KFA – Krankenfürsorgeanstalt der Bediensteten der Stadt Wien
Schlesingerplatz 5, A-1080 Wien, Tel. +43 1 40436 0
e-mail: generaldirektion@kfa.co.at
http://www.kfa.co.at
DVR Nr. 0047155

KFA Wien Trustcenter

Zertifizierungsrichtlinien

Certification Policy

V 1.1

November 2015

Inhalt

1. Einleitung

Mit diesen Zertifizierungsrichtlinien wird die Ausstellung von Zertifikaten durch die KFA - Krankenfürsorgeanstalt der Bediensteten

der Stadt Wien geregelt.

Die Zertifikate des Trustcenter der KFA (Sub-CA Benutzer und Sub-CA Externe) entsprechen der Definition der „fortgeschrittenen elektronischen Signatur" nach Art. 2 Z 2 der Signaturrichtlinie 1999/93/EG sowohl als auch § 2 Z 3 lit. a bis d Signaturgesetz [SigG].

2. Zuständigkeit

Dieses Dokument wurde von der IT Abteilung der KFA Wien erstellt und wird auch von dieser Stelle gewartet.

Betreiber:

Krankenfürsorgeanstalt der Bediensteten
der Stadt Wien (KFA)
Schlesingerplatz 5, A-1080 Wien, Tel. +43 1 40 436 0
Telefax +43 1 40436 99 46863
e-mail: generaldirektion@kfa.co.at
DVR: 0000191

Kontaktperson:

Peter Pfläging
Abteilungsleiter IT
Schlesingerplatz 5
A-1080 Wien
Email: peter.pflaeging@kfa.co.at
Tel.: (+43 1) 40 436-46881
Fax.: (+43 1) 40 436-99-46881
Web : http://www.kfa.co.at

2.1. Identifikation der Policy

Name: KFA WIEN TRUSTCENTER – Richtlinien für die Ausstellung von Zertifikaten durch die KFA Wien
Version: 1.1 vom 23. November 2015

3. Anwendungsbereich

Sämtliche vom KFA WIEN TRUSTCENTER-Zertifizierungsdienst ausgestellten Zertifikate werden für den Einsatz bei Mitarbeitern und auf Rechnern der KFA Wien, bei deren externen Dienstleistern sowie bei Kunden 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.

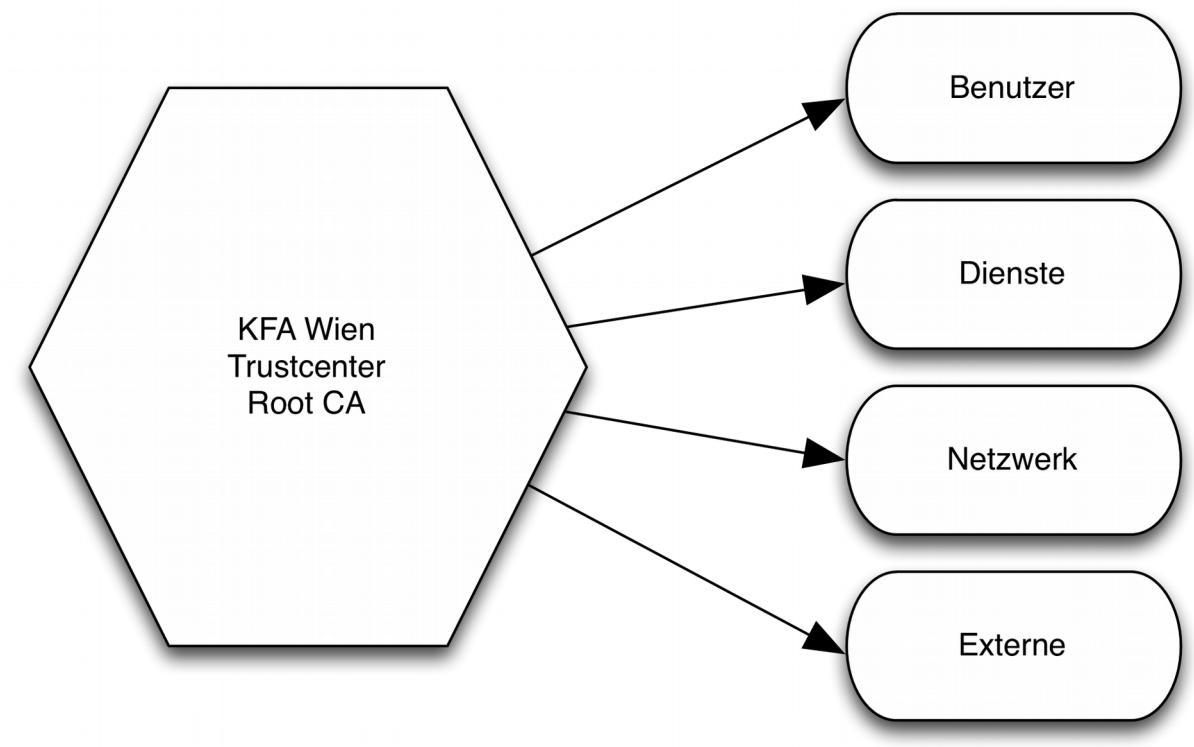

Abbildung 1: Struktur der KFA Wien Trustcenter Zertifizierungshierarchie

a) KFA-Wien-Root-CA

Die Root-CA bildet die Wurzel der KFA WIEN TRUSTCENTER Zertifizierungshierarchie. Sie stellt ausschließlich Zertifikate für untergeordnete Zertifizierungsstellen aus.

b) Benutzer-CA

Die Benutzer-CA stellt Signaturzertifikate für Benutzer aus.

Signaturen dieser CA sind fortgeschrittene Signaturen nach nach der Definition der „fortgeschrittenen elektronischen Signatur" nach Art. 2 Z 2 der Signaturrichtlinie 1999/93/EG sowohl als auch § 2 Z 3 lit. a bis d SigG.

Diese Zertifikate sind auch für den Einsatz bei der Verschlüsselung von Daten während der Speicherung oder bei der Übertragung von Daten geeignet.

c) Dienste-CA

Die Dienste-CA stellt Zertifikate für Applikationen aus, die nicht einem bestimmten Benutzer zugeordnet werden, sondern einer Applikation, die sich einer anderen gegenüber mit Hilfe dieses Zertifikats identifiziert. Ein Beispiel hierfür sind Webserver, Applikationsserver, Applikationensaccounts, WebServices ....

d) Netzwerk-CA

Die Netzwerk-CA stellt Zertifikate für Geräte aus, die nicht einem bestimmten Benutzer zugeordnet werden, sondern ein Gerät in bestimmten Netzwerkbereichen identifizieren

Weiterhin werden auch Zertifikate für Komponenten einer Netzwerk-Infrastruktur ausgestellt, wie sie beispielsweise für den Einsatz von IPSEC benötigt werden.

e) Externe-CA

Diese CA stellt Zertifikate für Applikationen aus, die extern bei Dienstleistungsunternehmen, Kunden oder anderen Vertragspartnern eingesetzt werden. Diese Zertifikate können sowohl Verschlüsselungs- als auch Signaturzertifikate sein.

Signaturen dieser CA sind fortgeschrittene Signaturen nach nach der Definition der „fortgeschrittenen elektronischen Signatur" nach Art. 2 Z 2 der Signaturrichtlinie 1999/93/EG sowohl als auch § 2 Z 3 lit. a bis d SigG.

4. 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.

Mit den folgenden Massnahmen wird eine eindeutige Identifikation des Signaturinhabers (Signators) garantiert (§ 2 Z 3 lit. a und b SigG).

4.1. Personenbezogene Identitätsprüfung

Der Antragsteller muss persönlich erscheinen und ist entweder amtsbekannt oder identifiziert sich mit einem amtlichen Lichtbildausweis. Der KFA WIEN TRUSTCENTER-Mitarbeiter dokumentiert die Art der Identifikation. Für die Ausstellung von Zertifikaten an Externe werden dieselben Mechanismen angewandt. Zusätzlich wird noch durch geeignete Dokumente (Firmenbuchauszug oder Überprüfung der Zeichnungsberechtigung) geprüft, ob die Person berechtigt ist, die externe Stelle für den Zweck der Zertifikatsausstellung zu vertreten.

Für die Durchführung der Prüfung sind verantwortlich

- Für externe Benutzer wird eine zentrale Registrierungsstelle (RA) eingerichtet.
- Die Identität von Mitarbeitern wird entweder bei dieser zentralen RA oder in der Personalabteilung geprüft, die dann die Funktion einer RA ausübt.

Die Registrierungsstellen protokollieren die durchgeführten Identitätsprüfungen mit Hilfe einer einfachen Liste, in der mitgeführt wird, welcher RA-Mitarbeiter welchen Zertifikatswerber überprüft hat und welches Mittel der Identifikation verwendet wurde. Das Anlegen von Kopien von amtlichen Lichtbildausweisen o.Ä. wird nicht generell gefordert; Kopien können jedoch bei Bedarf erzeugt und aufbewahrt werden. Im Falle von externen Benutzern wird jedoch die Art und Nummer des Ausweisdokumentes in der Liste dokumentiert.

4.2. Zertifikate für Dienste

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.

4.3. CA-Generiert

Es wird sowohl der Schlüssel als auch das Zertifikat von KFA WIEN TRUSTCENTER generiert und von einem Mitarbeiter zur Dienststelle

gebracht oder verschickt. Der Schlüssel wird bei der Übertragung mit PKCS#12 gesichert und das dazugehörige Passwort auf einem alternativen, sicheren Weg der Dienststelle übermittelt.

4.4. Zulässige Überprüfungsmethoden

Die folgende Tabelle zeigt die für die einzelnen Zertifizierungsstellen zulässigen Identitätsprüfungsmethoden. Dabei

Zertifizerungsstelle	Pers.bez.	Server	CA-Gen.
Root-CA	n.a.[1]	n.a.	n.a.
Dienste-CA		✓	✓
Netzwerk-CA		✓	✓
Benutzer-CA	✓		✓
Externe-CA	✓	✓	✓

Tabelle 1: Identifikationsprüfung, mögliche Kombinationen

4.5. 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. Wenn der Antragsteller den Widerruf bei einer externen Registrierungsstelle beantragt (beispielsweise Personalabteilung) dann ist der Antrag der RA an die CA auch digital zu signieren.

[1] nicht anwendbar

5. Zertifikatsantrag und –ausstellung

Um von einer der KFA WIEN TRUSTCENTER-CAs ein Zertifikat erhalten zu können, muss der Antragsteller eine selbst-signierte Zertifizierungs-anforderung vorlegen. Für die Benutzer-CA ist dies nicht erforderlich, da dort sowohl Schlüssel als auch die Zertifikate von KFA WIEN TRUSTCENTER erzeugt werden. Der Antrag kann über E-Mail (Signatur Request) übermittelt, oder persönlich vorgelegt werden.

Die KFA WIEN TRUSTCENTER-CA wird die Echtheit des Antrags durch Prüfung des Fingerprints feststellen und, falls erfolgreich, ein Zertifikat ausstellen. Die Gültigkeitsdauer der an Anwender ausgestellten Zertifikate beträgt drei Jahre. Die KFA WIEN TRUSTCENTER-CA behält sich vor, Anträge auf Zertifikatsausstellung abzulehnen.

Bei diesem Vorgang wird garantiert und überprüft, dass die Signaturdaten in der alleinigen Kontrolle des Signierenden verbleibt (§ 2 Z 3 lit. c SigG). Dies geschieht entweder dadurch, dass der Antragsteller einen Signaturrequest übermittelt, welcher signiert wird, oder (bei der Beantragung über das Webinterface) dadurch, dass der Request mit einem durch den Benutzer frei wählbaren Passwort verschlüsselt wird.

Des weiteren wird der Benutzer darüber aufgeklärt, entsprechende Sicherheitsmassnahmen für sein Zertifikat zu etablieren und das Passwort, welches auf dem Zertifikat liegt, entsprechend den allgemein üblichen Passwortregeln zu verwalten.

Alle ausgestellten Zertifikate entsprechen dem X.509v3-Standard und werden dem Antragsteller als Zertifikatskette (beginnend bei der KFA WIEN TRUSTCENTER-Root-CA) in Form einer DER- oder PEM-formatierten PKCS#7-certlist, oder einem anderen geeigneten Format, über email oder auf einem anderen Medium zugestellt. Dem Antragsteller wird empfohlen, die Zertifikatskette bei Inempfangnahme zu prüfen.

Die KFA WIEN TRUSTCENTER-CA wird die ausgestellten Zertifikate (über ldap oder http) veröffentlichen, mit Ausnahme der Zertifikate, bei denen die Antragsteller das Unterlassen der Veröffentlichung gefordert haben.

5.1. Gültigkeit von Zertifikaten

Für die Gültigkeit der ausgestellten Zertifikate gelten folgende Regeln:

- Das selbst-signierte Wurzelzertifikat der KFA WIEN TRUSTCENTER-CA-Hierarchie ist 30 Jahre gültig.
- Zertifikate, die von der KFA WIEN TRUSTCENTER-Wurzel-CA ausgestellt werden, sind 10 Jahre gültig.
- Zertifikate für Endanwender und Services sind bis zu 5 Jahre gültig.

5.2. Zertifikatserneuerung

Zertifikate der KFA Wien können erneuert werden. Es gelten in diesem Fall die gleichen Regeln wie bei der Ausstellung eines neuen Zertifikats.

6. Widerruf

Die KFA WIEN TRUSTCENTER-CA veröffentlicht für die abgeleiteten CAs zumindest wöchentlich, jedenfalls jedoch nach erfolgtem Widerruf eines Zertifikates, eine neue Zertifikatswiderrufsliste (CRL), die dem Standard X.509v2 entsprechen. Jedes ausgestellte Zertifikat enthält eine *CRL Distribution Points* Erweiterung mit einer URL, unter der die Widerufsliste abgerufen werden kann. Es ist Aufgabe des Anwenders von Zertifikaten, bzw. der von ihm eingesetzten Software, diese Widerrufslisten herunterzuladen und auszuwerten. KFA WIEN TRUSTCENTER behält sich vor, in Zukunft auch OCSP-Widerufsdienste anzubieten.

KFA WIEN TRUSTCENTER wird jedes Zertifikat widerrufen, bei dem der Verdacht besteht, dass die mit dem Zertifikat bestätigte Information ungültig wird oder kompromittiert wurde, bzw. der begründete Verdacht dafür besteht. Insbesondere betrifft dies die folgenden Fälle:

- Die mit dem Zertifikat bestätigten Daten des Antragsstellers haben sich geändert;
- der private Schlüssel wurde kompromittiert;
- der Antragssteller hält seine Verpflichtungen nicht ein.

Ein Widerruf kann vom Inhaber eines Zertifikats gefordert werden, aber auch von jeder anderen Person, die den Nachweis der Kompromittierung oder der geänderten Daten vorlegen kann.

Eine Person, die den Widerruf eines Zertifikats fordert, muss sich authentisieren. Jeder Widerrufsantrag, der mit einem nicht abgelaufenen und nicht widerrufenen Zertifikat, ausgestellt von KFA WIEN TRUSTCENTER oder einem von ihr anerkannten Zertifizierungsdienst, signiert wurde, gilt hierbei als authentisiert. Alternativ kann eine Registrierungsstelle von KFA WIEN TRUSTCENTER aufgesucht und ein geeignetes Dokument zur Identifikation vorgelegt werden. Der Widerruf ist auch über die IT-Hotline möglich, welche unter der Nummer +43 1 40436 46666 erreichbar ist. Der Zertifizierungsdienst ruft zur Überprüfung der Identität die zu dem Zertifikat gehörende eingetragene Telefonnummer zurück.

Widerrufe werden werktags zwischen 8:00 und 15:30 Uhr entgegengenommen und werden innerhalb von maximal 96 Stunden bearbeitet.

KFA WIEN TRUSTCENTER kann auch selbst ein Zertifikat aus einem der oben genannten Gründe oder ähnlichen Ursachen widerrufen.

7. Suspendierung

Suspendierung von Zertifikaten wird nicht unterstützt.

8. Namensgebung

Jedes ausgestellte Zertifikat enthält einen *Distinguished Name* (DN), der den Antragssteller eindeutig identifiziert, und dem folgenden Namensschema unterliegt:

Sämtliche ausgestellten Zertifikate enthalten folgende Felder

AVA	Bedeutung	Inhalt
C	Country	at
CN	Common Name	Name der natürlichen Person oder des Dienstes, für die das Zertifikat ausgestellt wurde. Pseudonyme sind nicht zulässig. Beispiele: ***Johann Mustermitarbeiter*** ***www.kfa.co.at*** ***Sanatorium Hera Postausgang***
O	Organisation	Für an intern ausgestellte Zertifikate ***KFA Wien*** oder ***Sanatorium Hera*** Sonst der Name der externen Firma
OU	Organisational Unit (Abteilung)	Bezeichnung der Abteilung soweit erwünscht oder notwendig. (optional)
E	Email	Bei natürlichen Personen: Email-Adresse. Diese wird auch in der *Subject-Alternate-Name*-Erweiterung veröffentlicht.

9. Algorithmen und Schlüssellängen

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

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

- Der zum selbst-signierten Wurzelzertifikat der KFA WIEN TRUSTCENTER-CA-Hierarchie gehörige private Schlüssel ist zumindest 2048 Bit lang.
- Die privaten Schlüssel der einzelnen Sub-CAs sind ebenfalls zumindest 2048 Bit lang.
- Schlüssel der Endanwender und Services sind zumindest 2048 Bit lang.

Diese Algorithmen und Schlüssellängen genügen § 2 Z 3 lit. d SigG.

10.Eingesetzte Komponenten

Die KFA WIEN TRUSTCENTER-CA verwendet einen Server-PC unter Linux. Als Zertifzierungssoftware wird EJBCA und Open-SSL in der jeweils aktuellen Version eingesetzt.

11.Schlüsselerzeugung und –speicherung

Es ist Aufgabe des Antragstellers, den Schlüssel mit einer geeigneten Mindestlänge zu erzeugen und für die Sicherheit der Speicherung des privaten Schlüssels durch geeignete Maßnahmen, wie Verwendung von Smartcards oder Verschlüsselung über Passwort-basierte Verfahren zu sorgen. Die KFA WIEN TRUSTCENTER-CA übernimmt weder Verantwortung noch Haftung für Schäden oder andere Folgen die durch ungeeignete Schlüsselgenerierung oder –speicherung hervorgerufen werden.

Für Benutzersignaturen werden die Schlüssel von der KFA WIEN TRUSTCENTER-CA für das RSA-Verfahren mit einer Länge von 2048 Bit erzeugt und in einem PKCS-12-File passwort- oder passphrasen-geschützt gespeichert.

Beim Erzeugen der Zufallszahlen wird ein Algorithmus verwendet, der Hardwareereignisse des Signaturrechners in die Gewinnunf mit einbezieht.

12.Verpflichtungen des Zertifikatsinhaber

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.

13.Durchführung

Für die Interpretation dieser Policy gilt österreichisches Recht. KFA WIEN TRUSTCENTER stellt keine qualifizierten Zertifikate aus.

14.Haftung

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

15.Gebühren

Die Gebühren der Zertifikate des KFA WIEN TRUSTCENTER sind auf Anfrage an die KFA Wien oder die IT-Abteilung der KFA Wien erhältlich.

16. Sicherheit

KFA-WIEN-Root-CA wird offline auf einer Arbeitsstation ohne Netzwerkverbindung betrieben.

Die delegierten Unter-CAs sind auf gesicherten Rechnern im abgeschlossenen Netz der KFA Wien in Betrieb. Der Zugang zu den Geräten entspricht den Vorgaben für Transaktion auf sensible Daten (§ 4 (2) DSG 2000) und Risikoanalysestrategie (SIHB Teil 1/3.4.1)

„Schutzbedarfskategorie hoch". Zugang zu den Geräten haben nur befugte vertrauenswürdige Mitarbeiter von KFA WIEN TRUSTCENTER.

Die Authentisierung gegenüber dem Rechner erfolgt durch Smartcards oder Passworte.

Der private Schlüssel für die Ausstellung der Zertifikate ist ein Schlüssel mit zumindest 2048 Bit für RSA und DSA sowie mindestens 160 Bit für ECDSA, der durch eine Passphrase geschützt ist. Der Schlüssel wird auf einem externen Medium, wie Diskette, Zip-disk, CDROM oder Smartcard, aufbewahrt. Um sich gegen Probleme durch Zerstörung des Mediums zu schützen, kann eine Kopie des Schlüssels auf einem vergleichbaren Medium aufbewahrt werden.

17.Aufzeichnungen

Das KFA WIEN TRUSTCENTER wird folgende Informationen archivieren:

- Zertifikatsanforderungen der ausgestellten Zertifikate
- Ausgestellte Zertifikate
- Ausgestellte CRLs
- Verträge mit anderen Parteien
- Kopien von Dokumente und andere Validierungsinformation der Antragsteller, mit Ausnahme persönlich bekannter Antragsteller, sofern eine Kopie erzeugt wurde.

Die Dokumente werden für mindestens fünf Jahre archiviert.

18.Veröffentlichung

Ausgestellte Zertifikate und CRL's sind auf http://service.kfa.co.at zu finden. Zertifikate entsprechen dem X.509v3-Standard, CRL's X.509v2. Sie werden PEM- oder DER-kodiert veröffentlicht. Der Inhalt der Zertifikate entspricht dem RFC 3280. KFA WIEN TRUSTCENTER behält sich vor, in

Zukunft auch andere Zertifikatsformate, wie Attributzertifikate oder Zertifikate im XML-Format auszugeben.

Anhang A: Begriffe und Abkürzungen

AVA	***A**ttribute-**V**alue-**A**ssertion;* Komponente eines Namens in einem Zertifikat
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	
LDAP	***L**ightweight **D**irectory **A**ccess **P**rotocol* Zugangsprotokoll für Verzeichnisdienste
OCSP	***O**nline **C**ertificate **S**tatus **P**rotocol* Protokoll zur Online-Abfrage des Status eines Zertifikates.
PEM	***P**rivacy **E**nhanced **M**ail*; definiert 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 sicher 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)nummerische 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]
Wiederholungsidentität	*die Bezeichnung von Betroffenen (Z 7) in der Weise, dass zwar nicht ihre eindeutige Identität, aber ihre Wiedererkennung im Hinblick auf ein früheres Ereignis, wie etwa ein früher gestelltes Anbringen, gesichert ist* [EGovG]
Identifikation	*den 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	*den Vorgang, der zum Nachweis bzw. zur Feststellung der Authentizität erforderlich ist* [EGovG]

Anhang B: Bibliographie und Gesetzesverweise

[SigG] Signaturgesetz, BGBl. I Nr. 190/1999, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 75/2010.

[SigV] Signaturverordnung, BGBl. II Nr. 3/2008 vom 7. Jänner 2008, geändert durch BGBl. II Nr. 401/2010, in Kraft getreten am 9.12.2010.

[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

Anhang C: Änderungen

15.4.2015	Peter Pfläging	Version 1.0	Initialversion
23.11.2015	Peter Pfläging	Version 1.1	• Eine weitere Sub-CA „Netzwerk" wurde eingeführt.Die entsprechenden Textsegmente wurde angepasst. • Die Anhänge wurden als solche markiert. • Gesetzesverweise auf neuere Versionen.