ARGE DATEN

# A-CERT Certificate Policy

## [gültig für Zertifikate für einfache und fortgeschrittene Signaturen]

Version 1.6/Juli 2009 - a-cert-certificate-policy.doc

OID-Nummer: 1.2.40.0.24.1.1.1.3

OID-Nummer: 1.2.40.0.24.1.1.5.1

OID-Nummer: 1.2.40.0.24.1.1.9.1

Gültigkeitshistorie OID-Nummer: 1.2.40.0.24.1.1.1.99



**Redaktionelle Hinweise:**
Das vorliegende Dokument ist mit einer fortgeschrittenen Signatur versehen. Das Datum der Signatur kann aus verschiedenen rechtlichen und organisatorischen Gründen vom Datum des Gültigkeitsbeginns des Dokuments abweichen. Die Signatur gibt keine Auskunft über den Gültigkeitsbeginn des Dokuments, sondern bestätigt nur die Unversehrtheit des Inhalts.

Mag. Dr. Hans G. Zeger, Vertretung ARGE DATEN als Obmann
cn=Mag. Dr. Hans G. Zeger, Vertretung ARGE DATEN als Obmann, c=AT, l=Wien, st=Wien, o=ARGE DATEN - Österreichische Gesellschaft für Datenschutz, email=hans.zeger@argedaten.at
2012.07.02 16:29:47 +02'00'

ARGE DATEN - Österr. Gesellschaft für Datenschutz http://www.argedaten.at info@a-cert.at ☎ +43/676/9107032, Fax +43/1/5320974
A-1160 Wien, Redtenbacherg. 20 DVR 0530794 ZVR 774004629 UID ATU 56627966 Gerichtsstand Wien

# INHALT:

# ANHANG:

# I. ÄNDERUNGSDOKUMENTATION

## 1. ÄNDERUNGEN 7. JULI 2009

- Klarstellung Bedeutung der verschiedenen Produkt- und Zertifikatsbezeichnungen
- Hinweis auf Beachtung der spezifischen GOVERNMENT-Policy-Anforderungen
- Definition der Verwendung von Zwischenzertifikaten
- Klarstellungen und Ergänzungen in den Zertifizierungsprozessen auf Grund betrieblicher Erfahrungen
- Anpassung der Gesetzeszitate an die Änderungen im Signaturgesetz von 2008
- Integration der Policy für einfache Signaturen und Verschlüsselung (OID=1.2.40.0.24.1.1.5.1 + Gültigkeitshistorie OID=1.2.40.0.24.1.1.5.99) und für Clienten-Zertifikate (OID=1.2.40.0.24.1.1.9.1 + Gültigkeitshistorie OID=1.2.40.0.24.1.1.9.99)
- Definition der Rolle von Dienstleistern, Zertifizierungspartnern und Vertriebspartnern
- Änderung der Vereinsangaben (entfernen der Bankverbindungsdaten, Anpassen der Kontaktdaten)
- Ergänzungen und Korrekturen in der Literaturliste
- redaktionelle Berichtigungen (Schreib- und Nummerierungsfehler)

## 2. ÄNDERUNGEN 12. APRIL 2007

- Konformität mit ETSI 102 042 hinzugefügt
- Klarstellung zur sicheren Aufbewahrung des privaten Schlüssels bei einfachen Signaturen, wie A-CERT CLIENT
- Ergänzungen zur Aufbewahrung des privaten Schlüssels in der Signaturerstellungseinheit
- Regeln zum Eintrag der Signaturerstellungseinheit als X.509v3-Erweiterung im Zertifikat und als zusätzliche Information im Verzeichnisdienst ldap://ldap.a-cert.at:389
- Abgrenzung zwischen Herausgeber und Zertifizierungsdienst präzisiert
- OID-Nummer für englische Übersetzung der Policy vergeben
- redaktionelle Berichtigungen (Schreib- und Nummerierungsfehler)

## 3. ÄNDERUNGEN 12. DEZEMBER 2005

- Hinzufügen der OID-Nummer dieses Dokuments in das Deckblatt des Dokuments
- Festlegung der Aufbewahrungsdauer der Zertifizierungsdokumentation auf 35 Jahre
- Definition von Testzertifikaten und Festlegen einer die Testzertifikate kennzeichnende OID-Nummer
- Einfügen einer X.509v3-Erweiterung zur Kennzeichnung von Testzertifikaten

- Erweiterung der Widerrufsmöglichkeiten der Zertifikate durch den Herausgeber
- redaktionelle Berichtigungen (Schreib- und Nummerierungsfehler)

## 4. ÄNDERUNGEN 4. OKTOBER 2004

- Ergänzung bei der Identitätsprüfung des Antragstellers (Signators)

## 5. ÄNDERUNGEN 22. SEPTEMBER 2004

- Ergänzungen bei der Erstellung des Private Key durch den Signator

## 6. STAMMFASSUNG 11. SEPTEMBER 2004

# II. GRUNDLAGEN

## A. DEFINITIONEN UND KURZBEZEICHNUNGEN

**Herausgeber**
Herausgeber dieser Certificate Policy ist die ARGE DATEN - Österreichische Gesellschaft für Datenschutz als Erbringer aller zu A-CERT zugeordneten Zertifizierungsdienste.

**fortgeschrittene Signatur**
elektronische Signatur im Sinne § 2 Z 3 [SigG], Zertifikate werden entsprechend den Vorgaben des [SigG] ausgegeben.

**qualifizierte Signatur**
elektronische Signatur im Sinne § 2 Z 3a [SigG], Zertifikate werden entsprechend den Vorgaben des [SigG] ausgegeben.

**qualifiziertes Zertifikat**
Zertifikat im Sinne § 2 Z 9 [SigG], Zertifikate werden entsprechend den Vorgaben des [SigG] ausgegeben.

**einfache Signatur**
elektronische Signatur im Sinne § 2 Z 1 [SigG], die weder den Anforderungen der fortgeschrittenen Signatur, noch denen der qualifizierten Signatur entspricht, Zertifikate werden entsprechend den Vorgaben des [SigG] ausgegeben.

**Root-Zertifikat**
Zertifikat, dass als oberste Instanz nur von sich selbst unterschrieben wird (auch Self-Signed-Zertifikat).

**Stamm-Zertifikat**
Zertifikat, dass die Ausstellung weiterer Zertifikate erlaubt und von einem übergeordneten Zertifikat unterschrieben ist.

**Sub-Zertifikat**
Zertifikat, dass von einem Stamm-Zertifikat unterschrieben ist.

**A-CERT**
Ist der Sammelbegriff für alle Zertifizierungsdienste des Herausgebers. Unterschiedliche Zertifizierungsdienste werden mit Zusätzen zu A-CERT gekennzeichnet. Die A-CERT Website ist unter http://www.a-cert.at abzurufen.

**ADVANCED**
Zusatz im Zertifikatsnamen (im Rahmen des X.509v3-Standards Teil der CN-Bezeichnung, z.B. A-CERT ADVANCED). Bezeichnet Zertifikate, die für die Erstellung fortgeschrittener Signaturen geeignet sind.

**GOVERNMENT**
Zusatz im Zertifikatsnamen (im Rahmen des X.509v3-Standards Teil der CN-Bezeichnung, z.B. A-CERT GOVERNMENT). Bezeichnet Zertifikate, die für die Erstellung von Amtssignaturen nach dem österreichischen E-Government-Gesetz geeignet sind. Diese Zertifikate sind gleichzeitig für fortgeschrittene Signaturen geeignet. Die Beschränkungen der Vergabe von Zertifikaten zur Amtssignatur sind in der GOVERNMENT-Policy (OID=1.2.40.0.24.1.1.3.1) beschrieben und unter http://www.a-cert.at/certificate-policy.html abrufbar.

**COMPANY**
Zusatz im Zertifikatsnamen (im Rahmen des X.509v3-Standards Teil der CN-Bezeichnung, z.B. A-CERT COMPANY). Bezeichnet Zwischenzertifikate, die gemäß den Regeln zur Ausstellung von Zertifikaten für fortgeschrittene Signaturen ausgestellt werden und die zur Erstellung von Zertifikaten (Sub-Zertifikate) und weiterer Zwischenzertifikate (Sub-CAs) geeignet sind. Die Regeln zur Vergabe der Sub-Zertifikate und Sub-CAs werden durch eigene COMPANY-Policies definiert. Fehlt eine eigene COMPANY-Policy, dann ist die vorliegende Policy, beschränkt auf Zertifikate für einfache Signaturen, in Verbindung mit der COMPANY-Policy (OID=1.2.40.0.24.1.1.2.1) anzuwenden. Diese ist unter http://www.a-cert.at/certificate-policy.html abrufbar.

**QUALIFIED**
Zusatz im Zertifikatsnamen (im Rahmen des X.509v3-Standards Teil der CN-Bezeichnung, z.B. A-CERT QUALIFIED). Bezeichnet qualifizierte Zertifikate, die für die Erstellung qualifizierter Signaturen geeignet sind. Diese Zertifikate unterliegen zusätzlichen Anwendungsbeschränkungen.

**CLIENT, SERVERCERT, FREECERT, DEMO**
Weitere mögliche Zusätze im Zertifikatsnamen (im Rahmen des X.509v3-Standards Teil der CN-Bezeichnung, z.B. A-CERT CLIENT, A-CERT SERVERCERT). Bezeichnet Zertifikate, die für die Erstellung sonstiger Signaturen (einfache Signaturen) und zur Verschlüsselung geeignet sind. Sonstige nicht angeführte Zusätze bezeichnen immer Zertifikate, die ausschließlich zur Erstellung einfacher Signaturen und zur Verschlüsselung geeignet sind.

**Policy**
Die in diesem Dokument beschriebene A-CERT Certification Policy wird im Folgenden kurz als "Policy" bezeichnet. Diese Policy ist als Rahmen zu verstehen, innerhalb dessen die Zertifizierungsdienste erbracht werden. Dieser Rahmen kann nicht erweitert werden. Eine Einschränkung der Anwendbarkeit der Policy auf bestimmte Zertifizierungsfälle und Signaturvorgänge ist jedoch durch Vereinbarungen möglich. Die AGB's des Herausgebers oder zusätzliche Vereinbarungen der Partnerunternehmen können jedoch nicht die vorliegende Policy ganz oder teilweise außer Kraft setzen. Die zu A-CERT ADVANCED gültige Policy wird im vorliegenden Dokument beschrieben und hat die OID-Nummer 1.2.40.0.24.1.1.1.3. Historische Versionen des Dokuments sind bei der Aufsichtsstelle

abzurufen oder unter der OID-Nummer 1.2.40.0.24.1.1.1.99 auf der Website des Herausgebers abgelegt. Die englische Übersetzung dieser Policy ist unter der OID-Nummer 1.2.40.0.24.1.1.1.12 abgelegt.

**Testzertifikate**
Bezeichnet Zertifikate, die auf Basis des X.509v3-Standards zu Testzwecken ausgestellt werden. Eine Identitätsprüfung der Antragsteller (Signatoren) findet nicht statt. Testzertifikate sind erkennbar, wenn zumindest eine der Bedingungen erfüllt ist:
- bei X509v3-Zertifikaten lautet die **CN-Bezeichnung** des Herausgebers (Issuer) **A-CERT FREECERT, A-CERT ADVANCED TEST**, **A-CERT GOVERNMENT TEST**, allgemein **A-CERT *** TEST**
- bei X509v3-Zertifikaten hat die **O-Bezeichnung** (Organisationsbezeichnung) des Antragstellers (Subject) den führenden Vermerk "Test: ", bei Privatpersonen den Eintrag "Testzertifikat",
- bei X509v3-Zertifikaten enthält das Zertifikat die zusätzliche X.509v3-Erweiterung **1.2.40.0.24.4.1.0=DER:01:01:FF** (Testeigenschaft = TRUE),
- bei anderen Zertifikatstypen sind Herausgeber- und/oder Antragstellerangaben so zu wählen, das ihre Testeigenschaft eindeutig zum Ausdruck kommt.

Die Kennzeichen eines Testzertifikats können in beliebigen Kombinationen auftreten. Für diese Zertifikate gilt abweichend die Certificate Policy für Testzertifikate (OID-Nummer: 1.2.40.0.24.1.1.4.1).

**Antragsteller**
Der Signator, der auf Basis dieser Policy, der AGB's des Herausgebers und allfälliger zusätzlicher Geschäftsbedingungen der Partnerunternehmen einen Antrag auf die Ausstellung eines Zertifikats stellt, wird im Folgenden als Antragsteller bezeichnet.

**Registrierungsstelle**
Die Geschäftsstellen des Herausgebers und weitere vom Herausgeber autorisierte Stellen die zur Entgegennahme und Prüfung von Zertifizierungsanträgen berechtigt sind. Personen, die die Entgegennahme und Prüfung der Zertifizierungsanträge durchführen werden als Zertifizierungspartner des Herausgebers bezeichnet.

**Dienstleister**
Einrichtungen, die vom Herausgeber mit der technischen oder wirtschaftlichen Umsetzung von Zertifizierungsdiensten teilweise oder ganz betraut sind.

**Vertriebspartner**
Einrichtungen, die mit dem Herausgeber spezifische Vertriebsvereinbarungen haben. Die Liste der Vertriebspartner ist über die Website des Herausgebers abrufbar.

**autorisierte Person**

Natürliche Person, die zur Prüfung von Zertifizierungsanträgen berechtigt ist. Dies können Mitarbeiter des Herausgebers, einer Registrierungsstelle, eines Dienstleisters, vertraglich berechtigte Zertifizierungspartner oder Mitarbeiter von Anbietern kommerzieller Identifizierungsdienste sein.

**Signaturbestimmungen**
Gesamtheit der in den Dokumenten [SigG], [SigV], [SigRL] (=EU-Signaturrichtlinie) verabschiedeten Bestimmungen.

**Beteiligte**
Gesamtheit aller Personen, die dieser Policy unterworfen sind. Insbesondere sind dies der Herausgeber, Registrierungsstellen, Dienstleister und Zertifizierungspartner in Hinblick auf Antragsprüfung, Ausgabe, Archivierung und Widerruf von Zertifikaten im Sinne dieser Policy. Weiters der Signator im Rahmen der Anwendung des Zertifikats bei elektronischen Signaturen und der Empfänger eines Zertifikates im Zusammenhang mit einer elektronischen Signatur im Rahmen der Prüfung der zulässigen Verwendung des Zertifikates.

**Aufsichtsbehörde**
Die für die A-CERT Zertifizierungsdienste zuständige Aufsichtsbehörde.

**Bestätigungsstelle**
Nach dem österreichischen Signaturgesetz (§ 19 SigG) eingerichtete Bestätigungsstelle oder eine nach einer auf Basis der EU-Richtlinie 1999/93/EG [SigRL] erlassenen gesetzlichen Bestimmung in einem anderen Staat eingerichtete Bestätigungsstelle für sichere Signaturerstellungseinheiten (§ 18 Abs. 5 3. Satz SigG).

Ansonsten werden die Begriffe gemäß [SigG], [SigVO], [SigRL], [X.509v3], [RFC5280] und [RFC3647] oder anderer in **Fehler! Verweisquelle konnte nicht gefunden werden.** (p**Fehler! Textmarke nicht definiert.**) genannten Dokumente verwendet.

# B. ÜBERBLICK

Die vorliegende Certificate Policy enthält alle Regeln für die Ausstellung und Verwendung von Zertifikaten für einfache und fortgeschrittene Signaturen. Die Zertifikate entsprechen der Definition § 2 Abs. 8 [SigG]. Die Certificate Policy entspricht den Vorgaben „Normalized Certificate Policy“ (NCP) in [ETSI TS 102 042].

Diese Policy wurde in Übereinstimmung mit den Signaturbestimmungen verfasst und bildet gemeinsam mit den "A-CERT Allgemeine Betriebs- und Nutzungsbedingungen" (AGBs) und der - soweit gemäß [SigG] erforderlichen - Anzeige bei der Aufsichtsbehörde die Grundlage für die Verwendung von A-CERT Zertifikaten durch den Signator.

Änderungen auf Grund gesetzlicher Änderungen werden zum Zeitpunkt des Inkrafttretens der gesetzlichen Bestimmungen wirksam, sonstige Änderungen vier Wochen nach Verlautbarung auf der Website von A-CERT.

# C. ANWENDUNGSBEREICH

Die A-CERT Certificate Policy gilt für alle Zertifikate, die für einfache und fortgeschrittene Signaturen ausgestellt wurden. Weiters gilt die Policy auch für alle Dienste, die mittels A-CERT Zertifikaten vom Herausgeber selbst betrieben werden.

Die ausgestellten Zertifikate können vom Betreiber sowohl zur Durchführung von Signatur- und Geheimhaltungsoperationen, als auch zum Signieren einzelner elektronischer Dokumente (Dateien) verwendet werden.

Die mittels dieser Policy ausgestellten Zertifikate (Zertifikate mit der Zusatzbezeichnung ADVANCED, GOVERNMENT bzw. QUALIFIED) sind auch zur Erstellung von Signaturen im Sinne des § 2 Z 3 (fortgeschrittene Signaturen) [SigG] geeignet.

# III. VERPFLICHTUNGEN UND HAFTUNGSBESTIMMUNGEN

## A. VERPFLICHTUNGEN DES HERAUSGEBERS

Der Herausgeber verpflichtet sich sicherzustellen, dass alle Anforderungen, die im Abschnitt III dargelegt sind, den Beteiligten zur Kenntis gebracht werden und die Erfüllung vertraglich vereinbart wird.

Der Herausgeber ist verantwortlich für die Einhaltung aller Geschäftsprozesse zu Ausstellung, Verwaltung und Widerruf von Zertifikaten, die in der gegenständlichen Policy beschrieben sind; dies gilt auch für jene Funktionen, deren Ausführung an Vertragspartner ausgegliedert wurden (z. B. Führung eines Verzeichnisdienstes, Vertrieb, Identitätsprüfung).
Es sind keine zusätzlichen Verpflichtungen direkt oder durch Referenzierung in den Zertifikaten ausgewiesen.

Zertifikate zu Schlüsseln, die mit Verfahren erstellt werden, die gemäß Signaturverordnung oder gemäß der Entscheidung der Aufsichtsstelle oder anerkannter Standardisierungsgremien (insbesondere gemäß den speziellen Empfehlungen [ETSI SR 002 176] bzw. des ab 2009 geplanten Folgestandards ETSI TS 102 176) als nicht mehr sicher anzusehen sind, werden vom Herausgeber widerrufen.

Der Herausgeber behält sich das Recht vor, auch dann Zertifikate zu widerrufen, wenn die verwendeten Verfahren nach internen Erkenntnissen nicht mehr sicher sind oder die enthaltenen Eigenschaften irreführend oder unvollständig sind.

Erfolgt der durch den Herausgeber veranlasste Widerruf vor Ablauf der vertraglich vereinbarten Gültigkeitsdauer des Zertifikats, hat der Signator für die Dauer der vertraglich vereinbarten Restlaufzeit Anspruch auf Ausstellung eines gleichwertigen, mit sicheren Verfahren hergestellten Zertifikats. Sonstige Entschädigungen oder Kostenersätze sind nicht vorgesehen.

## B. VERPFLICHTUNGEN DES SIGNATORS

Der Herausgeber bindet den Signator vertraglich an die Einhaltung der nachfolgend angeführten Verpflichtungen.

Dem Antragsteller werden alle Vertragsbedingungen auf der Website des Herausgebers zugänglich gemacht. Gleichzeitig mit dem Absenden des Bestellformulars bestätigt er deren Kenntnisnahme und Akzeptanz.

Die dem Signator auferlegten Verpflichtungen umfassen:

1. die Angabe vollständiger und korrekter Informationen in Übereinstimmung mit den Anforderungen dieser Policy insbesondere anlässlich des Vorgangs der Registrierung,
2. die Aufbewahrung des privaten Schlüssels in einer Hardware-Einheit, zu der der Signator den alleinigen Zugriff hat (z.B. verschlüsseltes Abspeichern des privaten Schlüssels mittels Passwort bzw. Passphrase, spezielle Signaturerstellungseinheiten, die das Auslesen des privaten Schlüssels verhindern oder wesentlich erschweren).
   Im Fall einfacher Signaturen, wie zum Beispiel A-CERT CLIENT, sind auch Zutrittsbeschränkungen und organisatorische Maßnahmen, die den Zugang zum Computer der das Zertifikat enthält beschränken, als ausreichende Sicherheitsmaßnahmen im Sinne dieser Policy zu verstehen.
3. im Falle der Selbstgenerierung des privaten Schlüssels werden geeignete sichere Verfahren angewandt, die eine ausreichende Zufallsqualität bei der Schlüsselerzeugung gewährleisten, insbesondere sind dies ausdrücklich dafür vorgesehene Hardwarekomponenten, wie HSM-Module oder Softwarekomponenten, die es erlauben durch Systemereignisse die Zufallsqualität zu erhöhen (Angabe von Dateien mit Zufallszahlen, Durchführen von Mausbewegungen oder Tastaturanschlägen während der Schlüsselgenerierung). A-CERT behält sich vor, vom Signator vollständige Auskunft über den Schlüsselgenerierungsvorgang zu verlangen und bei Bedenken bezüglich der Zufallsqualität des Schlüssels einen Zertifizierungsantrag abzulehnen. Ungeeignete Verfahren zur Schlüsselgenerierung werden auf der Website von A-CERT bekannt gemacht und dürfen nicht verwendet werden,
4. die Anwendung entsprechender Vorsicht, um den unbefugten Gebrauch des privaten Schlüssels zu verhindern und die sichere Vernichtung desselben nach Ablauf der Gültigkeitsperiode,
5. die unverzügliche Benachrichtigung des Herausgebers, wenn vor Ablauf der Gültigkeitsdauer eines Zertifikats eine oder mehrere der folgenden Bedingungen eintreten:
   - der private Schlüssel des Signators wurde möglicherweise kompromittiert,
   - die Kontrolle über den privaten Schlüssel ging verloren,
   - die im Zertifikat beinhalteten Informationen sind inkorrekt oder haben sich geändert,
   - die weitere Verwendung des Schlüssels im Sinne dieser Policy ist nicht mehr erlaubt.
6. Die sichere Verwahrung des Schlüssels liegt in der ausschließlichen Verantwortung des Signators.

**Einsatz auslesbarer Datenträger für private Schlüssel:**
Soweit der private Schlüssel in auslesbaren Datenträgern gespeichert ist (Diskette, USB-Stick, Festplatte usw.), verpflichtet sich der Signator zur getrennten Verwahrung des notwendigen Passwortes und zur besonders sorgfältigen Verwahrung des Datenträgers. Bei transportablen Datenträgern (Diskette, USB-Stick, CD, ...) erfolgt die Aufbewahrung in verschlossenen, nur für den Signator zugänglichen Behältern, bei fix eingebauten Datenträgern (Festplatten) ist der Zugriff auf den Signator beschränkt. Systemadministratoren sind vertraglich zur Sicherung

der Integrität des privaten Schlüssels zu verpflichten. Es ist sicherzustellen, dass nur vom Signator veranlasste Kopien erstellt werden (gilt auch für Backupkopien).

Weiters stellt der Signator nach dem Stand der Technik sicher, dass der verwendete Datenträger frei von Schadprogrammen ist, die den privaten Schlüssel auslesen, kopieren oder sonstwie verändern. Insbesondere unternimmt der Signator ausreichende Schutzmaßnahmen gegen Malware jeglicher Art, insbesondere Viren, Würmer, Programme mit Trapdoorfunktionen und Spyware-Programme.

# C. VERPFLICHTUNGEN DES EMPFÄNGERS VON ZERTIFIKATEN

Zertifikate des Herausgebers sind nur im Rahmen dieser Policy gültig, daher müssen Empfänger folgende Prüfschritte beachten:

- Überprüfung der Gültigkeitsperiode und des Widerrufsstatus des Zertifikats unter Verwendung der vom Herausgeber bereitgestellten Abfragemöglichkeiten,
- Beachtung der im Zertifikat oder den veröffentlichten Geschäftsbedingungen dargelegten Einschränkungen der Nutzung des Zertifikats.

Bestehen Zweifel an der Gültigkeit des Zertifikats, ist immer mit dem Herausgeber direkt Kontakt aufzunehmen. Es werden dann geeignete Maßnahmen zur Klärung der Gültigkeit des Zertifikats gesetzt.

# D. HAFTUNG

Der Herausgeber haftet

- für seinen Verantwortungsbereich für die Einhaltung dieser Policy, insbesondere für die darin festgelegten Maßnahmen zur prompten Veröffentlichung von Widerrufslisten und die Einhaltung der in der Policy genannten Widerruf-Standards (ITU X.509v2).
- dafür, Antragsteller, Signatoren und Empfänger von Signaturen und Zertifikaten über ihre Verpflichtungen zur Beachtung der Policy nachweislich in Kenntnis gesetzt zu haben. Der Nachweis der Kenntnisnahme ist jedenfalls erbracht, wenn die vom Herausgeber ausgegebenen Zertifikate eindeutige Verweise auf die Dokumentationsstellen für die anzuwendende Policy enthält.
- dafür, dass die im Zertifikat enthaltenen Daten des Antragstellers zum Zeitpunkt der Ausstellung des Zertifikats überprüft wurden und keine Abweichungen der Daten gegenüber den Prüfverzeichnissen und vorgelegten Dokumenten festgestellt wurden. Die Prüfmaßnahmen sind in dieser Policy dokumentiert, die verwendeten Prüfverzeichnisse ergeben sich aus der Art des Antragstellers und können sachlich und regional unterschiedliche Quellen umfassen. Welche Quellen für welche Antragsteller verwendet werden, wird im Detail im Rahmen der internen Prozessdokumentation geregelt.
- dafür, dass Hinweisen einer fehlerhaften Identitätsprüfung durch eine Registrierungsstelle oder anderen vom Herausgeber

autorisierten Personen und Stellen in jedem Fall nachgegangen wird und Zertifikate ohne ausreichende Identifikation des Signators nicht freigegeben oder bei Zweifel einer ordnungsgemäßen Identitätsprüfung unverzüglich widerrufen werden.

Der Herausgeber haftet nicht, falls er nachweisen kann, dass ihn an der Verletzung der oben angeführten Verpflichtungen keine Schuld trifft, dies trifft insbesondere zu, wenn Antragsteller oder Signatoren ausgegebene Zertifikate entgegen der gültigen Policy verwenden oder Empfänger von Signaturen und Zertifikaten es unterlassen Gültigkeitszeitraum, bestehende Widerrufe oder sonstige Beschränkungen einer durch ein Zertifikat des Herausgebers bestätigten Unterschrift zu beachten.

# IV. SPEZIFIKATIONEN ZUR ERBRINGUNG VON ZERTIFIZIERUNGSDIENSTEN

## A. ALLGEMEINES

Im Rahmen dieser Policy werden folgende (Teil-)Dienste spezifiziert: Bereitstellung von Registrierungsdiensten, Zertifikatsgenerierung, Zertifikatsausgabe, Widerrufsdienste und Abfragedienste über den Zertifikatsstatus.

## B. OPERATIVE MAßNAHMEN ZUR BEREITSTELLUNG DES ZERTIFIZIERUNGSDIENSTES

Zur Gewährleistung eines ordnungsgemäßen und in jedem Schritt nachvollziehbaren Zertifizierungsprozesses wurden folgende Maßnahmen ergriffen:

1. Die für die Zertifizierung notwendigen Prozesse sind vom Herausgeber vollständig dokumentiert.
2. Über die Website des Herausgebers werden sowohl diese Policy, die allgemeinen Betriebs- und Nutzungsbedingungen (AGB's), als auch laufende Informationen zu den angebotenen Diensten und verwendeten Verfahren zugänglich gemacht.
3. Der Vorstand des Herausgebers genehmigt die notwendigen Dokumentationen und Zertifizierungsrichtlinien und ernennt jene Personen und externe Vertragspartner, die für die operative Umsetzung verantwortlich sind. Verabschiedung und Ernennung werden schriftlich dokumentiert.
4. Der Vorstand des Herausgeber entscheidet auch, an welchem Ort die Zertifizierungen stattzufinden haben.
5. Über die Website bzw. sofern bei den Zertifikatsinhabern verfügbar per eMail wird zeitgerecht über Änderungen informiert, die in der Certification Policy vorgenommen werden. Die aktuelle Version ist jeweils online abrufbar.
6. Die den Betrieb des Zertifizierungsdienstes betreffenden Ereignisprotokolle werden 35 Jahre aufbewahrt.
7. Der Vorstand kann für die Dienste dieser Policy eine geeignete bevollmächtigte Person oder einen geeigneten Dienstleister beauftragen. Diesem obliegen auch die Festlegung und Umsetzung aller operativen Maßnahmen inkl. der Festlegung der erforderlichen Dokumentationen, Zertifizierungsrichtlinien und Betriebsstandorte.

# C. SCHLÜSSELVERWALTUNG HERAUSGEBER (CA SCHLÜSSEL)

## 1. ERZEUGUNG DER CA SCHLÜSSEL

Die notwendigen Schlüssel zur Erbringung der Zertifizierungsdienste gemäß dieser Policy werden in einem dedizierten System nach dem Vier-Augen-Prinzip generiert. Soweit diese Schlüssel zur Ausstellung von qualifizierten Zertifikaten verwendet werden, werden sie in Systemen erstellt, die den Anforderungen [ETSI TS 101 456] in der zum Zeitpunkt der Schlüsselerstellung gültigen Version insbesondere gemäß § 3 [SigVO] entsprechen.

Die verwendeten Algorithmen und Schlüssellängen entsprechen den zum Zeitpunkt der Erstellung gültigen technischen Empfehlungen der jeweils zutreffenden Aufsichtsbehörde, nationalen oder internationalen Bestimmungen, den ETSI-Standards oder den Vorgaben anderer (privater oder staatlicher) Einrichtungen, die zur Prüfung der Zertifizierungsdienste des Herausgebers herangezogen werden. Soweit die verschiedenen Empfehlungen unterschiedliche Anforderungen und Sicherheitsniveaus beschreiben wird jene Variante gewählt die zumindest den Mindestanforderungen aller relevanten Empfehlungen entspricht.

## 2. SPEICHERUNG DER CA SCHLÜSSEL

Der Schlüssel bleibt im für die Durchführung der Zertifizierung vorgesehenen System gespeichert. Darüber hinaus werden keine Sicherungskopien erstellt oder aufbewahrt. Die Verwendung des Schlüssels ist nur durch je zwei befugte Personen erlaubt.

## 3. VERTEILUNG DER ÖFFENTLICHEN CA SCHLÜSSEL

Der Herausgeber stellt durch die folgenden Maßnahmen sicher, dass die Integrität und Authentizität der öffentlichen Schlüssel anlässlich der Verteilung gewahrt bleibt:

- durch Übergabe des Root-Schlüssels zur Veröffentlichung an die Aufsichtsstelle durch Übermittlung eines signierten PKCS#10 Certificate Requests,
- durch Ausstellung und Veröffentlichung eines selbst signierten Root-Zertifikats auf der Website des Betreibers,
- durch freiwillige Zertifizierungen durch anerkannte (private oder staatliche) Audit- und Prüfeinrichtungen,
- durch Publikation und Integration in Software vertrauenswürdiger Drittfirmen. Der aktuelle Stand der Integration des Root-Zertifikates bei Drittfirmen kann über die Website des Herausgebers abgerufen werden.

Im Zusammenhang mit Zertifikaten für fortgeschrittene und einfache Signaturen muss zumindest eine der Veröffentlichungsformen erfüllt sein. Im Zusammenhang mit qualifizierten Zertifikaten ist

jedenfalls eine Veröffentlichung durch die vorgesehene Aufsichtsstelle erforderlich.

Das Zertifikat des CA Schlüssels wird den Signatoren durch Veröffentlichung im Rahmen des Verzeichnisdienstes (ldap://ldap.a-cert.at:389) zugänglich gemacht. Der Herausgeber gewährleistet die Authentizität dieses Zertifikats.

### 4. SCHLÜSSELOFFENLEGUNG

Der geheime Schlüssel der Root CA ist nicht öffentlich verfügbar.

### 5. VERWENDUNGSZWECK VON CA SCHLÜSSELN

Der private Schlüssel der Zertifizierungsstelle wird nur für die Erstellung von den dafür ausdrücklich vorgesehenen Zertifikaten und für die Signatur der zugehörigen Widerrufslisten innerhalb der für die Zertifizierung bestimmten Räumlichkeiten verwendet.

### 6. ENDE DER GÜLTIGKEITSPERIODE VON CA SCHLÜSSELN

Geheime Schlüssel zur Signatur von Zertifikaten werden verwendet, solange die verwendeten Algorithmen als sicher im Sinne II.A dieser Policy anzusehen sind.

Schlüssel, die den Sicherheitsanforderungen nicht mehr entsprechen oder aus anderen Gründen nicht mehr weiter betrieben werden, werden gelöscht. Es erfolgt keine Archivierung nicht aktiver Schlüssel.

## D. SCHLÜSSELVERWALTUNG SIGNATOR

Die Schlüssel des Signators werden abhängig vom betriebenen Zertifizierungsdienst entweder vom Signator oder vom Herausgeber erzeugt oder die Methode wird dem Signator freigestellt. Die Methode wird bei der Anzeige des jeweiligen Dienstes der Aufsichtsbehörde bekannt gegeben.

Werden Schlüssel zu qualifizierten Zertifikaten erstellt, ist die Verwendung geeigneter dedizierter Signaturerstellungseinheiten zwingend erforderlich. Geeignete Signaturerstellungseinheiten werden auf Anfrage vom Herausgeber bekannt gegeben oder auf der Website des Herausgebers veröffentlicht.

### 1. VERWAHRUNG DES PRIVATEN SCHLÜSSELS IN EINER SIGNATURERSTELLUNGSEINHEIT BEIM SIGNATOR

Werden für die Signaturerstellungseinheit spezielle Hardwarekomponenten verwendet die das Auslesen des privaten Schlüssels verhindern, können diese von Bestätigungsstellen evaluiert sein, alternativ kann die Eignung durch

Selbstdeklaration des Herstellers gegeben sein. Welchen Kriterien und Standards eine Signaturerstellungseinheit genügt wird vom Herausgeber dokumentiert und kann über die Website des Herausgebers oder auf Anfrage beim Herausgeber abgerufen werden.

Die Verwendung derartiger Signaturerstellungseinheiten kann als X.509v3-Erweiterung im Zertifikat eingetragen werden.

Der Eintrag kann in folgender Form erfolgen:
- Bereitstellung durch den Herausgeber
- Angaben des Signators

### a) Bereitstellung durch den Herausgeber

*Variante I: dedizierte Signaturerstellungseinheit*

Der private Schlüssel des Signators wird vom Herausgeber in einer dafür speziell geeigneten Signaturerstellungseinheit generiert und nur in dieser Signaturerstellungeinheit ausgeliefert. Es existiert keine Kopie des privaten Schlüssels in anderer Form.

Das Zertifikat erhält dann folgenden X.509v3-Erweiterung:
1.2.40.0.24.4.1.1: <verwendete Hardware>

Unter "<verwendete Hardware>" wird die handelsübliche oder durch eine Bestätigungsstelle verwendete Bezeichnung zur eindeutigen Kennzeichnung der Hardware verwendet, z.B. "Aladdin eToken Pro64k" für einen USB-Token mit der evaluierten Komponente "CardOS V4.2 CNS with Application for Digital Signature" der Firma Siemens.

Der aktuelle Stand der unterstützten Hardwarekomponenten und welche Bestätigungsstellen nach welchen gesetzlichen Bestimmungen die Evaluation durchführten, findet sich auf der Website des Herausgebers.

Wird das Zertifikat im ldap-Verzeichnisdienst des Herausgebers veröffentlicht wird in den Stammdaten zusätzlich die verwendete Hardware unter der Bezeichnung "**acertIssuerInfo**" eingetragen.

*Variante II: gesicherte Erstellung des Schlüssels für den Signator*

Der private Schlüssel des Signators wird vom Herausgeber in einer dafür speziell betrieben Signaturerstellungsumgebung und mit einem vom Signator vergebenen Passwort verschlüsselt. Die Übergabe des Schlüssels erfolgt entweder persönlich oder durch gesicherte (verschlüsselte) Datenübertragungswege. Zu keinem Übergabezeitpunkt kann auf den privaten Schlüssel ohne Kenntnis eines Passwortes zugegriffen werden. Kopien der privaten Schlüssels werden nach Ende des Übergabeverfahrens beim Herausgeber gelöscht. Allfällig vorhandene Backup-Kopien werden beim Herausgeber so gesichert aufbewahrt, dass eine unbeabsichtigte Übernahme in produktive Systeme nicht möglich ist.

### b) ANGABEN DES SIGNATORS

Der Signator gibt an, mit welcher Hardware er den privaten Schlüssel generiert hat.

Diese Angaben werden vom Herausgeber dahingehend geprüft, ob das angegebene Produkt tatsächlich zur gesicherten Verwahrung eines privaten Schlüssels geeignet ist. Grundlage dieser Überprüfung sind Herstellerangaben ("Selbst-Deklaration") oder Berichte von Bestätigungsstellen.

Das Zertifikat erhält dann folgende X.509v3-Erweiterung:
1.2.40.0.24.4.1.2: <verwendete Hardware>

Unter "<verwendete Hardware>" wird die handelsübliche oder durch eine Bestätigungsstelle verwendete Bezeichnung zur eindeutigen Kennzeichnung der Hardware angegeben.

Wird das Zertifikat im ldap-Verzeichnisdienst des Herausgebers veröffentlicht wird in den Stammdaten zusätzlich die verwendete Hardware unter der Bezeichnung "**acertSignerInfo**" eingetragen.

### c) ABSCHLUSS

Fehlen beide X509v3-Erweiterungen, dann gelten die Aufbewahrungsbestimmungen für den privaten Schlüssel gemäß "Verpflichtungen des Signators Abschnitt: Einsatz auslesbarer Datenträger für private Schlüssel" (p12).

# E. ZERTIFIKATE DER ANTRAGSTELLER

## *1. ANTRAGSTELLUNG*

Anträge zur Zertifizierung werden sowohl online als auch offline entgegen genommen.

Die Maßnahmen und Abläufe zur Identifikation und Registrierung des Antragstellers orientieren sich am jeweiligen

Zertifizierungsdienst und können sowohl sachliche, als auch regionale Unterschiede aufweisen.

Die Identifikation des Antragstellers gilt als abgeschlossen, wenn keine sachlich begründeten Zweifel an der Identität des Antragstellers bestehen. Der Abschluss des Identifikationsprozesses / die erfolgreiche Identifikation wird
(a) durch Vorlage ausreichender gerichtlich oder notariell beglaubigter Urkunden oder
(b) durch schriftliche Bestätigung durch einen autorisierten Mitarbeiter des Herausgebers oder
(c) durch einen autorisierten Zertifizierungspartner des Herausgebers oder
(d) durch sonstige kommerzielle Identitätsprüfdienste, insbesondere von Logistikunternehmen
bestätigt.

Die vorliegende Policy beschreibt den grundlegenden Ablauf, der im Einzelfall auf Grund sachlicher oder rechtlicher Gegebenheiten verfeinert werden kann.

1. Bevor der Vertrag zwischen dem Signator und dem Herausgeber abgeschlossen wird, werden dem Signator die Geschäftsbedingungen und allfällige sonstige Bestimmungen zur Nutzung des Zertifikats elektronisch zugänglich gemacht.
2. Das Antragsformular und die Informationen sind über die Website des Herausgebers oder der Vertriebspartner zugänglich.
3. Der Zertifikatsantrag enthält folgende Mindestangaben: den vollständigen Namen und die Anschrift des Signators.
4. Zusätzliche Angaben zur Person des Signators: Telefonnummer, Faxnummer und eMailadresse, Berufs- und Qualifikationsangaben, allenfalls weitere Kontaktdaten. Abhängig vom Zertifizierungsdienst können einzelne Angaben optional oder obligatorisch sein. Soweit der Signator eine natürliche Person ist, sind die Angabe der Nummer eines amtlichen Personaldokuments und der Name der ausstellenden Behörde erforderlich. Soweit das Dokument nicht im Original oder als beglaubigte Ausweiskopie zur Prüfung vorgelegt wird, ist die Übermittlung einer Ausweiskopie an den Herausgeber erforderlich. Beglaubigte Ausweiskopien sind jedenfalls im Original an den Herausgeber zu übermitteln.
5. Zusätzliche Angaben zur vertretenen Organisation: Wird von einer Person ein Zertifikat beansprucht, mit dem Rechtsgeschäfte für eine Organisation oder eine andere Person erledigt werden können, dann sind folgende Zusatzinformationen obligatorisch: Name und Anschrift der Organisation/Person und Organisationsform (z.B. eingetragener Verein, protokolliertes Unternehmen, ...). Weiters ist zumindest eine Stelle anzugeben, die als Bestätigungsstelle für diese Organisation geeignet ist (z.B. zugehörige Kammer, Firmenbuch, Vereinsbehörde, Aufsichtsbehörde, ...). Als Bestätigungsstelle sind grundsätzlich alle staatlich anerkannten Behörden und Organisationen geeignet, die öffentlich abrufbare Verzeichnisse führen und vor Aufnahme in diese Verzeichnisse eine

Identitätsprüfung durchführen. Sind Organisationen per Gesetz eingerichtet, ist statt der Bestätigungsstelle die Gesetzesstelle anzuführen, auf Grund der die Einrichtung erfolgte. Zur Prüfung der Adressangaben der Organisation werden das amtliche Telefonbuch oder der Amtskalender herangezogen. Organisationen, die weder bei einer geeigneten Bestätigungsstelle registriert sind noch per Gesetz eingerichtet sind, werden den Privatpersonen gleichgestellt behandelt. Die Organisationsangaben werden als optionale Zusatzangaben, vergleichbar dem Beruf oder der Qualifikation einer Privatperson angesehen.
Weiters kann angegeben werden, für welche Aufgaben (Aufgabenbereiche) der Signator vertretungsbefugt ist (gegebenenfalls ist der Umfang wertmäßig oder vorgangsmäßig zu begrenzen).

6. Angaben zum Zweck der Verwendung des Zertifikats:
   Die Angaben zum Zweck können je nach bereitgestelltem Zertifizierungsdienst optional oder obligatorisch sein.
7. Kenntnisnahme und Zustimmung zu den Allgemeinen Betriebs- und Nutzungsbedingungen (AGB's) des Herausgebers, zur vorliegenden Policy und gegebenenfalls zu weiteren zertifizierungsabhängigen Vereinbarungen.
8. Der Antragsteller hat ein Aktivierungspasswort anzugeben, mit dessen Hilfe er nach erfolgter Zertifizierung Zugang zu den bereitgestellten Unterlagen (persönliches Zertifikat, privater Schlüssel, ...) hat.

## 2. ANTRAGSPRÜFUNG

Die Antragsprüfung ist vollständig dokumentiert.

Die Registrierungsstelle nimmt die folgenden Überprüfungen des Antrags vor:

- Prüfung der Organisation (gemäß vom Antragsteller vorgelegter unbedenklicher Bescheinigungen, lt. Auskunft (inkl. Datenbankabfrage) einer zuständigen Bestätigungsstelle oder anhand von Datenbanken vertrauenswürdiger Dritter),
- Prüfung der Vertretungsbefugnis und der Angaben/Unterlagen der im Antrag genannten Personen,
- die Identitätsprüfung ist abgeschlossen, sofern der Antrag persönlich in einer der Registrierungsstellen erfolgte und vom Antragsteller ein amtliches Personaldokument im Original vorgelegt wurde oder ein durch Gericht oder Notar beglaubigter Identitätsnachweis im Original übermittelt wurde. In allen anderen Fällen erfolgt der Abschluss der Identitätsprüfung im Zuge der Antragsbearbeitung (siehe "Antragsbearbeitung" p22).

Zusätzliche Prüfungen werden ausdrücklich vorbehalten und können erforderlich sein, wenn

- die Auskünfte der Bestätigungsstellen ungenügend sind,
- Zweifel an der Verfügungsberechtigung über bestimmte Nummern- oder Namenselemente bestehen (etwa Verfügungsberechtigung über einen bestimmten Domainnamen),

- die Vertretungsbefugnis nicht ausreichend umschrieben bzw. dokumentiert ist,
- bei sonstigen Widersprüchen oder Unklarheiten im Zertifizierungsantrag.

## 3. ANTRAGSBEARBEITUNG

Zur Sicherung der Identität des Signators wird nach Erstellung des Zertifikats und/oder des privaten Schlüssels eine Zertifizierungsbestätigung zugestellt.

Abhängig von der Antragstellung erfolgt die Zustellung
- bei Zertifikaten für fortgeschrittene Signaturen und Amtssignaturen als gewöhnliche Post (soweit möglich auch als elektronische Post inkl. E-Mail oder Fax), sofern die Identitätsprüfung im Rahmen der Antragstellung abgeschlossen wurde.
- bei Zertifikaten für fortgeschrittene Signaturen und Amtssignaturen über einen Zustelldienst, der auch eine Identitätsprüfung bei der Übergabe von Dokumenten anbietet (in Österreich ist das insbesondere die POST AG, , sofern die Identitätsprüfung noch nicht vollständig abgeschlossen wurde. In Fall der POST AG werden Poststücke als "eingeschrieben, eigenhändig mit Rückschein" zugestellt, bei anderen Zustelldiensten werden gleichwertige Verfahren verwendet. Die Identitätsprüfung gilt in diesem Fall als abgeschlossen, wenn die zugestellte Zertifizierungsbestätigung unterschrieben retourniert wird und die darin enthaltene Unterschrift mit der Unterschrift auf vorab vorgelegten amtlichen Dokumenten vergleichbar ist. Bei erheblichen Abweichungen wird über einen getrennten Weg ein Unterschriftsprobenblatt mit der aktuellen Unterschrift des Antragstellers angefordert.
- bei Zertifikaten für fortgeschrittene Signaturen und Amtssignaturen durch persönliche Abholung beim Herausgeber oder einer Registrierungsstelle, sofern die Identitätsprüfung noch nicht vollständig abgeschlossen wurde. Die Identitätsprüfung gilt als abgeschlossen, wenn die ausgehändigte Zertifizierungsbestätigung vor einer autorisierten Person unterschrieben wird und sich der Antragsteller durch ein amtliches Dokument (Original) ausweisen kann. Der Vorgang ist durch die autorisierte Person zu bestätigen.
- bei qualifizierten Zertifikaten erfolgt die Zustellung ident wie bei Zertifikaten für fortgeschrittene Signaturen und Amtssignaturen, jedoch mit der Einschränkung, dass Signaturerstellungseinheiten jedenfalls eingeschrieben zuzustellen sind.
- bei Zertifikaten für einfache Signaturen als gewöhnliche Post (sofern geeignet auch als elektronische Post inkl. E-Mail oder Fax), sofern keine vernünftigen Zweifel zu den Identitätsangaben des Antragstellers existieren.

Nach Erhalt und erfolgreicher Unterschriftsprüfung der vom Empfänger unterfertigten Zertifizierungsbestätigung wird der Zugang zu Zertifikat und/oder privatem Schlüssel freigeschalten.

Der Abruf dieser Informationen ist nur mit Hilfe des vom Antragsteller selbst vergebenen Aktivierungspassworts und der in der Zertifizierungsbestätigung genannten Referenznummer möglich.

Auf Grund dieser Maßnahmen ist sichergestellt, dass sowohl die Identität des Antragstellers ausreichend geprüft wird, als auch die gesamte Auftragsbearbeitung eindeutig verantwortlichen Personen zugeordnet werden kann.

Für Zertifikate, die bloß für einfache Signaturen vorgesehen sind, erfolgt die Zustellung in einer Form in der die Kenntnisnahme durch den Empfänger als unbedenklich erscheint.

## 4. ANTRAGSARCHIVIERUNG

Der Zertifikatsantrag und alle damit im Zusammenhang stehenden vom Antragsteller zugesandten und in Papierform vorliegenden Daten und Dokumente (Ausweiskopien, ggf. Bestätigungen über das Unternehmen und die Vertretungsbefugnis) werden auf die Dauer von mind. 35 Jahren nach Ablauf der Gültigkeit elektronisch oder in Papierform in dem Umfang archiviert, dass die ursprüngliche Antragstellung, Zertifikatsausstellung und Zertifikatszustellung nachvollzogen werden können.

Die privaten Schlüssel des Signators werden, sofern sie vom Herausgeber erstellt wurden und Kopien vorhanden sind, nach Abruf durch den Signator und der Bestätigung des Signators des korrekten Empfangs durch den Signator, beim Herausgeber gelöscht.

## 5. ZERTIFIKATERSTELLUNG

Der Herausgeber erstellt Zertifikate gem. der jeweiligen Anzeige bei der Aufsichtsbehörde oder auf Grund der auf seiner Website veröffentlichten Produktbeschreibung. Insbesondere sind dies Zertifikate im X.509v3 Format oder im PGP-Format.

Die eindeutige Zuordnung des Zertifikats zum Signator ist sicher gestellt durch:

- Erstellung des PKCS#10-Requests (bei X.509v3 Zertifikaten) bzw. eines PGP-Requests (bei PGP-Zertifikaten) als Grundlage für die Zertifizierung,
- Erzeugung des Zertifikats nach Überprüfung aller Antragsdaten auf ihre Korrektheit durch eine Registrierungsstelle oder
- Erzeugung des Zertifikats nach Überprüfung aller Antragsdaten an der Zertifizierungsstelle des Herausgebers.

Die in einer Registrierungsstelle erzeugten Zertifikatsdaten werden signiert und verschlüsselt (SSL) an die Zertifizierungsstelle des Herausgebers übertragen. Vertraulichkeit und Integrität sämtlicher Daten sind sicher gestellt.

## 6. ZERTIFIKATSINHALT

Inhalt und technische Beschreibung des Zertifikats sind der jeweiligen Anzeige bzw. den Dokumentationen auf der Website des Herausgebers zu entnehmen. Bei der Verwendung von standardisierten Zertifikatsformaten (z.B. X509v3) genügt der Verweis auf die anzuwendenden Standards.

## 7. VERLÄNGERUNG DER GÜLTIGKEITSDAUER EINES ZERTIFIKATS, AUSSTELLUNG VON WEITEREN ZERTIFIKATEN UND NEUAUSSTELLUNGEN

Durch folgende Maßnahmen wird sicher gestellt, dass Anträge von Antragstellern, die anlässlich einer vorhergehenden Zertifikatsausstellung bereits registriert wurden, vollständig, korrekt und ordnungsgemäß autorisiert sind.

Die Maßnahmen gelten sowohl für die Verlängerung der Gültigkeitsdauer, für die Ausstellung weiterer gleichartiger Zertifikate, als auch für die Neuausstellung nach Ablauf oder Widerruf eines Zertifikats.

- Die Registrierungsstelle prüft die im Zertifikat enthaltenen Daten hinsichtlich ihrer aktuellen Gültigkeit.
- Änderungen in der vorliegenden Policy, in den Geschäftsbedingungen und in den sonstigen Vereinbarungen werden zur Kenntnis gebracht.

Ein bestehendes Zertifikat kann nicht verlängert werden, es ist jedoch zulässig zu einem bestehenden privaten Schlüssel bzw. zu einem bestehenden CSR ein neues Zertifikat mit neuer Laufzeit und neuen Zertifikatsangaben zu machen. Sofern das ursprüngliche Zertifikat nicht schon abgelaufen ist, ist es zu widerrufen.

# F. BEKANNTMACHUNG DER VERTRAGSBEDINGUNGEN

Der Herausgeber macht den Signatoren und den Benutzern, die auf die Zuverlässigkeit der A-CERT Dienste vertrauen, die Bedingungen, die die Benutzung des jeweiligen Zertifikats betreffen, durch Veröffentlichung folgender Dokumente auf der A-CERT Website zugänglich:

1. die gegenständliche Certificate Policy, sofern für einen Dienst erforderlich weitere in diesem Dokumenten bezeichnete Certificate Policies,
2. die Allgemeinen Betriebs- und Nutzungsbedingungen,
3. ergänzende Beschreibungen zu den einzelnen Zertifizierungsdiensten,
4. - sofern anwendbar - ein Verweis auf die Anzeige des Zertifizierungsdienstes bei der Aufsichtsbehörde,
5. durch sonstige Mitteilungen.

Änderungen werden dem Signator mittels Bekanntmachung auf der A-CERT Website und ggf. zusätzlich per e-mail oder brieflich mitgeteilt. Jedermann kann sie über die A-CERT Website abrufen.

# G. VERÖFFENTLICHUNG DER ZERTIFIKATE

Grundsätzlich werden alle von A-CERT ausgestellten Zertifikate den Signatoren und den Überprüfern folgendermaßen verfügbar gemacht:

1. Grundsätzlich werden alle Zertifikate in den Verzeichnisdienst(en) von A-CERT veröffentlicht. Die Nutzungsdetails werden auf der Website von A-CERT veröffentlicht.
2. Die Bedingungen für die Benutzung eines Zertifikats werden von A-CERT allen Beteiligten in Form der Certificate Policy zur Kenntnis gebracht.
4. Der Verzeichnisdienst ist an sieben Tagen pro Woche jeweils 24 Stunden verfügbar. Unterbrechungen von mehr als 24h werden als Störfälle dokumentiert. Diese Dokumentation ist für Aufsichts- und Auditstellen zugänglich, bei Vorhandensein berechtigter Interessen werden für einen relevanten Zeitraum die Unterlagen auch Dritten bereit gestellt.
5. Die Verzeichnisdienste sind öffentlich und international zugänglich.

Eine Aufnahme in den Verzeichnisdienst unterbleibt, wenn

- der Signator es wünscht und
- die Art des Zertifizierungsdienstes es erlaubt (wesentlich sind der Inhalt der Anzeige bei der Aufsichtsbehörde, Vorgaben durch Standards und Gesetze oder sonstige verbindliche rechtliche Vorgaben).

Auch zu den Zertifikaten die nicht im Verzeichnisdienst automatisiert veröffentlicht werden, wird Auskunft über den Inhaber erteilt, sofern der Auskunftssuchende ein berechtigtes rechtliches Interesse glaubhaft macht.

# H. WIDERRUF

Um eine möglichst praxisnahe Nutzung der Zertifikate zu gewährleisten, wird ein zweistufiges Widerrufskonzept angewandt.

Ein vorläufiger Widerruf wird sofort wirksam (auch bei mangelhafter oder unvollständiger Identitätsprüfung) und wird beim Widerrufsgrund in der Widerrufsliste mit dem entsprechenden Zusatz vermerkt. Anschließend wird der Signator über das Einlangen des Widerrufs verständigt und um Bestätigung oder Aufhebung des Widerrufsantrags ersucht.

Ein vorläufiger Widerruf wird zu einem irreversiblen Widerruf, wenn innerhalb von drei Werktagen eine Bestätigung erfolgt oder keine Aufhebung des Widerrufs verlangt wird.

Ein irreversibler Widerruf erfolgt nach vollständiger Identitätsprüfung und führt zur vorzeitigen Beendigung der Gültigkeit eines Zertifikats.

Zum Widerruf berechtigt ist der Signator. Für die Fälle, bei denen der Signator in Vertretung einer Person oder einer Organisation handelt, ist auch diese Person bzw. ein ausgewiesener Vertreter der Organisation zum Widerruf berechtigt. Weiters ist der Herausgeber berechtigt jederzeit Zertifikate gemäß den Bedingungen unter "Verpflichtungen des Herausgebers" (p11) zu widerrufen.

Ein Widerrufsantrag kann formlos unter Angabe geeigneter Zertifikatsangaben und Kennzeichen (Produktbezeichnung, Seriennummer, Fingerprint, ...) eingebracht werden. Anträge per Telefon, Fax, Post und e-mail werden während der Geschäftszeiten Mo-Fr 9-17 Uhr (werktags) entgegen genommen und bearbeitet. Widerrufe via http werden rund um die Uhr entgegen genommen und - sofern ausreichend spezifiziert - sofort automatisiert bearbeitet (ansonsten werden sie wie e-mails behandelt).

Sofern es die berechtigte widerrufende Stelle wünscht, kann sofort der irreversible Widerruf durchgeführt werden. Ebenso sind Widerrufe, bei denen Berechtigung und Identität des Widerrufenden zweifelsfrei feststeht oder die der Herausgeber veranlasst hat irreversibel.

Nach Einlangen des Widerrufantrags ist der vorläufige Widerruf binnen 1 Stunde wirksam.

Die über das Internet abrufbaren Widerrufslisten werden nach jedem Widerruf aktualisiert, spätestens jedoch nach 30 Tagen.

Die Verzeichnisdienste für Widerrufslisten sind öffentlich und international zugänglich.

Eine Veröffentlichungssperre ist bei widerrufenen Zertifikaten nicht möglich.

# I. WIDERRUFSINHALT

Der Inhalt der Widerrufsliste ist - sofern anzeigepflichtig - der Anzeige des jeweiligen Zertifizierungsdienstes bei der Aufsichtsbehörde bzw. den Dokumentationen auf der Website des Herausgebers zu entnehmen. Bei der Verwendung von standardisierten Zertifikatsformaten (z.B. X509v3) genügt der Verweis auf die anzuwendenden Standards.

Der Inhalt der Widerrufsliste entspricht bei Zertifikaten die zur Amtssignatur oder zur fortgeschrittenen Signatur geeignet sind [RFC3280].

# V. BETRIEBSORGANISATION VON A-CERT

## A. SICHERHEITSMANAGEMENT

Der Herausgeber ist für die Gestaltung und Dokumentation aller Prozesse im Rahmen der Zertifizierungsdienste verantwortlich; dies gilt auch für die an Vertragspartner ausgelagerten Dienste. Die Aufgaben und zugeordneten Verantwortlichkeiten der Vertragspartner sind klar geregelt, weiters sind Kontrollen zur Überprüfung der ordnungsgemäßen Tätigkeit eingerichtet.

Die für die Sicherheit relevanten Vorgehensweisen sind in dieser Policy veröffentlicht. Zusätzlich behält sich der Herausgeber vor spezifische Sicherheitsmaßnahmen in einer nicht öffentlichen Security Policy festzulegen.

Die Betriebsinfrastruktur des Herausgebers wird ständig überprüft und an geänderte Anforderungen angepasst. Jegliche Änderungen, die einen Einfluss auf das Ausmaß der erreichten Sicherheit haben, sind vom Vorstand des Herausgebers oder dem von ihn beauftragten Dienstleister zu genehmigen.

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

Der technische Betrieb erfolgt in den Räumen des Herausgebers oder bei entsprechend qualifizierten Vertragspartnern. Die jeweils aktuellen Vertragspartner werden der Aufsichtsbehörde bekannt gegeben und auf der Website von A-CERT veröffentlicht. Alle Vertragspartner sind an die Wahrung der Datensicherheit im Sinne dieser Policy, des DSG 2000, der Signaturbestimmungen und sonstiger zutreffender rechtlicher Bestimmungen und technischen Standards vertraglich gebunden.

Zur Steuerung des Betriebs wurden vier Sicherheitsstufen eingeführt, die zu entsprechend unterschiedlichen betrieblichen Sicherheitsmaßnahmen führen.

- Stufe public: Umfasst alle Daten, die auch zur Veröffentlichung bestimmt oder geeignet sind. Der Zugriff auf diese Daten ist herausgeberintern nicht beschränkt, es werden jedoch Maßnahmen zum Erhalt der Verfügbarkeit und der Datenintegrität ergriffen.

Alle weiteren Stufen enthalten Daten, die nicht zur Veröffentlichung geeignet sind. Der Zugriff ist jeweils auf die für die Verwendung der Daten vorgesehenen Funktionsträger beschränkt. Abstufungen ergeben sich weiters bei den Maßnahmen zum Erhalt der Verfügbarkeit und der Datenintegrität.

- Stufe administration: Umfasst alle Daten, die zur ordnungsgemäßen Betriebsführung im kaufmännischen Sinn dienen, inkl. interne Dokumentationen, Buchhaltung, Kunden- und Interessentenadministration, Angebot- und Rechnungslegung.

- Stufe systemadministration: Umfasst alle Daten, die zur Aufrechterhaltung und Weiterführung des IT-Betriebs dienen.

- Stufe security: Umfasst alle Daten, die besonderen Prozessen unterworfen sind, insbesondere sind dies die Daten die im unmittelbaren Zusammenhang mit Schlüsselerstellung und Zertifikatgenerierung stehen.

# B. ZUGRIFFSVERWALTUNG

Eine Benutzerverwaltung, die den verschiedenen Funktionen unterschiedliche Zugriffsrechte einräumt, ist eingerichtet; insbesondere werden sicherheitsrelevante von nicht sicherheitskritischen Funktionen sorgfältig getrennt. Alle mit der Zertifizierung im unmittelbaren Zusammenhang stehenden technischen Prozesse sind zugriffsgesichert und erfordern

- den Zutritt zu bestimmten, gesichert aufbewahrten Hardwarekomponenten und/oder
- die Eingabe von 1 bis 2 Passwörtern (im Falle von zwei Passwörtern sind unterschiedliche Personen zwingend erforderlich).

Die individuellen Erfordernisse jedes einzelnen Prozessschrittes sind dokumentiert.

Mittels Firewalls wird das interne Netzwerk vor Zugriffen durch Dritte geschützt.

Vertrauliche Daten werden bei Übertragung über unsichere Netzwerke durch Verschlüsselung geschützt.

Änderungen in den Zugriffsrechten werden im System unverzüglich nachgezogen. Die Kontrolle der Benutzerverwaltung ist Teil des internen Audits.

Zugriff auf Informationen und Anwendungen ist auf Grund der vergebenen Zugriffsrechte eingeschränkt. Administrative Prozesse (insbesondere Auftragsverwaltung, Abrechnung, Marketing) und den Zertifizierungsbetrieb unmittelbar betreffende Prozesse sind getrennt.

Das Personal muss sich vor jedem kritischen Zugriff auf Applikationen, die in Zusammenhang mit dem Zertifikatsmanagement stehen, authentifizieren.

Die Zugriffe werden in Log-Dateien aufgezeichnet und regelmäßig bezüglich der Rechtmäßigkeit geprüft. Das Personal wird für die ausgeführten Tätigkeiten zur Verantwortung gezogen.

Änderungen (Löschungen, Hinzufügungen) bei den Verzeichnis- und Widerrufsdiensten werden durch eine Signatur der Zertifizierungsstelle gesichert.

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

Die Systemadministratoren und sonstiges mit Zertifizierungsaufgaben betrautes Personal werden zur Einhaltung der Datensicherheitsbestimmungen gem. DSG 2000 § 14 vertraglich verpflichtet.

# C. PERSONELLE SICHERHEITSMAßNAHMEN

Die Mitarbeiter des Herausgebers sind als qualifiziertes Personal besonders geeignet, die in dieser Policy verankerten Bestimmungen umzusetzen und zu gewährleisten.

- Sicherheitsrelevante Funktionen und Verantwortlichkeiten werden in den internen Stellenbeschreibungen und im internen Rollenplan dokumentiert. Jene Funktionen, von denen die Sicherheit der Zertifizierungsdienste abhängt, sind eindeutig identifiziert.
- Für die Mitarbeiter des Herausgebers sind klare Stellenbeschreibungen ausgearbeitet, in denen die Pflichten, Zugriffsrechte und Kompetenzen dargelegt sind.
- Alle Leitungsfunktionen sind mit Personen besetzt, die über Erfahrung mit der Technologie elektronischer Signaturen und Verschlüsselungen und mit der Führung von Personal, das Verantwortung für sicherheitskritische Tätigkeiten trägt, verfügen.
- Entsprechend § 10 Abs 4 [SigV] beschäftigt der Herausgeber keine Personen, die strafbare Handlungen begangen haben, welche sie für eine vertrauenswürdige Position ungeeignet erscheinen lassen.

# D. PHYSIKALISCHE UND ORGANISATORISCHE SICHERHEITSMAßNAHMEN

Es ist sicher gestellt, dass der Zutritt zu Räumlichkeiten, in denen sicherheitskritische Funktionen ausgeübt werden, beschränkt ist und die Risken einer physischen Beschädigung von Anlagen minimiert sind.

Insbesondere gilt:

1. Der Zugriff zu den Geräten, in denen Zertifizierungs- und Widerrufsdienste erbracht werden, ist auf autorisiertes Personal beschränkt. Die Systeme, welche Zertifikate ausstellen, sind vor Gefährdung durch Umweltkatastrophen baulich geschützt.

2. Es werden Maßnahmen ergriffen, um den Verlust, die Beschädigung oder die Kompromittierung von Anlagen und die Unterbrechung des Betriebes zu verhindern.
3. Weitere Maßnahmen gewährleisten, dass eine Kompromittierung oder ein Diebstahl von Daten und Daten verarbeitenden Anlagen nicht möglich ist.
4. Die Systeme für die Zertifikatsgenerierung und die Widerrufsdienste werden durch technische und organisatorische Maßnahmen in einer gesicherten Umgebung betrieben, sodass eine Kompromittierung durch unautorisierte Zugriffe nicht möglich ist.
5. Die Abgrenzung der Systeme für Zertifikatsgenerierung und Widerrufsdienste erfolgt durch klar definierte Sicherheitszonen, d. h. durch räumliche Trennung von anderen organisatorischen Einheiten sowie physischen Zutrittsschutz.
6. Die Sicherheitsmaßnahmen beinhalten den Gebäudeschutz, die Computersysteme selbst und alle sonstigen Einrichtungen, die für deren Betrieb unerlässlich sind. Der Schutz der Einrichtungen für die Zertifikatserstellung und Bereitstellung der Widerrufsdienste umfasst physische Zutrittskontrolle, Abwendung von Gefahren durch Naturgewalten, Feuer, Rohrbrüche und Gebäudeeinstürze, Schutz vor Ausfall von Versorgungseinheiten sowie vor Diebstahl, Einbruch und Systemausfällen.
7. Die unautorisierte Entnahme von Informationen, Datenträgern, Software und Einrichtungsgegenständen, welche zu den Zertifizierungsdiensten gehören, wird durch Kontrollmaßnahmen verhindert.

# E. LAUFENDE BETRIEBLICHE MAßNAHMEN

1. Schäden durch sicherheitskritische Zwischenfälle und Fehlfunktionen werden durch entsprechende Aufzeichnungen und Fehlerbehebungsprozeduren frühzeitig erkannt, verhindert oder zumindest minimiert.
2. Datenträger werden vor Beschädigung, Diebstahl und unautorisiertem Zugriff geschützt.
3. Für die Ausführung von sicherheitskritischen und administrativen Aufgaben, die sich auf die Erbringung der Zertifizierungsdienste auswirken, sind detaillierte Prozesse in Verwendung.
4. Datenträger werden je nach ihrer Sicherheitsstufe behandelt und aufbewahrt. Nicht mehr benötigte Datenträger, die vertrauliche Daten beinhalten, werden in sicherer Weise vernichtet.
5. Die Integrität der Computersysteme und Informationen ist gegen Viren und böswillige oder unautorisierte Software geschützt.
6. Kapazitätserfordernisse werden beobachtet und künftige Entwicklungen prognostiziert, sodass stets angemessene Bandbreiten, Prozessorleistungen und sonstige IT-Ressourcen zur Verfügung stehen.
7. Die sicherheitskritischen Funktionen im Rahmen der Zertifizierungs- und Widerrufsdienste werden von den gewöhnlichen administrativen Funktionen strikt getrennt. Als

sicherheitskritische Funktionen werden alle IT-Maßnahmen angesehen, die zur Erhaltung der Betriebsfähigkeit des Zertifizierungsdienstes dienen. Insbesondere sind dies
- Planung und Abnahme von Sicherheitssystemen,
- Schutz vor böswilliger Software und Angriffen,
- Aktive Überprüfung von Log-Files und Prüfberichten, Analyse von Zwischenfällen,
- Allgemeine System-Wartungstätigkeiten,
- Netzwerkadministration,
- Datenmanagement, Datenträgerverwaltung und –sicherheit,
- Softwareupdates.

Die Überwachung der sicherheitskritischen Funktionen obliegt unmittelbar einem vom Vorstand des Herausgebers oder vom verantwortlichen Dienstleister nominierten Sicherheitsbeauftragten.

# F. SYSTEMENTWICKLUNG

Die Systementwicklung erfolgt in vom Echtbetrieb getrennten Entwicklungssystemen.

Die für die Zertifizierungsdienste notwendigen Prozesse werden laufend weiterentwickelt und optimiert. Neben einer Optimierung der Sicherheit bestimmt auch die Verbesserung der Kundenfreundlichkeit die Systementwicklung.

Die in Betrieb befindlichen Softwaremodule werden elektronisch signiert. Die Signaturen werden laufend geprüft, unerwünschte Änderungen können sofort erkannt werden.

Zur Installation neuer Softwaremodule existieren Übergabeverfahren.

# G. ERHALTUNG DES UNGESTÖRTEN BETRIEBES UND BEHANDLUNG VON ZWISCHENFÄLLEN

Gegen physikalische Störungen bestehen technische, bauliche und organisatorische Sicherungsmaßnahmen wie redundante Systemführungen, Notstromaggregate, Brandschutz. Diese ermöglichen auch unter der Annahme der vollständigen Zerstörung der Primäreinrichtung eine Wiederaufnahme innerhalb eines Werktages.

Als Katastrophenszenario ("worst case") wird die Kompromittierung eines Zertifizierungsschlüssels angesehen. Für diesen Fall wird der Herausgeber die Aufsichtsstelle (gem. § 6 Abs 5 [SigG]), die Signatoren, die auf die Verlässlichkeit der Zertifizierungsdienste vertrauenden Personen und ggf. andere Zertifizierungsdiensteanbieter, mit denen Vereinbarungen bestehen, davon unterrichten und mitteilen, dass die Widerrufs- und Zertifikatsinformationen nicht mehr als zuverlässig anzusehen sind.

Zertifikate und Widerrufslisten werden als nicht mehr gültig gekennzeichnet. Den Signatoren werden mit Hilfe eines neu generierten sicheren Zertifizierungsschlüssels neue Zertifikate ausgestellt.

# VI. SONSTIGES

## A. KOSTEN UND KONDITIONEN

Die jeweils gültigen Kosten und Konditionen werden auf der A-CERT Website publiziert (http://www.a-cert.at/).

## B. EINSTELLUNG DER TÄTIGKEIT

Gem. § 12 SigG wird der Herausgeber die Einstellung der Tätigkeit - sofern vorgesehen - unverzüglich der Aufsichtsstelle anzeigen und sicher stellen, dass eine eventuelle Beeinträchtigung ihrer Dienstleistungen sowohl gegenüber Signatoren als auch gegenüber allen auf die Zuverlässigkeit der Dienste vertrauenden Parteien möglichst gering gehalten wird.

## C. INFORMATION GEM. DSG 2000

Alle im Rahmen der Zertifizierungsdienste erhaltenen Informationen werden grundsätzlich vertraulich behandelt und nur für Zwecke des Zertifizierungsdienstes und für Verständigungszwecke im Zusammenhang mit den Zertifizierungsdienstleistungen des Herausgebers verwendet.

Veröffentlicht werden Daten des Signators ausschließlich auf Grund der Erfordernisse des jeweiligen Zertifizierungsdienstes (Verzeichnisdienst, Widerrufsdienst) oder auf ausdrücklichen Wunsch des Signators.

Gesetzliche Aufbewahrungs- und Übermittlungsverpflichtungen bleiben unberührt. Eine Datenweitergabe gem. § 151 GewO an Adressenverlage wird ausdrücklich ausgeschlossen.

# ANHANG

## ANHANG A: LITERATURLISTE

Sofern nicht anders vermerkt gelten bei den angeführten Dokumenten die zum Zeitpunkt der Inbetriebnahme des Dienstes bzw. Genehmigung durch die Aufsichtsstelle jeweils aktuelle Fassung.

[ASZ] Karlinger G., Amtssignaturzertifikate (ASZ) - Allgemeine Richtlinien für Amtssignaturzertifikate in der Verwaltung, Version 1.0.0, 2005-04-06

[DSG 2000] Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000) idgF, StF BGBl. I Nr. 165/1999

[E-GOVG] Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz - E-GovG) - StF BGBl. I Nr. 10/2004

[ETSI SR 002 176] ETSI SR 002 176 V1.1.1 Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures

[ETSI TS 102 158] ETSI TS 102 158 V1.1.1 (2003-10) - Electronic Signatures and Infrastructures (ESI); Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates

[ETSI TS 101 862] ETSI TS 101 862 v1.3.3 Qualified Certificate profile

[ETSI TS 102 042] ETSI TS 102 042 V1.1.1 (2002-04) Policy requirements for certification authorities issuing public key certificates

[ETSI TS 101 456] ETSI TS 101 456 V1.4.3 (2007-05) Technical Specification - Policy requirements for certification authorities issuing qualified certificates inkl. den Vorgängerversionen

[FIPS-140-2] FIPS PUB 140-2 - SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES inkl. Annex A-D

[ITU-X509v3] ITU-T Recommendation X.509v3 - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks

[ITU-X509v3-ERR] ITU-T Recommendation X.509v3 Fehlerbehebung

[ITU-X.680] ITU-T Recommendation X.680 (1997), ISO/IEC 8824-1: 1998, Information Technology – Abstract Syntax Notation One (ASN.1), Specification of Basic Notation

[ITU-X.690] ITU-T Recommendation X.690 (1997), ISO/IEC 8825-1: 1998, Information Technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)

[OID] Hollosi A.: Object Identifier der öffentlichen Verwaltung, OID 1.0.4, 2005-02-21

[POS] RTR GmbH, Positionspapier zu § 2 Z 3 lit. a bis d SigG („fortgeschrittene elektronische Signatur“), Version 1.0, 2004-04-13

[RFC2560] rfc2560 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP, Juni 1999

[RFC3161] rfc3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

[RFC3279] rfc3279 - Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[RFC3647] rfc3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003

[RFC5280] rfc5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[SigG] Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG) idgF, StF BGBl. I Nr. 190/1999

[SigRL] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, 13.12.1999

[SigVO] BGBl. II Nr. 3/2008 (StF) idgF - Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung 2008 – SigV 2008)

[X509ext] Hollosi A., X.509 Zertifikatserweiterungen für die Verwaltung, X509ext - 1.0.3, 2005-02-21

[VKZ] Verwaltungskennzeichen (VKZ) 1.2.0 Kennzeichen für Organisationseinheiten von Gebietskörperschaften bzw. Körperschaften öffentlichen Rechts, 2007-03-25

# ANHANG B: DOKUMENTENINFORMATION

Die historischen Policies sind unter http://www.a-cert.at/static und dem angegebenen Dokumentennamen abrufbar.

Die Gültigkeit der jeweiligen Dokumente ergibt sich aus dem Beginndatum der Gültigkeit und dem Beginndatum der Gültigkeit des nächstfolgenden Dokuments. Sofern nicht anders vermerkt endet die Gültigkeit des alten Dokuments am Vortag der Gültigkeit des neuen Dokuments.

## *AUTOR(EN) UND GÜLTIGKEITSHISTORIE:*

bis 7.7.2009: Gültigkeitshistorie OID 1.2.40.0.24.1.1.1.99
ab 7.7.2009: Gültigkeitshistorie OID 1.2.40.0.24.1.1.1.99 + 1.2.40.0.24.1.1.5.99 + 1.2.40.0.24.1.1.9.99

| Name | Version | Bearbeitung gültig ab | Datei | Kommentar |
|---|---|---|---|---|
| | 0 | 0 | dokumentation-argedaten.dot | interne Dokumentenvorlage, Online nicht verfügbar |
| Hans G. Zeger | 1.1 | 13.09.2004 nicht freigegeben | a-cert-certificate-policy.20040913.pdf | interne Stammfassung, Online nicht verfügbar |
| Hans G. Zeger | 1.2 | 22.09.2004 nicht freigegeben | a-cert-certificate-policy.20040922.pdf | Ergänzungen, Online nicht verfügbar |
| Hans G. Zeger | 1.3 | 04.10.2004 04.10.2004 | a-cert-certificate-policy.20041004.pdf | Ergänzungen |
| Hans G. Zeger | 1.4 | 30.08.2005 10.12.2005 | a-cert-certificate-policy.20050830.pdf | Änderungen |
| Charlotte Schönherr | 1.4.eng | 13.03.2007 nicht freigegeben | a-cert-certificate-policy-english.20070313.pdf | official english translation of policy v1.4, not adopted |
| Daniel Weller | 1.5 | 12.04.2007 04.06.2007 | a-cert-certificate-policy.20070412.pdf | Änderungen lt. I. Änderungsdokumentation |
| Charlotte Schönherr | 1.5.eng | 04.06.2007 04.06.2007 | a-cert-certificate-policy-english.20070604.pdf | official english translation of policy v1.5 |
| **Hans G. Zeger** | **1.6** | **07.07.2009 07.07.2009** | **a-cert-certificate-policy.pdf** | **Änderungen lt. I. Änderungsdokumentation Änderungen 7. Juli 2009** |
| **Charlotte Schönherr** | **1.6.eng** | **07.07.2009 07.07.2009** | **a-cert-certificate-policy-english.pdf** | **official english translation of policy v1.6** |