

A-CERT Certificate Policy

[gültig für A-CERT GOVERNMENT Zertifikate für
gewöhnliche und fortgeschrittene Signaturen]

Version 1.2/Oktober 05 - a-cert-government-policy.051019.doc
OID-Nummer: 1.2.40.0.24.1.1.3.1

© ARGE DATEN - Österreichische Gesellschaft für Datenschutz 2005

INHALT:

Inhalt:.....	2
I. Grundlagen	4
A. Motivation	4
B. Definitionen und Kurzbezeichnungen	4
C. Überblick	5
D. Anwendungsbereich.....	5
II. Verpflichtungen und Haftungsbestimmungen	6
A. Verpflichtungen des Herausgebers	6
B. Verpflichtungen des Signators.....	6
C. Verpflichtungen des Empfängers von Zertifikaten	8
D. Haftung.....	8
III. Spezifikationen zur Erbringung von Zertifizierungsdiensten	9
A. Allgemeines.....	9
B. Operative Maßnahmen zur Bereitstellung des Zertifizierungsdienstes	9
C. Schlüsselverwaltung	9
1. Erzeugung der CA Schlüssel	9
2. Speicherung der CA Schlüssel	10
3. Verteilung der öffentlichen CA Schlüssel	10
4. Schlüsseloffenlegung	10
5. Verwendungszweck von CA Schlüsseln.....	10
6. Ende der Gültigkeitsperiode von CA Schlüsseln	10
7. Erzeugung der Schlüssel für die Signatoren	10
D. Zertifikate der Antragsteller.....	11
1. Antragstellung	11
2. Antragsprüfung	12
3. Zertifikaterstellung	13
4. Zertifikatsinhalt	13
5. Antragsbearbeitung	14
6. Antragsarchivierung.....	14
7. Ausstellung von weiteren Zertifikaten und Neuausstellungen	14
E. Bekanntmachung der Vertragsbedingungen	15
F. Veröffentlichung der Zertifikate	15
G. Widerruf.....	16
1. Widerruf durch den Signator	16
2. Widerruf durch die Organisation	16

3. Abwicklung	16
H. Widerrufsinhalt	17
IV. A-CERT Betriebsorganisation	17
A. Sicherheitsmanagement	17
B. Zugriffsverwaltung	18
C. Personelle Sicherheitsmaßnahmen	19
D. Physikalische und organisatorische Sicherheitsmaßnahmen	19
E. Laufende betriebliche Maßnahmen	20
F. Systementwicklung	21
G. Erhaltung des ungestörten Betriebes und Behandlung von Zwischenfällen	21
V. Sonstiges	21
A. Kosten und Konditionen	21
B. Einstellung der Tätigkeit	22
C. Information gem. DSG 2000	22
Anhang	23

ANHANG:

Anhang A: Literaturliste.....	23
Anhang B: Dokumenteninformation	24

I. GRUNDLAGEN

A. MOTIVATION

Diese Policy beschreibt die Umsetzung der "Allgemeinen Richtlinien für Amtssignaturzertifikate in der Verwaltung" [ASZ] durch das Zertifizierungsdienstangebot A-CERT GOVERNMENT.

B. DEFINITIONEN UND KURZBEZEICHNUNGEN

Herausgeber

Herausgeber dieser Certificate Policy ist die ARGE DATEN - Österreichische Gesellschaft für Datenschutz

A-CERT

Ist der Sammelbegriff für alle Zertifizierungsdienste des Herausgebers. Unterschiedliche Zertifizierungsdienste werden mit Zusätzen zu A-CERT gekennzeichnet.

A-CERT GOVERNMENT

Kennzeichnet alle Zertifikate die im Rahmen dieser Policy ausgestellt wurden. Die Zertifikate enthalten als CN-Bezeichnung des Herausgebers (Issuer) den Vermerk 'A-CERT GOVERNMENT'

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 GOVERNMENT gültige Policy wird im vorliegenden Dokument beschrieben und hat die OID-Nummer 1.2.40.0.24.1.1.3.1. Historische Versionen des Dokuments sind bei der Aufsichtsstelle abzurufen oder unter der OID-Nummer 1.2.40.0.24.1.1.3.99 abgelegt.

Testzertifikate

Bezeichnet Zertifikate, die auf Basis des X.509-Standards zu Testzwecken an Dritte ausgestellt werden. Eine Identitätsprüfung der Antragsteller (Signatoren) findet nicht statt. Testzertifikate sind erkennbar, wenn zumindest eine der Bedingungen erfüllt ist:

- die CN-Bezeichnung des Herausgebers (Issuer) lautet **A-CERT GOVERNMENT TEST**,
- das Zertifikat enthält das zusätzliche X.509v3-Attribut **1.2.40.0.24.4.1.0=DER:01:01:FF** (Testeigenschaft = TRUE).

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 gemäß den Bestimmungen zum Verwaltungskennzeichen [VKZ] und der Amtssignaturzertifikate [ASZ] einen Antrag auf die Ausstellung eines Amtssignaturzertifikats stellt, wird im Folgenden als Antragsteller bezeichnet.

Registrierungsstelle

Die Geschäftsstellen des Herausgebers und weitere vom Herausgeber autorisierte Stellen und Personen zur Entgegennahme und Prüfung von Zertifizierungsanträgen.

Signaturbestimmungen

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

Aufsichtsbehörde

Die für die A-CERT Zertifizierungsdienste zuständige Aufsichtsbehörde.

Ansonsten werden die Begriffe gemäß SigG, SigV, SigRL, gem. X.509, X.680, X.690 und [X509ext] und den RFCs 3647 und 3280 verwendet.

C. ÜBERBLICK

Die vorliegende Certificate Policy enthält alle Regeln für die Ausstellung und Verwendung von Zertifikaten für gewöhnliche und fortgeschrittene Signaturen. Die Zertifikate entsprechen der Definition §2 Abs. 8 [SigG].

Diese Policy wurde in Übereinstimmung mit den Signaturbestimmungen verfasst und bildet gemeinsam mit den "A-CERT Allgemeine Betriebs- und Nutzungsbedingungen" und der 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 Internet-Seite von A-CERT.

D. ANWENDUNGSBEREICH

Diese A-CERT Certificate Policy gilt für alle Zertifikate, die für gewöhnliche und fortgeschrittene Signaturen im Rahmen des Dienstes A-CERT GOVERNMENT 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 sind auch zur Erstellung von Signaturen im Sinne des §2 Z3 lit. a bis d [SigG] geeignet.

II. VERPFLICHTUNGEN UND HAFTUNGSBESTIMMUNGEN

A. VERPFLICHTUNGEN DES HERAUSGEBERS

Der Herausgeber verpflichtet sich sicherzustellen, dass alle Anforderungen, die im Abschnitt III dargelegt sind, erfüllt werden.

Der Herausgeber ist verantwortlich für die Einhaltung aller Richtlinien, die in der gegenständlichen Policy beschrieben sind; dies gilt auch für jene Funktionen, deren Ausführung an Vertragspartner ausgegliedert wurde (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 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 Homepage 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 Generierung und 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),
3. zur Generierung 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 Homepage 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.

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 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 die Einhaltung dieser Policy, insbesondere für die darin festgelegten Maßnahmen zur prompten Veröffentlichung von Widerruflisten und die Einhaltung der in der Policy genannten Widerruf-Standards (ITU X.509v2)
- 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 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.

Der Herausgeber haftet nicht, falls er nachweisen kann, dass ihn an der Verletzung der oben angeführten Verpflichtungen keine Schuld trifft.

III. SPEZIFIKATIONEN ZUR ERBRINGUNG VON ZERTIFIZIERUNGSDIENSTEN

A. ALLGEMEINES

Im Rahmen dieser Policy werden folgende (Teil-)Dienste spezifiziert: Bereitstellung von Registrierungsdiensten, Zertifikatsgenerierung, Zertifikatsausgabe, Widerrufsdiensten und Abfragediensten 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 Webseite 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 Herausgebers entscheidet auch, an welchem Ort die Zertifizierungen stattzufinden haben.
5. Über die Webseite bzw. sofern bei den Zertifikatsinhabern verfügbar per eMail wird zeitgerecht über Änderungen informiert, die im Certification Practice Statement vorgenommen werden. Die aktuelle Version ist jeweils online abrufbar.

C. SCHLÜSSELVERWALTUNG

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.

Die verwendeten Algorithmen und Schlüssellängen werden in den jeweiligen Anzeigen an die Telekom-Control-Kommission zu den einzelnen Diensten angegeben.

2. SPEICHERUNG DER CA SCHLÜSSEL

Der Schlüssel bleibt im für die Durchführung der Zertifizierung vorgesehenen System gespeichert. Eine Sicherungskopie wird extern in einem Tresor verwahrt. Die für die Verwendung des Schlüssels benötigten Passwortteile werden von je zwei Personen getrennt verwahrt.

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 Request
- durch Ausstellung und Veröffentlichung eines selbst signierten Root-Zertifikats.

Das Zertifikat des CA Schlüssels wird den Signatoren durch Veröffentlichung im Rahmen des Verzeichnisdienstes zugänglich gemacht. Der Herausgeber gewährleistet die Authentizität dieses Zertifikats.

4. SCHLÜSSELOFFENLEGUNG

Der geheime Schlüssel 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. Die Zertifikate über die Schlüssel der Zertifizierungsstelle werden alle sieben Jahre erneuert.

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.

7. ERZEUGUNG DER SCHLÜSSEL FÜR DIE SIGNATOREN

Die Schlüssel der Signatoren 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.

D. 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 wird entweder durch Vorlage einer gerichtlich oder notariell beglaubigten Urkunde oder durch schriftliche Bestätigung durch einen autorisierten Mitarbeiter des Herausgebers 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 Webseite des Herausgebers oder der Vertriebspartner zugänglich.
3. Der Zertifikatsantrag enthält folgende Mindestangaben: den vollständigen Namen des Signators, sein Geburtsdatum, Rückrufnummer, Name der Organisation, an der der Signator tätig ist.
4. Zusätzliche Angaben zur Person des Signators: Telefonnummer, Faxnummer und eMailadresse, Berufs- und Qualifikationsangaben, allenfalls weitere Kontaktdaten. Diese zusätzlichen Angaben sind optional. Weiters ist die Angabe der Nummer eines amtlichen Personaldokuments und 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 im Sinne des [VKZ]:
Name und Anschrift der Organisation und Organisationsform (z.B. per Gesetz eingerichtet, ...), Organisationseinheit, Verwaltungskennzeichen. Weiters ist zumindest eine Stelle

anzugeben, die als Bestätigungsstelle für diese Organisation geeignet ist (z.B. Datenverarbeitungsregister, ...) 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. Alternativ kann jene Gesetzesstelle, die Grundlage für diese Organisation ist, angegeben werden. Zur Prüfung der Adressangaben der Organisation werden das amtliche Telefonbuch oder der Amtskalender herangezogen.

6. Kenntnisnahme und Zustimmung zu den Allgemeinen Betriebs- und Nutzungsbedingungen (AGB's) des Herausgebers, zur vorliegenden Policy und gegebenenfalls zu weiteren zertifizierungsabhängigen Vereinbarungen.
7. 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 Registrierungsstelle nimmt die folgenden Überprüfungen des Antrags vor:

- Prüfung der Organisation (lt. Auskunft der Bestätigungsstelle, oder anhand von Datenbanken oder Eintragungen vertrauenswürdiger Dritter, wie dem amtlichen Telefonbuch oder dem Amtskalender). Im Zuge dieser Prüfung wird auch die Identität der angegebenen Telefonnummer mit den Angaben des amtlichen Telefonverzeichnisses geprüft.
- Prüfung durch Rückruf bei der angegebenen Organisation, ob der Antragsteller bei dieser Organisation beschäftigt ist und ob für den Zertifikatswerber ein Amtssignaturzertifikat beantragt wurde.

Diese Prüfung entfällt, wenn mit der angegebenen Organisation eine eigene Rahmenvereinbarung abgeschlossen wurde. Dieser Vertrag regelt detailliert die Antragstellung durch die Behörde selbst, insbesondere wird in diesem Zuge einem vertretungsbefugten Mitarbeiter ein passwortgesicherter Zugang zur A-CERT GOVERNMENT-Administration eingeräumt und Anträge auf ein Amtssignaturzertifikat werden mit Hilfe dieses Zugangs abgegeben. Diese Prüfung entfällt auch, wenn der Antragsteller bei der Registrierungsstelle persönlich erscheint und

- (a) sich durch Vorlage eines Amtsausweises jener Organisation legitimiert, für die er ein Amtssignaturzertifikat beantragt oder
- (b) eine amtlichen Bestätigung der Zugehörigkeit zur Organisation für die er ein Amtssignaturzertifikat beantragt im Original vorlegt

- die Identitätsprüfung ist abgeschlossen, sofern der Antrag persönlich in einer der Registrierungsstellen erfolgte und 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).

Zusätzliche Prüfungen werden ausdrücklich vorbehalten und können erforderlich sein, wenn

- die Auskünfte der Bestätigungsstellen ungenügend sind,
- Zweifel in der Verfügungsberechtigung über bestimmte Nummern- oder Namens Elemente bestehen (etwa Domainnamen),
- die Vertretungsbefugnis nicht ausreichend umschrieben bzw. dokumentiert ist,
- bei sonstigen Widersprüchen im Zertifizierungsantrag.

3. ZERTIFIKATERSTELLUNG

Der Herausgeber erstellt Zertifikate im X.509v3 Format.

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

- Erstellung des PKCS#10-Requests (bei X.509v3 Zertifikaten) als Grundlage für die Zertifizierung,
- Erzeugung des Zertifikats nach Überprüfung aller Antragsdaten auf ihre Korrektheit durch die Registrierungsstelle.

Die in der Registrierungsstelle aufgenommenen Daten werden signiert und verschlüsselt (SSL) an die Zertifizierungsstelle übertragen. Vertraulichkeit und Integrität sämtlicher Daten sind sicher gestellt.

Zertifikate die zu Testzwecken ausgestellt wurden erhalten die X.509-Erweiterung "Zertifikat nur für Testzwecke vorgesehen" 1.2.40.0.24.4.1.0=TRUE

4. ZERTIFIKATSINHALT

Das Feld Subject des Zertifikats benennt im CN den Namen des Antragstellers sowie in O (Organisationsbezeichnung) bzw. OU (Abteilung/Dienststelle) die Behörde, für die der Antragsteller als Organwalter tätig ist.

Das Zertifikat trägt die Zertifikatserweiterung Verwaltungseigenschaft gemäß [X509ext].

Das Zertifikat enthält die für eine automatische Bildung der Zertifikatskette sowie für die automatische Widerrufsprüfung nötigen Zertifikatserweiterungen (Authority Information Access, CRL Distribution Point).

Das Zertifikat enthält die Zertifikatserweiterung Certification Policies, in der auf die angewendete Policy verwiesen wird.

5. 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

- als gewöhnliche Post, sofern die Identitätsprüfung im Rahmen der Antragstellung abgeschlossen wurde,
- als "eingeschrieben, eigenhändig mit Rückschein" versehene Post, sofern die Identitätsprüfung noch nicht vollständig abgeschlossen wurde.

Das Poststück, das "eingeschrieben, eigenhändig mit Rückschein" zugestellt wurde, darf gemäß Zustellbestimmungen der Post nur dem Adressaten persönlich ausgefolgt werden. Der Empfang wird mit einer posteigenen Rücksendekarte mit Unterschrift des Adressaten bestätigt.

In jedem Fall hat der Empfänger per Fax den Empfang der Zertifizierungsbestätigung mit seiner Unterschrift zu bestätigen.

Nach Erhalt der vom Empfänger unterfertigten Bestätigung wird der Zugang zu Zertifikat und/oder privatem Schlüssel freigeschaltet. Der Abruf dieser Informationen ist nur mit Hilfe des vom Antragsteller selbst vergebenen Aktivierungspassworts und der in der Zertifikatsbestätigung genannten Referenznummer möglich.

Auf Grund dieser Maßnahmen ist einerseits sichergestellt, dass sowohl die Identität des Antragstellers ausreichend geprüft wird, andererseits auch die gesamte Auftragsbearbeitung eindeutig einer Person zugeordnet werden kann.

6. 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 archiviert.

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

7. AUSSTELLUNG VON WEITEREN ZERTIFIKATEN UND NEUAUSSTELLUNGEN

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

- 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.

E. 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 Homepage zugänglich:

1. die gegenständliche Certificate Policy,
2. die Allgemeinen Betriebs- und Nutzungsbedingungen,
3. ergänzende Beschreibungen zu den einzelnen Zertifizierungsdiensten,
4. ein Verweis auf die Anzeige des Zertifizierungsdienstes bei der Aufsichtsbehörde,
5. sonstige Mitteilungen.

Änderungen werden dem Signator mittels Bekanntmachung auf der A-CERT Homepage und ggf. zusätzlich per e-mail oder brieflich mitgeteilt. Sie sind von jedermann über die A-CERT Homepage abrufbar.

F. VERÖFFENTLICHUNG DER ZERTIFIKATE

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

1. Alle Zertifikate werden in den Verzeichnisdienst(en) von A-CERT veröffentlicht.
2. Die Bedingungen für die Benutzung eines Zertifikats werden von A-CERT allen Beteiligten in Form dieser 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.
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 ist der Inhalt der Anzeige bei der Aufsichtsbehörde).

Derartige Zertifikate werden als "gesperrt" bezeichnet.

Auch zu den "gesperrten" Zertifikaten wird Auskunft erteilt, sofern der Auskunftssuchende ein rechtliches Interesse glaubhaft macht.

Die Aufnahme des Betriebs des Verzeichnisdienstes wird gesondert angekündigt.

G. WIDERRUF

Zum Widerruf berechtigt ist der Signator oder die Organisation, in dessen Namen der Signator tätig ist

1. *WIDERRUF DURCH DEN SIGNATOR*

Der Widerruf wird durchgeführt, wenn der Wille des Signators zweifelsfrei feststeht. Dies erfolgt durch Antragstellung durch den Signator.

Um möglichst hohe Praxistauglichkeit zu erzielen, kann ein Widerrufsanspruch formlos unter Angabe geeigneter Zertifikatsangaben und Kennzeichen (Produktbezeichnung, Seriennummer, Fingerprint, ...) eingebracht werden.

Anträge werden über alle Kontaktmöglichkeiten (Telefon, Fax, Post und eMail) entgegen genommen. Sofern die Standardnummern und -adressen gewählt werden, werden Widerrufe während der Geschäftszeiten Mo-Fr 9-17 Uhr (werktags) entgegen genommen und bearbeitet. Widerrufe die außerhalb dieser Zeiten abgegeben werden, gelten mit Beginn des nächsten Werktags als eingelangt. Zertifikatinhabern wird darüber hinaus eine eigene Telefonnummer genannt, die Widerrufe auch außerhalb der Bürozeiten ermöglicht.

Der Widerrufswunsch wird unverzüglich durch Rückfrage beim Signator geprüft, er gilt erst nach Bestätigung als eingelangt.

2. *WIDERRUF DURCH DIE ORGANISATION*

Widerrufe durch die Organisation erfordern die Schriftform und haben neben den Angaben des Signators auch die Unterschrift einer für die Organisation approbationsbefugten Person zu enthalten.

Das Schreiben kann per Post oder Fax zugestellt werden.

3. *ABWICKLUNG*

Nach Einlangen des Widerrufsanspruchs ist der Widerruf binnen 24 Stunden wirksam.

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

Die Verzeichnisdienste für Widerrufslisten sind öffentlich und international zugänglich.

Eine Veröffentlichungssperre ist bei widerrufenen Zertifikaten nicht möglich.

Über den Widerruf werden Signator und Organisation per eMail, Fax oder Post verständigt.

H. WIDERRUFSINHALT

Der Inhalt der Widerrufsliste entspricht [RFC3280].

IV. A-CERT BETRIEBSORGANISATION

A. SICHERHEITSMANAGEMENT

Der Herausgeber ist für alle Prozesse im Rahmen der Zertifizierungsdienste verantwortlich; dies gilt auch für die an Vertragspartner ausgelagerten Dienste. Die Verantwortlichkeiten der Vertragspartner sind klar geregelt, weiters sind Kontrollen zur Überprüfung der ordnungsgemäßen Tätigkeit eingerichtet. Die für die Sicherheit relevanten Vorgehensweisen sind in dieser Policy veröffentlicht.

Die Betriebsinfrastruktur von A-CERT 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 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 Webseite von A-CERT veröffentlicht. Alle Vertragspartner sind an die Wahrung der Datensicherheit im Sinne dieser Policy, des DSG 2000 und der Signaturbestimmungen 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 Zertifizierung 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.

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 sofort nachgezogen. Die Kontrolle der Benutzerverwaltung ist Teil des internen Audits.

Zugriff auf Informationen und Anwendungen ist auf Grund der vergebenen Zugriffsrechte eingeschränkt. Administrative und den Betrieb 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. 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 unauthorisierten Zugriffs auf Verzeichnis- und Widerrufsdienste werden aufgezeichnet.

Die Systemadministratoren und sonstiges Personal sind zur Einhaltung der Datensicherheitsbestimmungen gem. DSG 2000 §14 verpflichtet.

C. PERSONELLE SICHERHEITSMABNAHMEN

Die Mitarbeiter von A-CERT sind als qualifiziertes Personal besonders geeignet, die in dieser Policy verankerten Bestimmungen umzusetzen und zu gewährleisten.

- Sicherheitsrelevante Funktionen und Verantwortlichkeiten werden in den jeweiligen Stellenbeschreibungen dokumentiert. Jene Funktionen, von denen die Sicherheit der Zertifizierungsdienste abhängt, sind eindeutig identifiziert.
- Für die Mitarbeiter bei A-CERT 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 digitaler 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 SICHERHEITSMABNAHMEN

Es ist sicher gestellt, dass der Zutritt zu Räumlichkeiten, in welchen sicherheitskritische Funktionen ausgeübt werden, beschränkt ist und die Risiken 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 nominierten Sicherheitsbeauftragten.

F. SYSTEMENTWICKLUNG

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

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.

V. SONSTIGES

A. KOSTEN UND KUNDENKONDITIONEN

Die jeweils gültigen Kosten und Konditionen werden auf der Webseite A-CERT publiziert (<http://www.a-cert.at/a-cert-government.html>).

B. EINSTELLUNG DER TÄTIGKEIT

Gem. § 12 SigG wird der Herausgeber die Einstellung der Tätigkeit 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. DSGVO 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

[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). BGBl. I Nr. 165/1999

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

[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, 13.4.2004

[RFC3280] RFC 3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002

[RFC3647] RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003

[SigG] Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG). 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

[SigV] Verordnung zum Signaturgesetz, BGBl II 2000/30, 2.2.2000, idF: BGBl. II Nr. 527/2004

[X.509] ITU-T Recommendation X.509, März 2000

[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

[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)

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

[VKZ] Grandits F., Hörbe R., Wiesner H.: Kennzeichen für Organisationseinheiten von Gebietskörperschaften bzw. Körperschaften öffentlichen Rechts (Verwaltungskennzeichen), VKZ 1.1.0, 2003-05-15

ANHANG B: DOKUMENTENINFORMATION

AUTOR(EN):

Name	Version	Bearbeitung	Datei	Kommentar
	0	0	dokumentation-argedaten.dot	Quelle
Hans G. Zeger	1.1	07.09.05 13:18	a-cert-government-policy.050907.doc	Stammfassung
Hans G. Zeger	1.2	19.10.05 13:00	a-cert-government-policy.051019.doc	Endfassung