Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie
Technische Universität Graz
Inffeldgasse 16a, A-8010 Graz
Tel. +43 316 873 5513
Fax: +43 316 873 5520
e-mail: europki@iaik.tugraz.at
http://europki.iaik.at

EuroPKI IAIK CA

Zertifizierungsrichtlinien
Certification Policy
V 1.1
Jänner 2008

1 Inhalt

2 Einleitung

Mit diesen Zertifizierungsrichtlinien wird die Ausstellung von Zertifikaten durch das Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie der TU Graz geregelt.

3 Zuständigkeit

Dieses Dokument wurde vom Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie der TU Graz erstellt und wird auch von dieser Stelle gewartet.

Betreiber:

Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie der TU Graz

Inffeldgasse 16a, A-8010 Graz

Tel. +43 316 873 5513

Fax: +43 316 873 5520

e-mail: europki-info@iaik.tugraz.at

http://europki.iaik.tugraz.at

Kontaktperson:

Dr. Peter Lipp

Inffeldgasse 16a, A-8010 Graz

Tel. +43 316 873 5513

Fax: +43 316 873 5520

Email: peter.lipp@iaik.tugraz.at

3.1 Identifikation der Policy

Name: EuroPKI IAIK CA Zertifizierungs-Policy und Certificate Practice Statement (CPS)

Version: 2.0 vom 20. März 2006

Objekt-ID: 1.3.6.1.4.1.2706.1.2.3.1.1

Die verwendete Policy-ID ist wie folgt aufgeschlüsselt:

ISO assigned	1
Organization acknowledged by ISO	3
US Department of Defense	6
Internet	1
Private	4
IANA registered private enterprises	1
IAIK	2706

PKI	1
CPS IAIK CA Major Version Minor Version	2 3 1 1

4 Anwendungsbereich

Sämtliche vom IAIK-EuroPKI-Zertifizierungsdienst ausgestellten Zertifikate werden von Mitarbeitern und Rechnern des Institutes für Angewandte Informationsverarbeitung und Kommunikationstechnologie der TU Graz sowie nahe stehender Organisationen (insbesondere der gesamten TU Graz; des Vereins A-SIT; des E-Government Innovationszentrums EGIZ; der Stiftung SIC) wie auch von Personen und Rechnern von Organisationen, mit denen das Institut in irgendeiner Form kooperiert, für den Zweck der elektronischen Kommunikation sowie der digitalen Signatur eingesetzt. Der Zertifizierungsdienst ist hierarchisch aufgebaut. **Abbildung 1** illustriert diese Hierarchie. Die folgenden Unterabschnitte legen den Anwendungsbereich der Zertifikate, die von der jeweiligen Sub-CA ausgestellt werden, fest.

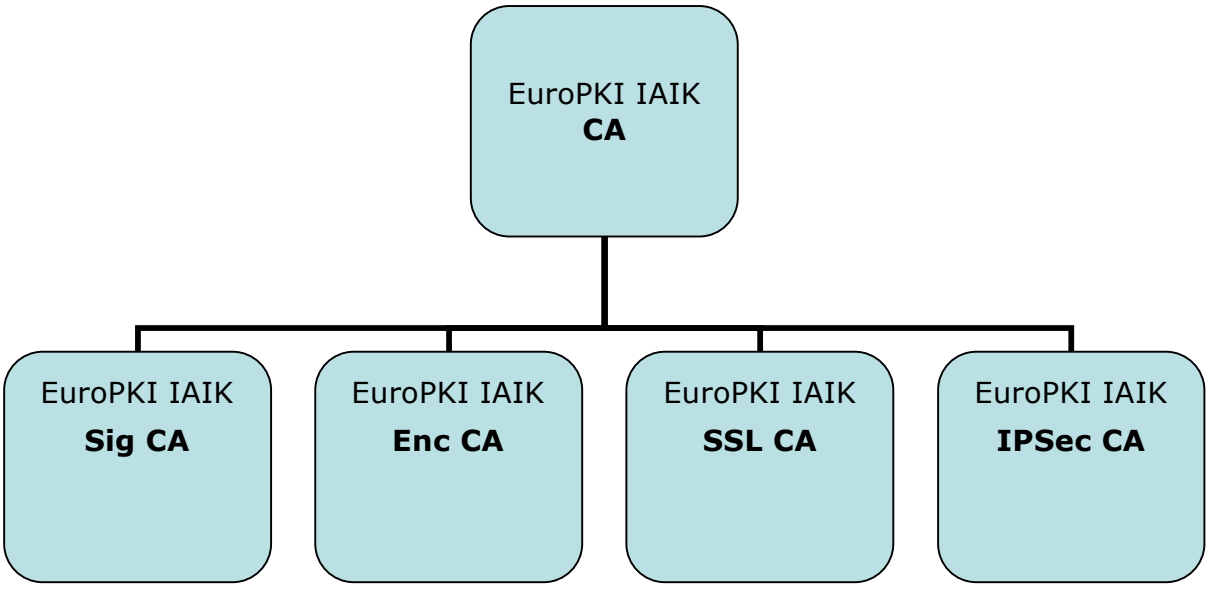

Abbildung 1: Struktur der EuroPKI IAIK Certification Authority Zertifizierungshierarchie

Die *EuroPKI IAIK Certification Authority* stellt Zertifikate für Zwischenzertifizierungsstellen aus, die ihrerseits verschiedene Dienste für Endanwender bieten. Dies erlaubt es den Anwendern der Zertifikate, Vertrauenseinstellungen spezifisch der beabsichtigten Verwendung der Zertifikate auf Ebene der Zertifizierungsstellen zu setzen. Die *EuroPKI IAIK Certification Authority* ist auch Teil der Forschungsaktivitäten des IAIK und unterliegt daher laufender Weiterentwicklung, um die Einsatzfähigkeit neuerer Technologien in der Praxis zu überprüfen. Die *EuroPKI IAIK Certification Authority* wird durch das Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK) der Technischen Universität in Graz, Steiermark, betrieben.

4.1 EuroPKI IAIK SIG CA

Die *EuroPKI IAIK TU-Graz SIG CA* stellt ausschließlich Zertifikate für Endanwender zum Zwecke der Signatur aus. Die Schlüssel-verwendungsbits *digital signature* und/oder *non-repudiation* sind in diesen Zertifikaten gesetzt.

4.2 EuroPKI IAIK ENC CA

Die EuroPKI IAIK ENC CA stellt ausschließlich Zertifikate für Endanwender zum Zwecke der Verschlüsselung aus. Die Schlüsselverwendungsbits *key encipherment* und/oder *data encipherment* sind in diesen Zertifikaten gesetzt.

4.3 EuroPKI IAIK SSL CA

Die EuroPKI IAIK SSL CA stellt ausschließlich Zertifikate für Endanwender für den Einsatz bei Webservern und anderen Servern oder Clients aus, die SSL oder TLS-Dienste verwenden. Die Schlüsselverwendungsbits *digital signature* und *key encipherment* sind in diesen Zertifikaten gesetzt.

4.4 EuroPKI IAIK TU-Graz IPSEC CA

Die EuroPKI IAIK IPSec CA stellt ausschließlich Zertifikate für Endanwender für den Einsatz bei Rechnern aus, die über IPSec eine VPN-Verbindung aufbauen möchten. Die Schlüsselverwendungsbits *digital signature*, key *encipherment, data encipherment* und/oder *key agreement* sind in diesen Zertifikaten gesetzt.

5 Identifizierung des Antragstellers

Dieser Abschnitt beschreibt die Vorgangsweise, die von den beteiligten Parteien einzuhalten ist, wenn die Identität eines Zertifikatsantragsstellers überprüft wird. Diese Vorgangsweise ist unterschiedlich und hängt vom Typ des beantragten Zertifikats ab.

5.1 Personenbezogene Identitätsprüfung

Der Antragsteller, der für sich (für Signatur- oder Verschlüsselungszertifikate) bzw. einen Rechner (Server bzw. IPSec Zertifikate) ein Zertifikat beantragt, muss sich mit einem amtlichen Lichtbildausweis identifizieren oder einem Mitarbeiter des Institutes persönlich bekannt sein, der die Identität des Antragsstellers garantiert. Die Korrektheit einer angegebenen Email-Adresse wird durch Zusenden eines eindeutigen Prüfcodes an diese Adresse geprüft. Wenn sich der Antragsteller im Intranet des IAIK befindet, findet ausschließlich die Prüfung der eingegebenen Emailadresse statt, da durch organisatorische Maßnahmen sichergestellt ist, dass ausschließlich berechtigte Benutzer Zugang zum Intranet haben. Der Nachweis des Besitzes des privaten Schlüssels wird durch die Notwendigkeit, signierte Zertifikatsanträge zu hinterlegen, geführt.

Durchgeführte Identitätsüberprüfungen werden in der Regel von den Mitarbeitern des Instituts nicht protokolliert. Das Anlegen von Kopien von amtlichen Lichtbildausweisen o.Ä. ist nicht zwingend vorgesehen. Signierte Zertifikatsanträge werden nur bis zur Ausstellung des Zertifikats aufbewahrt.

5.2 Server- und Applikationszertifikate

Zertifikate für Server-Software und Applikationen werden von zuständigen Mitarbeitern angefordert und applikationsspezifisch installiert. Diese Mitarbeiter gewährleisten, dass der Schlüssel und das Zertifikat tatsächlich auch am richtigen Server installiert werden.

5.3 Identifizierung bei Zertifikatswiderruf

Wenn ein Zertifikat widerrufen werden soll, gelten dieselben Identifizierungsregeln wie bei der Zertifikatsantragstellung. Zusätzlich wird auch ein mit dem aktuellen Schlüssel signierter Widerrufsantrag oder die Bekanntgabe eines bei der Zertifikatsantragstellung übermittelten geheimen Passworts als Authentisierung akzeptiert.

6 Zertifikatsantrag und –ausstellung

Um von einer der Zertifizierungsstellen ein Zertifikat erhalten zu können, muss der Antragsteller eine selbst-signierte Zertifizierungsanforderung vorlegen. Der Antrag kann über ein Webinterface übermittelt, oder persönlich vorgelegt werden.

Die Zertifizierungsstelle kann die Echtheit des Antrags durch Prüfung des Fingerprints feststellen und, falls erfolgreich, ein Zertifikat ausstellen. Die Gültigkeitsdauer der an Anwender ausgestellten Zertifikate beträgt in der Regel ein Jahr, maximal jedoch drei Jahre. Die *EuroPKI IAIK Certification Authority* behält sich vor, Anträge auf Zertifikatsausstellung abzulehnen.

Alle ausgestellten Zertifikate entsprechen dem X.509v3-Standard und werden dem Antragsteller in Form einer DER formatierten PKCS#7-Certlist oder einem anderen geeigneten Format, über HTTP, E-Mail oder auf einem anderen Medium zugestellt. Dem Antragsteller wird empfohlen, das Zertifikat bei Inempfangnahme zu prüfen.

Die *EuroPKI IAIK Certification Authority* wird die ausgestellten Zertifikate (über LDAP oder HTTP) veröffentlichen, mit Ausnahme der Zertifikate, bei denen die Antragsteller das Unterlassen der Veröffentlichung explizit gefordert haben.

6.1 Gültigkeit von Zertifikaten

Für die Gültigkeit der ausgestellten Zertifikate gelten folgende Regeln:

- Zertifikate für Zertifizierungsstellen sind bis zu sechs Jahre gültig.
- Zertifikate für Endanwender und Services sind bis zu drei Jahre gültig.

6.2 Zertifikatserneuerung

Die Erneuerung von Endanwender-Zertifikaten ist nicht vorgesehen. CA-Zertifikate können erneuert werden.

6.3 Ausnahmen

Falls innerhalb eines bestimmten Projektes erforderlich, behält sich die EuroPKI IAIK Certification Authority vor, in Übereinkunft mit dem

Zertifikatsantragsteller eine Vorgehensweise für Zertifikats-Antragstellung/Ausstellung zu wählen, die nicht explizit im CPS festgehalten ist, aber den Richtlinien der EurpoPki-Policy genügen muss.

7 Widerruf

Die *EuroPKI IAIK Certification Authority* stellt mindestens einmal pro Monat eine Zertifikatssperrliste (CRL) aus. Nach erfolgtem Widerruf eines Zertifikats wird unmittelbar eine neue CRL ausgestellt und publiziert. Jedes von der *EuroPKI IAIK Certification Authority* ausgestellte Zertifikat enthält eine *CRLDistributionPoints* Zertifikatserweiterung, welche einen URL enthält unter dem die entsprechende CRL gefunden werden kann. Es ist die Aufgabe des Anwenders des Zertifikats, CRLs zu holen und zu überprüfen. Ein Zertifikat ist zu widerrufen, wenn die im Zertifikat zertifizierte Information ungültig oder kompromittiert wurde, oder der begründete Verdacht dafür besteht. Dies inkludiert Situationen, in denen (siehe [ePKI-CPS]):

- sich die Daten des Antragstellers geändert haben oder nicht stimmen
- der private Schlüssel des Antragstellers kompromittiert wurde
- der Antragsteller seine Verpflichtungen nicht einhält

Ein Widerruf kann vom Inhaber eines Zertifikats gefordert werden, aber auch von jeder Person, die den Nachweis der Kompromittierung oder der geänderten Daten vorlegen kann. Eine Person, die den Widerruf eines Zertifikats fordert, muss sich gegenüber der *EuroPKI IAIK Certification Authority* authentifizieren. In Übereinstimmung mit der EuroPKI Richtlinie [ePKI-CPS] wird die *EuroPKI IAIK Certification Authority* einen Widerrufsantrag bearbeiten, der mit einem nicht abgelaufenen und nicht widerrufenen Zertifikat, ausgestellt unter der EuroPKI Policy, signiert wurde. Alternativ können die Räume der *EuroPKI IAIK Certification Authority* aufgesucht und ein geeignetes Dokument zur Identifikation vorgelegt werden. Die *EuroPKI IAIK Certification Authority* kann auch selbst ein Zertifikat aus einem der oben genannten Gründe oder ähnlichen Ursachen widerrufen.

Ein Widerruf kann während der üblichen Bürozeiten, also an Werktagen zwischen 9 und 16 Uhr, beantragt werden und wird schnellstmöglich, im Normalfall jedenfalls innerhalb eines Werktages, durchgeführt.

Widerrufsinformation kann auch über alternative Wege, wie OCSP oder HTTP, abgerufen werden.

8 Suspendierung

Suspendierung von Zertifikaten wird nicht unterstützt.

9 Namensgebung

Jedes durch die *EuroPKI IAIK Certification Authority* ausgestellte Zertifikat wird ein nicht leeres Feld mit einem Namen enthalten, das den Zertifikatsinhaber eindeutig identifiziert. In Übereinstimmung mit der

EuroPKI Certificate Policy [ePKI-CPS] muss dieser Name in dem Sinne ein aussagefähiger Name sein, als ein Bezug zwischen dem Namen und dem Antragsteller (Person, Server, ...) existiert. Abschnitt 5 spezifiziert die Regeln zu Identifizierung des Antragstellers.

Bei ausgestellten Zertifikaten werden die in der folgenden Tabelle angegebenen Attribute im Subject-Feld bzw. in der SubjectAltName-Erweiterung zur Indentifizierung des Zertifikatsinhabers herangezogen. Dabei werden in der Regel alle Attribute verwendet; einzelne Attribute können auch weggelassen werden, wenn die verwendeten Attribute zur Identifikation genügen.

Attribut-Typ	**Bedeutung**	**Inhalt (Attribut-Wert)**
C	Country	AT
CN	Common Name	Name der natürlichen Person oder des Dienstes, für die das Zertifikat ausgestellt wurde. Pseudonyme sind nicht zulässig. Beispiele: ***Hans Muster*** ***jce.iaik.tugraz.at***
O	Organization	Für an intern ausgestellte Zertifikate ***Graz University of Technology*** Sonst der Name der externen Firma
OU	Organizational Unit (Abteilung)	Bezeichnung der Abteilung; ***Institute for Applied Information Processing and Communications*** Wenn nicht anwendbar entfällt dieses Feld.
E	Email	Bei natürlichen Personen: Email-Adresse. Diese wird in der *Subject-Alternate-Name*-Erweiterung veröffentlicht.

10 Algorithmen und Schlüssellängen

Derzeit werden ausschließlich Zertifikate für das RSA-Verfahren ausgestellt und mittels SHA-1 und RSA signiert. In Zukunft könnten darüber hinaus auch andere Algorithmen, wie ECDSA, unterstützt werden.

Für die Schlüssellängen der privaten Schlüssel ausgestellter Zertifikate gelten folgende Regeln:

- Schlüssel von Zertifizierungsstellen sind zumindest 2048 Bit lang.
- Schlüssel der Endanwender und Services sind zumindest 1020 Bit lang.

11 Eingesetzte Komponenten

Die *EuroPKI IAIK Certification Authority* verwendet einen Standard-PC mit Red Hat Linux release 9 und selbst entwickelter CA-Software, die auf dem IAIK Java Crypto Toolkit aufbaut.

12 Schlüsselerzeugung und –speicherung

Es ist Aufgabe des Antragstellers den Schlüssel mit einer geeigneten Mindestlänge (im Fall von RSA 1020 Bit) zu erzeugen und für die Sicherheit der Speicherung des privaten Schlüssels durch geeignete Maßnahmen, wie Verschlüsselung über passwort-basierte Verfahren zu sorgen. Der Antragsteller kann dazu jedes Werkzeug in Hardware oder Software für die Generierung und Speicherung einsetzen, solange es der Policy von EuroPKI [ePKI-CPS] entspricht. Die *EuroPKI IAIK Certification Authority* übernimmt weder Verantwortung noch Haftung für Schäden oder andere Folgen die durch ungeeignete Schlüsselgenerierung oder –speicherung hervorgerufen werden.

13 Verpflichtungen des Zertifikatsinhabers

Zertifikatsinhaber dürfen ausgestellte Zertifikate nur für den vorgesehenen Zweck verwenden. Sie haben auch den privaten Schlüssel geeignet zu schützen und verwendete PINs und Passwörter nirgends schriftlich oder elektronisch aufzuzeichnen.

14 Durchführung

Für die Interpretation dieser Policy gilt österreichisches Recht. Die *EuroPKI IAIK Certification Authority* stellt keine qualifizierten Zertifikate aus. Die ausgestellten Zertifikate können aber für die Amtssignatur geeignet sein.

15 Haftung

Die *EuroPKI IAIK Certification Authority* übernimmt keine Garantien über die Sicherheit oder Eignung der angebotenen Dienste. Die Zertifizierungs- und Widerrufsdienste werden mit einem vernünftigen Maß an Sicherheit betrieben, eine Garantie wird dafür jedoch nicht übernommen. In keinem Fall werden Haftungen finanzieller oder anderer Art für Probleme, die durch den Dienst oder die ausgestellten Zertifikate entstehen, übernommen.

16 Gebühren

Die *EuroPKI IAIK Certification Authority* verrechnet keine Gebühren für die angebotenen Dienste.

17 Sicherheit

Die *EuroPKI IAIK Certification Authority* wird auf einer Arbeitsstation betrieben, die direkt nur aus dem Intranet erreichbar ist. Zugang zu den Geräten haben nur befugte vertrauenswürdige Mitarbeiter der EuroPKI IAIK Certification Authority. Authentisierung gegenüber dem Rechner

erfolgt durch Smartcards oder Paßwörter. Der private Schlüssel für die Ausstellung der Zertifikate ist ein Schlüssel mit zumindest 2048 Bit für RSA sowie mindestens 160 Bit für ECDSA, der durch eine Passphrase geschützt ist.

18 Aufzeichnungen

Die *EuroPKI IAIK Certification Authority* wird folgende Informationen archivieren:

- Ausgestellte Zertifikate
- Ausgestellte CRLs
- Kopien von Dokumenten der Antragsteller, sofern eine Kopie erzeugt wurde.

Zertifikate und CRLs werden zumindest für deren Gültigkeitsdauer, andere Dokumente zumindest für fünf Jahre archiviert.

19 Veröffentlichung

Ausgestellte Zertifikate und CRLs sind auf http://europki.iaik.at bzw. auf dem LDAP-Server ldap.iaik.at zu finden. Zertifikate entsprechen dem X.509v3-Standard, CRLs X.509v2. Sie werden PEM- oder DER-kodiert veröffentlicht. Der Inhalt der Zertifikate entspricht dem RFC 3280. Die *EuroPKI IAIK Certification Authority* behält sich vor, in Zukunft auch andere Zertifikatsformate, wie Attributzertifikate oder Zertifikate im XML-Format auszugeben.

20 Begriffe und Abkürzungen

CA	***C**ertification **A**uthority*, Zertifizierungsstelle
CRL	***C**ertificate **R**evocation **L**ist* Zertifikatswiderrufsliste
DER	***D**istinguished **E**ncoding **R**ules* Kodierungsvorschrift für ASN.1
DN	***D**istinguished **N**ame* Eindeutiger Name
HTTP	***H**yper**T**ext **T**ransfer **P**rotocol*
LDAP	***L**ightweight **D**irectory **A**ccess **P**rotocol* Zugangsprotokoll für Verzeichnisdienste
PEM	***P**rivacy **E**nhanced **M**ail*; definiert den häufig verwendeten Kodierungsstandard für Zertifikate.
PKCS	***P**ublic **K**ey **C**ryptography **S**tandard*
PKCS#7	Standard, der ein Format für signierte und verschlüsselte Dokumente spezifiziert. Vorläufer von CMS.
PKCS#12	Standard, der die sichere Speicherung privater

	Schlüssel und dazugehöriger Zertifikate spezifiziert.
RA	***R**egistration **A**uthority*, Registrierungsstelle
RSA	Asymmetrischer Kryptographischer Algorithmus, kann für Signatur und Verschlüsselung eingesetzt werden.
SHA-1	***S**ecure **H**ash* - Algorithmus
URL	***U**niversal **R**esource **L**ocator* Identifizieren eine Ressource über ihren primären Zugriffsmechanismus und den Ort der Ressource.
X.509	Standard für digitale Zertifikate und Widerrufslisten.
XML	**E**xtensible **M**arkup **L**anguage
Fingerprint	Hash über einen Schlüssel, ein Zertifikat oder eine andere Datenstruktur, die dieselbe eindeutig repräsentiert.
Identität	*Die Bezeichnung der Nämlichkeit von Betroffenen (Z 7) durch Merkmale, die in besonderer Weise geeignet sind, ihre Unterscheidbarkeit von anderen zu ermöglichen; solche Merkmale sind insbesondere der Name, das Geburtsdatum und der Geburtsort, aber auch etwa die Firma oder (alpha)numerische Bezeichnungen* [EGovG]
eindeutige Identität	*Die Bezeichnung der Nämlichkeit eines Betroffenen (Z 7) durch ein oder mehrere Merkmale, wodurch die unverwechselbare Unterscheidung von allen anderen bewirkt wird* [EGovG]
Identifikation	*Der Vorgang, der zum Nachweis bzw. zur Feststellung der Identität erforderlich ist* [EGovG]
Authentizität	*Die Echtheit einer Willenserklärung oder Handlung in dem Sinn, dass der vorgebliche Urheber auch ihr tatsächlicher Urheber ist* [EGovG]
Authentifizierung	*Der Vorgang, der zum Nachweis bzw. zur Feststellung der Authentizität erforderlich ist* [EGovG]
Amtssignatur	*Die Amtssignatur ist eine elektronische Signatur im Sinne des Signaturgesetzes, deren Besonderheit durch ein entsprechendes Attribut im Signaturzertifikat ausgewiesen wird.* [EGovG]

21 Bibliographie und Gesetzesverweise

[EGovG] E-Government-Gesetz, Bundesgesetzblatt vom 27. Februar 2004, http://www.a-sit.at/signatur/rechtsrahmen/e-govg_d.pdf

[SigG] Signaturgesetz, BGBl. I Nr. 190/1999, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 152/2001.

[SigV] Signaturverordnung, BGBl. II Nr. 30/2000 vom 2. Februar 2000, geändert durch BGBl. II Nr. 527/2004, in Kraft getreten am 1.1.2005.

[RFC 3280] Housley, R., Polk, W., Ford, W., Solo, D., Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile; April 2002, http://www.ietf.org/rfc/rfc3280.txt

[RFC 3647] Chokani, S., Ford, W., Sabett, R., Merrill, C., Wu, S.: Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework; November 2003. http://www.ietf.org/rfc/rfc3647.txt

[ePKI-CPS] EuroPKI Certificate Policy, Version 1.1, January 2004, OID: 1.3.6.1.4.1.5255.1.1.1