und
- zu überprüfen, ob das Zertifikat für den entsprechenden Zweck eingesetzt werden darf.

2.1.4 Verpflichtungen des a.sign Informationsdienstes

Der a.sign Informationsdienst ist verpflichtet 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 (Datenschutz) festgelegten Einschränkungen zu veröffentlichen.

2.2 Haftung

Ein Zertifizierungsdiensteanbieter, der ein a.sign User Light Zertifikat ausstellt, haftet dafür, dass die im Zertifikat enthaltene E-Mail-Adresse zum Zeitpunkt der Ausstellung korrekt war.

Ein Zertifizierungsdiensteanbieter, der a.sign User Light Zertifikate ausstellt, haftet nicht, falls er nachweisen kann, dass ihn an der Verletzung der oben angeführten Verpflichtung keine Schuld trifft.

2.3 Rechtliche Hinweise

2.3.1 Ausstellung eines a.sign User Zertifikates Light

Die CA kann einem Zertifikatswerber ohne Angabe von Gründen die Ausstellung eines User Zertifikates Light verweigern, d.h. es besteht kein rechtlicher Anspruch auf die Ausstellung eines Zertifikates.

2.3.2 Rechtliche Wirksamkeit und Verwendung eines Zertifikates *Light*

Die rechtliche Wirksamkeit und Verwendung eines a.sign User Zertifikates Light ist im Österreichischen Signaturgesetz und in den auf seiner Grundlage ergangenen Verordnungen geregelt. Insbesondere ist die Verwendung einer digitalen Signatur, die auf einem Zertifikat Light beruht, im Rechts- und Geschäftsverkehr zulässig. Zertifikate Light entsprechen nicht den qualifizierten Zertifikaten des Österreichischen Signaturgesetzes.

2.4 Entgelte

- Für die Ausgabe bzw. das Beziehen von Widerrufslisten (CRLs) und
- die Veröffentlichung von a.sign Policies bzw. CPSs, ausgenommen Selbstkosten bei einer Ausgabe auf entsprechenden Medien,

sind von Zertifizierungsdiensteanbietern keine Entgelte einzuheben Die Entgelte für alle anderen Dienstleistungen sind vom entsprechenden Service-Anbieter festzulegen.

2.5 Veröffentlichungen

2.5.1 Allgemeines

Die in den nachfolgenden Kapiteln angeführten Veröffentlichungen (a.sign Richtlinien, Zertifikatsverzeichnisse, Widerrufslisten und Material zur Unterrichtung von Zertifikatswerbern) werden durch den a.sign Zertifizeirungsdiensteanbieter veranlasst und vom a.sign Informationsdienst durchgeführt. Diese Veröffentlichungen haben in geeigneter, für die Allgemeinheit jederzeit über öffentliche Telekommunikationsverbindungen zugänglicher Weise zu erfolgen.

Der a.sign Informationsdienst ist angehalten, dafür zu sorgen, dass er ohne Einschränkungen öffentlich und jederzeit zugänglich ist.

Der a.sign Informationsdienst ist unter folgender Webadresse erreichbar: http://www.a-trust.at/.

2.5.2 a.sign Richtlinien

Mittels des a.sign Informationsdienstes hat der Zertifizierungsdiensteanbieter die a.sign Policy Projects für User Light Zertifikate sowie das CPS Projects in der aktuellen und allen vorangegangenen Versionen zu veröffentlichen.

2.5.3 Zertifikatsverzeichnisse

Der Zertifizierungsdiensteanbieter hat mit Hilfe des a.sign Informationsdienstes die ausgestellten Zertifikate unter folgenden Bedingungen zu veröffentlichen:

- Die Veröffentlichungen müssen mit einer angemessenen zeitlichen Verfügbarkeit (d.h. zumindest während der Geschäftszeiten) betrieben werden.

- Die Veröffentlichungen müssen authentisch und unter Berücksichtigung der in Kapitel 2.6 (Datenschutz) getroffenen Einschränkungen erfolgen.

- Für jedes im Zertifikatsverzeichnis enthaltene Zertifikat ist der aktuelle Status anzugeben.

- Zertifikate sind mindestens so lange in einem Zertifikatsverzeichnis zu führen, wie der im Zertifikat aufgeführte Algorithmus mit den dazugehörigen Parametern als geeignet beurteilt wird.

2.5.4 Widerrufslisten (CRLs)

Der a.sign Zertifizierungsdiensteanbieter hat mit Hilfe des a.sign Informationsdienstes alle widerrufenen Zertifikate unter folgenden Bedingungen zu veröffentlichen:

- Widerrufene Zertifikate sind authentisch und in einer elektronisch jederzeit allgemein zugänglichen Form zu veröffentlichen.

- Die Veröffentlichung der widerrufenen Zertifikate ist täglich sowie bei einem durchgeführten Zertifikats-Widerruf zu aktualisieren und hat den Zugriff in angemessener Zeit zuzulassen.

- Widerrufene Zertifikate sind so lange öffentlich zugänglich zu halten, bis die ursprüngliche Gültigkeitsdauer des Zertifikates überschritten ist.

2.5.5 Unterrichtung von Zertifikatswerbern

Zertifikatswerber sind über Themen im Zusammenhang mit Zertifikaten, digitalen Signaturen und ihrem privaten Schlüssel zu unterrichten. Die Zertifikatswerber sind daher schriftlich oder unter Verwendung eines dauerhaften Datenträgers entsprechendes Informationsmaterial zu den Themen

- Sicherheits- und Zertifizierungskonzept des Zertifizierungsdiensteanbieters, der die ausstellende CA betreibt,

- zulässige Verwendung des Zertifikates (Anwendungsbereich, Einschränkungen des Anwendungsbereiches, Obergrenze des zulässigen Transaktionswertes o.ä.),

- besondere Streitbeilegungsverfahren,
- zulässige Komponenten und Verfahren zur Erzeugung und Überprüfung von digitalen Signaturen sowie deren Gültigkeitsdauer,
- Rechtswirkungen der vom Signator erzeugten digitalen Signaturen,
- Pflichten des Signators und
- Haftung des Zertifizierungsdiensteanbieters, der die ausstellende CA betreibt,

zur Verfügung zu stellen.

Auf Verlangen ist auch Dritten, die ein rechtliches Interesse glaubhaft machen, entsprechendes Informationsmaterial zu den Themen

- Sicherheits- und Zertifizierungskonzept des Zertifizierungsdiensteanbieters, der die ausstellende CA betreibt,
- zulässige Verwendung des Zertifikates (Anwendungsbereich, Einschränkungen des Anwendungsbereiches, Obergrenze des zulässigen Transaktionswertes o.ä.) und
- besondere Streitbeilegungsverfahren

zur Verfügung zu stellen.

2.6 Datenschutz

Ein Zertifizierungsdiensteanbieter, der Zertifikate Light ausstellt, hat nur jene personenbezogenen Daten eines Signators zu verwenden, die er zur Durchführung seiner erbrachten Dienste benötigt. Diese Daten dürfen nur unmittelbar beim Betroffenen selbst oder mit seiner ausdrücklichen Zustimmung bei einem Dritten erhoben werden.

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.

3.1 Erstregistrierung

3.1.1 Identifikationsmerkmale und Namenskonventionen

3.1.1.1 Zertifizierungsdiensteanbieter

Ein Zertifizierungsdiensteanbieter, der Zertifikate Light ausstellt, ist in Zertifikaten zumindest mit seinem unverwechselbaren Namen sowie mit dem Staat seiner Niederlassung anzuführen.

3.1.1.2 Natürliche Personen

Ein a.sign User Light Zertifikat, das für eine natürliche Person ausgestellt wurde, hat zumindest den Vor- und Nachnamen des Signators oder ein Pseudonym sowie die E-Mail-Adresse des Signators zu enthalten. Im Falle der Verwendung eines Pseudonyms hat dieses weder anstößig noch offensichtlich zur Verwechslung mit Namen oder Kennzeichen geeignet zu sein.

3.1.2 Eindeutigkeit der Identifikationsmerkmale

Die in den Zertifikaten Light angeführten Identifikationsmerkmale müssen keinen eindeutigen Identifier des Signators (Sozialversicherungsnummer o.ä.) enthalten, d. h. der Signator muss nicht aufgrund dieser angeführten Merkmale eindeutig identifiziert werden können. Die CA ist jedoch dazu berechtigt, für eine interne eindeutige Identifikation des Zertifikatswerbers zusätzliche Identifikationsmerkmale des Zertifikatswerbers zu erfassen.

3.1.3 Identitätsüberprüfung bei User-Zertifikaten Light

Die Identitätsüberprüfung vor der Ausgabe eines User-Zertifikates *Light* erfordert kein persönliches Erscheinen des Zertifikatswerbers bei der CA. Es sind indirekte Verfahren zulässig, die die Überprüfung der im Kapitel 3.1.1.2 angeführten Identifikationsmerkmale des Zertifikatswerbers zuverlässig gewährleisten.

3.1.4 Nachweis des Besitzes des privaten Schlüssels

Um ein User-Zertifikat Light erhalten zu können, hat der Zertifikatswerber den Besitz des privaten Schlüssels durch ein authentisches Verfahren (z.B. durch digitales Signieren des Zertifikatantrages unter Verwendung dieses Schlüssels) nachzuweisen.

3.2 Verlängerung der Gültigkeit von Zertifikaten für Signatoren

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

3.3 Widerruf von Zertifikaten für Signatoren

Vor der Durchführung des Widerrufes eines Zertifikates Light ist der Zertifizierungsdienstean bieter dazu verpflichtet, mittels eines Authentisierungsverfahrens die Identität der Person, die den Widerruf beantragt hat, festzustellen.

4 Verfahrensanforderungen

Dieses Kapitel gibt dem Leser einen Überblick über jene Bestimmungen und Anforderungen, die sich für die Einheiten der a.sign Zertifizierungsinfrastruktur bei den einzelnen Verfahren im Rahmen der Zertifizierungsdienstleistungen ergeben.

4.1 Zertifizierung von natürlichen Personen

4.1.1 Beantragung eines Zertifikates

Das bei der Beantragung eines User-Zertifikates Light eingesetzte Verfahren hat die folgenden Eigenschaften zu umfassen:

- Ein persönliches Erscheinen des Zertifikatswerbers ist nicht erforderlich.
- Die E-Mail-Adresse des Zertifikatswerbers ist zu überprüfen. Für diese Überprüfung sind indirekte Verfahren zulässig.

4.1.2 Ausstellung eines Zertifikates

- Das Ausstellen eines Zertifikates für eine natürliche Person hat unter Einhaltung der in den Kapiteln 5 und 6 definierten Sicherheitsanforderungen zu erfolgen.
- Der Zertifikatswerber ist bezüglich der durchgeführten Ausstellung seines Zertifikates, der Zertifikatinhalte und der Modalitäten der Zertifikatabholung zu informieren.
- Das ausgestellte Zertifikat darf erst nach einer erfolgreichen Authentifizierung des Zertifikatswerbers an diesen freigegeben werden.

4.1.3 Entgegennehmen eines Zertifikates

Das Entgegennehmen eines Zertifikates impliziert das Akzeptieren der im entgegengenommenen Zertifikat enthaltenen Inhalte.

4.2 Verlängerung der Gültigkeit von Zertifikaten

4.2.1 Allgemeines

Es ist bis zum Ablauf der Gültigkeit eines Zertifikates zulässig, den Inhalt des Zertifikates (mit Ausnahme der Gültigkeitsdauer) neu zu zertifizieren und damit ein neues Zertifikat auszustellen, das sich auf dasselbe Schlüsselpaar bezieht. Für das Schlüsselpaar besteht daher (mit Ausnahme der auch im Kapitel 4.2.2 erwähnten Einschränkung bzgl. der Gültigkeit der bei der Erstellung, Speicherung und Anwendung des Schlüsselpaares eingesetzten technischen Komponenten und Verfahren) im Gegensatz zu Zertifikaten keine Beschränkung der Gültigkeitsdauer.

4.2.2 Durchführung der erneuten Zertifizierung

- Eine erneute Zertifizierung bezüglich eines Zertifikates *Light* im Sinne des Kapitels 4.2.1 ist nur zulässig, falls
  - sich die im Zertifikat enthaltenen Daten mit Ausnahme der Gültigkeitsdauer nicht geändert haben und
  - durch die Verlängerung die Gültigkeitsdauer der bei der Erstellung, Speicherung und Anwendung des Schlüsselpaares eingesetzten technischen Komponenten und Verfahren nicht überschritten wird.
- Die Gültigkeit der im Zertifikat enthaltenen Angaben ist von der CA analog zu dem Verfahren im Rahmen der Erstregistrierung erneut zu prüfen.
- Eine erneute Zertifizierung eines Schlüsselpaares eines widerrufenen Zertifikaten ist ausgeschlossen.

4.3 Überprüfung der Gültigkeit von Zertifikaten

Der a.sign Informationsdienst hat eine Online-Überprüfung des Status von Zertifikaten Light zur Verfügung zu stellen (siehe Kapitel 2.5.3).

4.4 Widerruf von Zertifikaten

4.4.1 Allgemeines

- Jeder Zertifizierungsdiensteanbieter, der Zertifikate *Light* ausstellt, hat den Signatoren geeignete Kommunikationsmöglichkeiten bekanntzugeben, mit denen diese jederzeit einen unverzüglichen Widerruf ihres Zertifikates veranlassen können.
- Der Widerrufsdienst hat mit einer angemessenen zeitlichen Verfügbarkeit betrieben zu werden, die zumindest während der Geschäftszeiten des Zertifizierungsdiensteanbieters gegeben sein muss.
- Ein Widerruf muss den Zeitpunkt, ab dem er wirksam wird, enthalten. Der Widerruf ist ab dem Zeitpunkt des Eintragens des Widerrufs im entsprechenden Verzeichnis wirksam. Ein rückwirkender Widerruf von Zertifikaten ist nicht möglich.
- Ein Signator ist von einem erfolgten Widerruf bzgl. seines Zertifikates zu verständigen.
- Der Widerruf eines Zertifikates kann nicht rückgängig gemacht werden.

4.4.2 Gründe für den Widerruf eines Zertifikates

Ein Zertifizierungsdiensteanbieter, der Zertifikate Light ausstellt, hat ein Zertifikat unverzüglich zu widerrufen, falls

- der Signator dies verlangt,
- die im Zertifikat angeführten Angaben nicht mehr zutreffen,
- das Zertifikat aufgrund unrichtiger Angaben erwirkt wurde,
- die ausstellende CA ihre Tätigkeit einstellt und der Widerrufsdienst nicht von einem anderen Zertifizierungsdiensteanbieter übernommen wird,
- der zugehörige private Schlüssel verloren gegangen ist,
- der Diebstahl des privaten Schlüssels vermutet werden muss oder erfolgt ist,
- ein unbefugter Zugriff auf den privaten Schlüssel vermutet werden muss oder erfolgt ist, oder

- sich der Signator nicht an die mit dem Zertifikat verknüpften Bedingungen hält.

4.4.3 Zum Widerruf Berechtigte

Der Widerruf eines Zertifikates kann jederzeit und ohne Angabe von Gründen durch den Zertifizierungsdiensteanbieter, der die ausstellende CA betreibt, sowie durch den Besitzer des Zertifikates selbst erfolgen.

4.4.4 Verfahren zur Beantragung eines Widerrufs

Ein Zertifizierungsdiensteanbieter, der Zertifikate Light ausstellt, hat im CPS die zulässigen Verfahren zur Beantragung eines Widerrufs zu spezifizieren. Bei der Spezifikation dieser Verfahren ist zu berücksichtigen, dass die CA dazu verpflichtet ist, vor der Durchführung des Widerrufs eines Zertifikates Light mittels eines Authentisierungsverfahrens die Identität der Person, die den Widerruf beantragt hat, festzustellen (siehe Kapitel 3.3).

4.4.5 Veröffentlichung widerrufener Zertifikate

Widerrufe von Zertifikaten Light sind in Form von Widerrufslisten (CRLs) unter Einhaltung der in Kapitel 2.5.4 angeführten Bestimmungen zu veröffentlichen.

4.5 Schlüsselaustausch

Ein Schlüsselaustausch (siehe Kapitel 0) ist ausschließlich durch Beantragung eines neuen Zertifikates (siehe Kapitel 4.1.1) möglich.

4.6 Dokumentation

4.6.1 Allgemeines

Ein Zertifizierungsdiensteanbieter, der Zertifikate Light ausstellt, hat alle maßgeblichen Umstände über ein Zertifikat Light aufzuzeichnen, sodass (vor allem in gerichtlichen Verfahren) die Zertifizierung nachgewiesen werden kann. Insbesondere sind

das Ausstellen und Widerrufen von Zertifikaten sowie Störfälle und besondere Betriebssituationen zu dokumentieren.

4.6.2 Durchführung der Archivierung

Die Dokumentation hat derart zu erfolgen, dass die Daten und ihre Unverfälschtheit sowie der Zeitpunkt ihrer Aufnahme in das Protokollierungssystem jederzeit nachprüfbar sind. Die Dokumentation hat in elektronischer Form vorzuliegen.

Die Daten sind über den gesetzlich vorgeschriebenen Zeitraum aufzubewahren und innerhalb dieses Zeitraums verfügbar zu halten und vor Verlust und Beschädigung zu schützen.

4.7 Ausnahmesituationen bezüglich eines privaten CA-Schlüssels

4.7.1 Verlust eines privaten CA-Schlüssels

Ist der private Schlüssel der CA verloren gegangen, ohne dass eine Kompromittierung erfolgte oder vermutet werden muss, so sind folgende Maßnahmen durchzuführen:

- Setzt die CA den Betrieb mit einem neuen privaten Schlüssel fort, so ist analog zu Kapitel 4.7.2 (Austausch eines privaten CA-Schlüssels) vorzugehen.
- Stellt die CA hingegen ihren Betrieb ein, so ist analog zu Kapitel 4.8 (Einstellen des Betriebes einer CA) vorzugehen.

4.7.2 Austausch eines privaten CA-Schlüssels

Die Vorgangsweise beim Auslaufen der Gültigkeit des privaten Schlüssels der CA und einem somit notwendig gewordenen Schlüsselaustausch ist von der CA in ihrem CPS festzulegen.

4.7.3 Kompromittierung eines privaten CA-Schlüssels

Die Vorgangsweise nach einer vermuteten oder erfolgten Kompromittierung des privaten Schlüssels einer CA ist von der CA in ihrem CPS festzulegen. Diese Vorgangsweise hat zumindest

- das Informieren jedes Inhabers eines gültigen, von der CA mit dem kompromittierten Schlüssel signierten Zertifikates, das Informieren jeder cross-zertifizierenden CA,
- das Generieren eines neuen Schlüsselpaares und die Ausstellung eines neuen CA-Zertifikates,
- den Widerruf aller Zertifikate für Signatoren, die mit dem kompromittierten Schlüssel signiert wurden, sowie das Informieren der betroffenen Signatoren und
- die Sicherstellung der Fortsetzung der authentischen Veröffentlichung von Zertifikatsverzeichnissen und Widerrufslisten

zu umfassen.

4.8 Einstellen des Betriebes einer CA

Die Vorgangsweise im Falle der Einstellung der Tätigkeit einer CA ist von der betroffenen CA in ihrem CPS festzulegen. Diese Vorgangsweise hat zumindest

- das Informieren jedes Inhabers eines gültigen, von der CA ausgestellten Zertifikates, das Informieren jeder cross-zertifizierenden CA,
- die öffentliche Ankündigung der geplante Einstellung in geeigneter Form,
- die Sicherstellung der Fortsetzung der authentischen Veröffentlichung von Zertifikatsverzeichnissen und Widerrufslisten durch andere Einheiten der a.sign Zertifizierungsinfrastruktur bzw. andere Zertifizierungsdiensteanbieter oder (falls diese Fortsetzung nicht möglich ist) den Widerruf aller zum Zeitpunkt der Terminierung noch gültigen Zertifikate für Signatoren und das Informieren der betroffenen Signatoren

zu umfassen.

5 Infrastrukturelles, organisatorisches und personelles Sicherheitskonzept

Dieses Kapitel beschreibt alle Sicherheitsanforderungen an die CA und Signatoren (ausgenommen technische Sicherheitsanforderungen). Damit soll eine zuverlässige und vertrauenswürdige Abwicklung der Schlüsselgenerierung, Authentifizierung, Ausstellung von Zertifikaten, des Widerrufes von Zertifikaten sowie der Audit- und Archivierungsvorgänge gewährleistet und vor allem ein Missbrauch von privaten Schlüsseln verhindert werden.

Die a.sign Projects CA ist verpflichtet, in ihrem CPS ein Sicherheitskonzept zu definieren, das die in den Kapiteln 5 und 6 behandelten Aspekte abdeckt und als Grundlage für Kontrollen (Audits) herangezogen wird.

5.1 Infrastrukturelle Sicherheitsmaßnahmen

Die IT-Ausstattung für den Betrieb einer CA muss in eigenen dafür tauglichen Räumlichkeiten untergebracht sein. Es muss gewährleistet sein, dass sich unbefugte Personen nicht Zutritt zu diesen Räumlichkeiten verschaffen können.

Die IT-Ausstattung muss durch geeignete Maßnahmen störungsfrei betrieben werden können. Dies beinhaltet insbesondere eine zuverlässige Stromversorgung sowie einen ausreichenden Feuerschutz.

Speichermedien müssen so aufbewahrt werden, dass diese vor unbefugtem Zugriff, Manipulation sowie physischer Beschädigung geschützt sind. Zusätzlich sollten CA-externe Speichermedien eingerichtet werden.

Zur Aufbewahrung von schützenswertem Schlüsselmaterial sind entsprechende Schlüsselbehältnisse einzurichten.

Für Hardware-Authentifizierungseinheiten (z.B. Chipkarten) zur Authentifizierung des Personals sowie für schriftliche oder elektronische Aufzeichnungen, die im Zuge der durchzuführenden Protokollierungs- und Archivierungsaufgaben anfallen, sind geeignete Aufbewahrungsmöglichkeiten vorzusehen.

5.2 Organisatorische Sicherheitsmaßnahmen

5.2.1 Der a.sign CA Projects

Durch die genaue Definition und Überwachung der Berechtigungen der einzelnen Mitarbeiter in einer CA ist zu verhindern, dass eine Person unberechtigt Schlüssel generiert, zertifiziert, verwendet oder vernichtet bzw. dass Zertifikatsverzeichnisse oder Widerrufslisten von Unbefugten verändert werden können.

Jede CA hat die authentische Protokollierung und Archivierung von Registrierungsdaten, Zertifizierungsdaten und Ereignissen durchzuführen, um die Nachprüfbarkeit von Daten und Abläufen jederzeit zu gewährleisten.

Es ist organisatorisch zu gewährleisten, dass der private Schlüssel der CA nicht von einer einzigen Person allein generiert werden kann.

Es ist für ein geeignetes Sicherungsverfahren (Backup) der Daten zu sorgen.

Zum Erstellen von Zertifikaten und Widerrufslisten sind eigene dafür bestimmte Schlüssel zu verwenden. Diese Signaturschlüssel der CA dürfen ausschließlich für die Erstellung von Zertifikaten und Widerrufslisten benutzt werden.

Alle Rechnersysteme, die zur Durchführung der diversen Zertifizierungsdienstleistungen eingesetzt werden, sind ausschließlich für diese Zwecke zu verwenden.

5.2.2 Signatoren

Die Signatoren haben durch Einhaltung der in Kapitel 2.1.2 angeführten organisatorischen Maßnahmen den sicheren Einsatz von a.sign User Light Zertifikaten und der entsprechenden privaten Schlüssel sicherzustellen.

5.3 Personelle Sicherheitsmaßnahmen

Für den Betrieb der CA ist zuverlässiges Personal mit den für die bereitgestellten Dienste erforderlichen Fachkenntnissen, Erfahrungen und Qualifikationen, insbesondere mit Managementfähigkeiten sowie mit Kenntnissen der Technologie digitaler Signaturen und angemessener Sicherheitsverfahren, zu beschäftigen.

Der CA ist die Beschäftigung von Mitarbeitern, deren Vertrauenswürdigkeit aufgrund strafbarer Handlungen in der Vergangenheit nicht gegeben ist, untersagt.

6 Technisches Sicherheitskonzept

In diesem Kapitel werden alle technischen Sicherheitsanforderungen an CAs, Signatoren, Dritte und den Informationsdienst definiert.

6.1 Generierung des privaten Schlüssels der CA

Bei der Generierung des privaten Schlüssels der a.sign Projects CA ist durch die Verwendung geeigneter technischer Komponenten und Verfahren zu gewährleisten, dass

- die unbefugte Verwendung des privaten Schlüssels der CA verlässlich verhindert wird und
- der private Schlüssel der CA nicht von einer Person allein generiert werden kann.

6.2 Schutz des privaten Schlüssels der CA

Für die Speicherung und Anwendung des privaten Schlüssels der CA sind solche technischen Komponenten und Verfahren einzusetzen, die dessen Bekanntwerden und unbefugte Verwendung verlässlich verhindern.

6.3 Aktivierungsdaten des CA-Krypto-Moduls

Aktivierungsdaten für den Betrieb des Krypto-Moduls müssen geheimgehalten werden und dürfen nicht im Klartext vorliegen. Die Aktivierung des Signatur-schlüssels durch Unbefugte muss technisch bzw. organisatorisch verhindert werden. Jede Aktivierung des Signaturschlüssels muss nachvollziehbar sein und authentisch protokolliert werden.

6.4 Technische Komponenten und Verfahren eines Zertifizierungsdiensteanbieters

6.4.1 Schutz der technischen Komponenten

Jeder Zertifizierungsdiensteanbieter hat Vorkehrungen zu treffen, die die zum Erstellen der Zertifikate und zum Abrufbarhalten der Verzeichnis- und Widerrufsdienste eingesetzten technischen Komponenten vor Kompromittierung und unbefugtem Zugriff schützen.

6.4.2 Weitere Anforderungen an technische Komponenten und Verfahren

Jeder Zertifizierungsdiensteanbieter hat durch entsprechende Sicherheitsmaßnahmen sicherzustellen, dass die Übertragung von Daten zwischen Einheiten, die organisatorisch und technisch getrennt geführt werden, nicht zu einer Kompromittierung der Signatur- oder Zertifizierungsdienste führt.

6.5 Gültigkeitsdauer von Zertifikaten

Die Gültigkeitsdauer eines User-Zertifikates Light ist vom Zertifizierungsdiensteanbieter in seinem Certification Practice Statement (CPS) festzulegen.

Der Zeitraum der Gültigkeit eines User-Zertifikates *Light* darf dabei den Zeitraum der Eignung der bei der Erstellung, Speicherung und Anwendung eingesetzten technischen Komponenten und Verfahren nicht überschreiten.

7 Zertifikats- und CRL-Profil

In diesem Kapitel wird das Profil der ausgegebenen Zertifikate und Widerrufslisten (CRLs) definiert.

7.1 Profil der ausgegebenen Zertifikate

7.1.1 Zulässige Formate

Die ausgegebenen User-Zertifikate Light haben den Spezifikationen für X.509 v3-Zertifikate zu entsprechen.

7.1.2 Mindestinhalte

Zertifikate Light haben alle zur Einstufung des Zertifikates als X.509 v3-Zertifikat erforderliche Angaben, insbesondere

- die in Kapitel 3.1.1 angegebenen Identifikationsmerkmale des Zertifikatsinhabers (Zertifizierungsdiensteanbieter oder natürliche Person) unter Berücksichtigung der dort angeführten Namenskonventionen,
- den öffentlichen Schlüssel sowie
- den Beginn und das Ende der Gültigkeit des Zertifikates
- zu enthalten. Zusätzlich sind im Zertifikat
- Informationen über die anzuwendende Policy Projects bzw. das anzuwendende CPS und
- Informationen über den Typ des Inhabers des Zertifikates (CA oder natürliche Person),
- anzuführen.

Die detaillierte Spezifikation der in einem Zertifikat Light enthaltenen Inhalte ist von der ausstellenden CA in ihrem CPS anzuführen.

7.1.3 Weitere Anforderungen

Ein Zertifikat Light ist mit der elektronischen Signatur der ausstellenden Zertifizierungsinstanz zu versehen.

7.2 Profil der ausgegebenen Widerrufslisten (CRLs)

Widerrufslisten (CRLs) sind als X.509 Version 2 CRLs auszugeben. Die detaillierte Spezifikation der in den Widerrufslisten (CRLs) enthaltenen Inhalte ist von der entsprechenden CA in ihrem CPS anzuführen.

8 Administration der Policy Projects für User Light Zertifikate

In diesem Kapitel werden Richtlinien zur Durchführung von Änderungen an der a.sign Policy Projects für User Light definiert.

8.1 Durchführung von Änderungen

8.1.1 Allgemeines

Die a.sign Policy Projects für User Light wird von einer a.sign Expertengruppe entwickelt, die sich aus den Bereichen Technik, Wirtschaft und Rechtswissenschaften zusammensetzt.

8.1.2 Erforderliche Schritte

- Änderungsvorschläge zur aktuellen Version der a.sign Policy Projects für User Light müssen zunächst der Expertengruppe in schriftlicher Form übermittelt werden.
- Die eingebrachten Änderungsvorschläge werden in der Policy-Expertengruppe behandelt und verabschiedet.
- Vor der Herausgabe der geänderten a.sign Policy Projects für User Light muss das Anerkennungsverfahren für a.sign Policies durchlaufen werden. Dabei werden die von der Expertengruppe verabschiedeten Änderungsvorschläge dem a.sign Plenary übermittelt. Dieses Plenary hat einen Monat Zeit, um die Vorschläge zu begutachten. Sollten innerhalb dieser Frist Einwände ausbleiben, wird die geänderte Policy Projects für User Light in einem Plenary-Meeting verabschiedet.

8.2 Veröffentlichung geänderter Policies

Jede neue Version der a.sign Policy Projects für User Light ist vom Informationsdienst zu veröffentlichen.

9 Anhang

Definitionen

Antragsteller: siehe → Zertifikatswerber

Aussteller: siehe → Zertifizierungsdiensteanbieter

authentifizieren: beglaubigen, die Echtheit bezeugen

authentisch: echt

Authentizität: Echtheit einer Schrift, Urkunde

Certificate Revocation List (CRL): siehe → Widerrufsliste

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

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

Common Name (CN): Name von Personen, Organisationen

Cross-Zertifikat: Zertifikat, mit dem eine Certification Authority einer anderen Hierarchie zertifiziert wird; erfordert Kompatibilität der Policies

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 das Dokument nicht nachträglich verändert wurde.

Distinguished Name (DN): eindeutiger, unverwechselbarer Name

Dritter: Person, die eine digitale Signatur empfängt oder 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)

Global Registration Authority (GRA): siehe → Globale Registrierungsstelle

Globale Registrierungsstelle: ist einer Certification Authority zugeordnet und mit zentralen Registrierungs- und Archivierungsaufgaben betraut

Hardware-Signaturerstellungseinheit: Hardware-Einheit, die als Signaturerstellungseinheit eingesetzt wird (siehe auch: → Signaturerstellungseinheit)

Kompromittierung des privaten Schlüssels: Der private Schlüssel ist zeitweise oder permanent für Unbefugte zugänglich.

Local Registration Authority (LRA): siehe → Lokale Registrierungsstelle

Lokale Registrierungsstelle: führt im Auftrag einer Certification Authority die Überprüfung der Identität eines Zertifikatswerbers entsprechend der Policy einer Zertifikatsklasse 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 den a.sign Primary Certification Authorities für jede Zertifikatsklasse ausgegeben werden

Primary Certification Authority (PCA): Certification Authority, die nur andere Certification Authorities zertifiziert; diese zertifizierten Certification Authorities müssen der entsprechenden Policy der PCA unterliegen

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 → Zertifizierungshierarchie**

Qualifiziertes Zertifikat: Zertifikat, das bestimmte, im Österreichischen Signaturgesetz festgelegte Angaben enthält und von einem Zertifizierungsdiensteanbieter ausgestellt wird, der bestimmten, im Österreichischen Signaturgesetz und in den auf seiner Grundlage ergangenen Verordnungen angegebenen Anforderungen genügt

Schlüsselaustausch: Bindung der Identität des Signators an ein neues Schlüsselpaar

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 Österreichischen Signaturgesetz und in den auf seiner Grundlage ergangenen Verordnungen festgelegte Sicherheitsanforderungen gestellt werden**

Signator: natürliche Person, der ein Schlüsselpaar (d.h. ein öffentlicher und ein privater Schlüssel) zugeordnet ist und die im eigenen Namen eine elektronische Signatur erstellt, oder ein Zertifizierungsdiensteanbieter, der Zertifikate für die Erbringung von Zertifizierungsdiensten verwendet

Signaturerstellungseinheit: **konfigurierte Software oder Hardware zur Verarbeitung des privaten Schlüssels**

Signaturprüfeinheit: **konfigurierte Software oder Hardware zum Überprüfen einer elektronischen Signatur**

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

Sperre eines Zertifikates: reversible, temporäre Ungültigkeitserklärung eines Zertifikates, um die Umstände eines möglicherweise erforderlichen Widerrufes eines Zertifikates klären zu können (siehe auch → Widerruf eines Zertifikates)

Sperrliste: Liste von Zertifikaten, die vor dem Ablauf ihrer Gültigkeitsdauer gesperrt wurden

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)**

Widerrufsliste: Liste von Zertifikaten, die vor dem Ablauf ihrer Gültigkeitsdauer widerrufen wurden

Widerruf eines Zertifikates: irreversible, dauerhafte Ungültigkeitserklärung eines Zertifikates (siehe auch → Sperre eines Zertifikates)

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

Zertifikat: elektronische Bescheinigung, mit der einer Person ein öffentlicher Schlüssel zugeordnet und die Identität der Person bestätigt wird (siehe auch → qualifiziertes Zertifikat)

Zertifikatinhaber: siehe → Signator

Zertifikatsklasse: Einteilung von Zertifikaten nach dem verwendeten Registrierungsverfahren (Light, Strong oder Uni)

Zertifikatstyp: Einteilung von Zertifikaten nach ihrem Verwendungszweck (User-, Server- oder Developer-Zertifikat)

Zertifikatsverzeichnis: Liste aller veröffentlichten Zertifikate

Zertifikatswerber: Person oder Institution, 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- und Zertifizierungsdienste erbringt (siehe auch → Signatur- und Zertifizierungsdienste)

Zertifizierungshierarchie: umfasst jene Einheiten, die im Rahmen von Zertifizierungen hierarchisch voneinander abhängen (Zertifizierungsinstanzen, Signatoren)

Zertifizierungsinfrastruktur: Gesamtheit der bei den Signatur- und Zertifizierungsdiensten beteiligten Einheiten (Certification Authority, Registrierungsstellen, Informationsdienst, ...)

Zertifizierungsinstanz: siehe → Zertifizierungsdiensteanbieter

Abkürzungen

Abkürzung	Bedeutung
CA	Certification Authority (Zertifizierungsinstanz)
CN	Common Name
CPS	Certification Practice Statement
CRL	Certificate Revocation List (Widerrufsliste für Zertifikate)
DN	Distinguished Name
FTP	File Transfer Protocol
GRA	Global Registration Authority (Globale Registrierungsstelle)
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol with SSL
LRA	Local Registration Authority (Lokale Registrierungsstelle)
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
SSL	Secure Socket Layer
S/MIME	Secure/Multipurpose Internet Mail Extensions
URL	Uniform Resource Locator