AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

Zertifikatsregeln für die Country Verifying Certification Authority (CVCA) der Liechtensteinischen Landesverwaltung

Version 1.0

01.09.2011

Städtle 38 | 9490 Vaduz | Liechtenstein | T +423 236 61 41 | F +423 236 61 64 | info@apa.llv.li | www.apa.llv.li

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

INHALTVERZEICHNIS

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

1. Einleitung

Durch die Zertifikatregeln soll zwischen den Zertifizierungsstellen (Country Verifying Certification Authorities - CVCA) der nationalen Wurzelzertifizierungsinstanzen und den verantwortlichen Stellen zur Prüfung von Reisedokumenten und Aufenthaltsausweisen (Dokumentenprüfinstanzen - Document Verifiers - DV) der verschiedenen Mitgliedstaaten (gemäß Abschnitt 1.6) Vertrauen geschaffen und eine ausreichende Interoperabilität sichergestellt werden, damit die EAC-PKI (Public-Key-Infrastruktur für die erweiterte Zugriffskontrolle) funktionieren kann.

Diese Zertifikatregeln werden gemäß Ziffer 5.5.3 der technischen Spezifikationen der Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten im Anhang der Entscheidung K(2006) 2909 vom 28.6.2006 festgelegt.

Die Zertifikatregeln beziehen sich nur auf die Verwendung von Zertifikaten für die Kontrolle des Zugriffs auf Fingerabdruckdaten auf für die erweiterte Zugriffskontrolle (Extended Access Control EAC) geeigneten Pässen und Reisedokumenten zum Zwecke der Grenzkontrolle und zur Kontrolle des Zugriffs auf Aufenthaltsausweise des Fürstentums Liechtenstein.

Sie enthalten Mindestanforderungen, die die Grundlage für die Verwendung von Zertifikaten der Liechtensteinischen Wurzelzertifizierungsinstanz (LI-CVCA) durch etwaige zukünftig betriebene Liechtenstein'sche Dokumentenprüfinstanzen (LI-DVCAs) und Kontrollinstanzen (LI-IS) bilden.

Diese Zertifikatregeln gründen sich auf der vom Bundesamt für Sicherheit in der Informationstechnik veröffentlichten technischen Richtlinie *Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.1.1, TR-03110 [BSI TR EAC]*.

1.1 Überblick

Das gegenständliche Dokument basiert auf den Vorgaben der Zertifizierungsrichtline der EU-Kommission [EU CP] und ist abgesehen von geringfügigen Anpassungen an die Erfordernisse der Liechtensteiner Landesverwaltung inhaltlich ident zur EU Vorgabe.

Diese Zertifikatregeln gelten für die unter Ziffer 2.2 („Public Key Infrastructure") der [BSI TR EAC] beschriebene Public-Key-Infrastruktur, die im Kontext der LI-CVCA sowohl für Reisedokumente als auch für Aufenthaltsausweise zur Anwendung kommt.

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

1.2 Dokumentenname sowie Identifikation

Der LI-CVCA-CP für Reisepass und Aufenthaltsausweis wird der

Object Identifier (OID) 2.16.438.10.20.1.1.0 [1] zugeordnet

zugeordnet (die letzten beiden Stellen benennen die Versions-Nummer der aktuell gültigen LI-CVCA-CP).

1.3 Teilnehmer der Zertifizierungsinfrastruktur (PKI)

Dieser Abschnitt gibt einen Überblick über die Zertifizierungsstellen, Zertifikatinhaber, Registrierungsstellen und Endanwender der Public-Key-Infrastruktur für die erweiterte Zugriffskontrolle (EAC-PKI). Die EAC-PKI ist Bestandteil der internationalen Sicherheitsinfrastruktur zur Gewährleistung und Kontrolle der Integrität und Authentizität der von den Mitgliedstaaten ausgestellten maschinenlesbaren Reisedokumente (Machine Readable Travel Document MRTD, Reisepass) und der Aufenthaltsausweise für Drittstaatsangehörige (Residence Permit RP).

	Zertifizierungs-stelle **(Certification Authority)**	**Registrierungs-stelle** **(Registration Authority)**	**Zertifikats-inhaber** **(Subscriber)**	**Vertrauens-partner** **(Relying Party)**
Zertifizierungsstelle der nationalen Wurzelzertifizierungsinstanz (Country Verifying Certificate Authority CVCA)	X	X		
Dokumentenprüfinstanz (Document Verifier DV)	X	X	X	X
Kontrollinstanz (Inspection System IS)			X	X
maschinenlesbares Reisedokument (Machine Readable Travel Document MRTD)			X	
maschinenlesbarer Aufenthaltstitel (Residence Permit RP)			X	

Tabelle 1: Überblick über die PKI-Teilnehmer der EAC-PKI

[1] 2.16.438.10.20 = APA
2.16.438.10.20.1 = Zertifikatsregeln für die CVCA
2.16.438.10.20.1.1.0 = Version 1.0

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

1.3.1 Zertifizierungsstellen

Liechtensteinische Wurzelzertifizierungsinstanz (LI-CVCA):

Die Zertifizierungsstelle der Liechtensteinischen Landesverwaltung wird LI-CVCA genannt. Die öffentlichen Schlüssel dieser CVCA sind in den selbstsignierten CVCA-Zertifikaten und in CVCA-Linkzertifikaten enthalten. Beide Klassen werden als „CVCA-Zertifikate“ bezeichnet. Die LI-CVCA regelt die Rechte aller (in- oder ausländischen) Dokumentenprüfinstanzen (F-DVCAs) auf Zugang zu sensiblen Daten auf Chips von Liechtensteinischen maschinenlesbaren Reisedokumenten bzw. Aufenthaltsausweisen durch Ausstellung von DV-Zertifikaten, die mit Zugriffskontrollattributen verbunden sind.

Die LI-CVCA stellt Zertifikatinhabern (Abonnenten) Zertifikate aus. In diesem Dokument werden Zertifikatinhaber als „Dokumentenprüfinstanz“ (Document Verifier - DV) bezeichnet. Eine Dokumentenprüfinstanz verwaltet zueinander gehörende Kontrollinstanzen (Inspection Systems – IS; gemeint ist das Kontrollsystem einschließlich der hoheitlichen Lesegeräte).

Dokumentenprüfinstanz (DVCA):

Eine Dokumentenprüfinstanz greift für die Ausstellung von Zertifikaten für ihre Kontrollinstanzen auf eine Zertifizierungsstelle (Certification Authority - CA) zu-rück. Die Zugangsrechte und die Gültigkeitsdauer des DV-Zertifikats gehen in der Regel auf das jeweilige von einer Dokumentenprüfinstanz ausgestellte Lesegerätzertifikat (IS-Zertifikat) über. Gleichwohl KANN die Dokumentenprüfinstanz die Zugangsrechte oder die Gültigkeitsdauer weiter einschränken.

1.3.2 Registrierungsstellen

Nationale Registrierungsstelle (Country Verifying Registration Authority CVRA):

Für die LI-CVCA gibt es nur eine Registrierungsstelle, nämlich die Liechtensteinische nationale Registrierungsstelle (LI-CVRA), die beim Ausländer- und Passamt der Liechtensteinischen Landesverwaltung (LLV/APA) angesiedelt ist.

Die LI-CVRA ist für die Identifizierung und Authentisierung von Zertifikatsanträgen der Dokumentenprüfinstanz zuständig; Zertifikatsanträge für Abonnentenzertifikate können mithin nur von Dokumentenprüfinstanzen gestellt werden. Zusätzlich leitet die LI-CVRA die Ausstellung von Zertifikaten für Dokumentenprüfinstanzen in die Wege und überprüft den Prozess des Widerrufs und die Erneuerung von Zertifikaten bei von der LI-CVCA ausgestellten Zertifikaten.

Im Folgenden wird die LI-CVRA als Teil der LI-CVCA betrachtet, und daher wird nur die Bezeichnung „LI-CVCA“ verwendet.

DV-Registrierungsstelle:

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

Dokumentenprüfinstanzen sind für die Identifizierung und Authentisierung von Zertifikatsanträgen der Kontrollinstanzen zuständig. Zusätzlich leitet ein Doku-mentprüfer die Ausstellung von Zertifikaten für Kontrollinstanzen in die Wege und überprüft den Prozess des Widerrufs und der Erneuerung von Zertifikaten.

Im Folgenden wird die DV-Registrierungsstelle als Teil der Dokumentenprüfinstanz betrachtet und daher wird nur der Begriff „Dokumentenprüfinstanz“ verwendet.

1.3.3 Zertifikatsinhaber / Abonnenten

Abonnenten im Rahmen dieser Regeln sind Dokumentenprüf- und Kontrollinstanzen. Der Begriff „Dokumentenprüfinstanz“ ist in Abschnitt 1.3.1 definiert.

Für die Zwecke dieser Zertifikatsregeln wird eine Kontrollinstanz als die Infrastruktur, Hardware und Software definiert, welche erforderlich ist, um IS-Zertifikate von zuständigen Dokumentenprüfinstanz einzuholen, um derartige IS-Zertifikate und die zugehörigen IS-Schlüssel aufzubewahren und zu verwalten und um mit Hilfe dieser IS-Zertifikate Fingerabdruckdaten von maschinenlesbaren Reisedokumenten und Aufenthaltsausweisen auszulesen; dies schließt auch die Verfahren zur Kontrolle des Zugangs zu den Lesegeräten ein.

1.3.4 Vertrauenspartner („Relying Parties“)

„Relying Parties“ im Rahmen einer EAC-PKI sind Dokumentenprüfinstanzen, Kontrollinstanzen und maschinenlesbare Reisedokumente sowie maschinenlesbare Aufenthaltsausweise.

Ein Vertrauenspartner ist eine Stelle, die die Unterschrift auf einem Zertifikat anhand eines als vertrauenswürdig geltenden Zertifizierungspfades (siehe Abschnitt 1.4) überprüft.

1.3.5 Sonstige Teilnehmer

Für das Fürstentum Liechtenstein gibt es keine weiteren Teilnehmer an der in diesem Dokument spezifizierten EAC-PKI.

1.4 Anwendungsbereich

Der Anwendungsbereich der gegenständlichen PKI besteht ausschließlich darin den Lesezugriff von Kontrollinstanzen auf Fingerabdruckdaten, die in maschinenlesbaren Reisedokumenten und Aufenthaltsausweisen gespeichert sind, zu ermöglichen. Der Lesezugriff ist ausschließlich zur Überprüfung der Identität des Inhabers mittels unmittelbar verfügbarer abgleichbarer Merkmale zulässig.

Schlüsselpaare und Zertifikate der LI-CVCA werden nur für folgende Zwecke verwendet:

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

1. Der private Schlüssel der LI-CVCA ist zur Signierung des Zertifikats einer Dokumentenprüfinstanz eines anderen Mitgliedstaats (F-DVCA) zu verwenden. (siehe Abschnitt 3.3);

2. Ein CVCA-Zertifikat ist zum Verifizieren von Signaturen von DV-Zertifikaten und von äußeren Signaturen von erstmaligen Zertifikatsanträgen zu verwenden.

3. Der private Schlüssel einer Dokumentenprüfinstanz DV ist zum Signieren von Zertifikaten von verwalteten Prüfinstanzen IS zu verwenden.

4. Das Zertifikat der Dokumentenprüfinstanz ist zur Überprüfung der Signatur auf Zertifikaten von Kontrollinstanzen zu verwenden.

Der von der LI-CVCA verwaltete vertrauenswürdige Zertifizierungspfad setzt sich aus folgenden Zertifikaten zusammen:

1. selbstsigniertes LI-CVCA-Zertifikat;

2. optional: ein oder mehrere LI-CVCA-Linkzertifikate;

3. ein von der LI-CVCA signiertes DV-Zertifikat;

4. ein von einer DVCA signiertes IS Zertifikat

Bei den einzelnen Vertrauenspartnern setzt sich der vertrauenswürdige Zertifizierungspfad wie folgt zusammen:

1. Dokumentenprüfinstanz (DV):

    a. LI-CVCA-Zertifikat und F-CVCA-Zertifikat des berechtigten Mitgliedstaats;

2. Kontrollinstanz (IS):

    a. Fremdes DV-Zertifikat (F-DVCA)

    b. LI-CVCA-Zertifikat und F-CVCA-Zertifikat des berechtigten Mitgliedstaats;

3. Maschinenlesbare Reisedokumente und Aufenthaltsausweise:

    a. IS-Zertifikat des berechtigten Mitgliedstaats,

    b. DVCA-Zertifikat des berechtigten Mitgliedstaats,

    c. LI-CVCA-Zertifikat und möglicherweise das Linkzertifikat sowie das entsprechende F-CVCA-Zertifikat.

Anmerkung: Der Begriff „national“ bezieht sich hier auf den Mitgliedstaat, der die Dokumentenprüfinstanz bzw. die Kontrollinstanz betreibt bzw. das maschinenlesbare Reisedokument bzw. Aufenthaltsausweis ausgestellt hat.

„Berechtigter Mitgliedsstaat" bezeichnet einen Mitgliedsstaat der berechtigt ist Fingerabdruckdaten von einem Reisepass bzw. Aufenthaltsausweis, unter Verwendung eines DV-Zertifikates, das von der CVCA des ausstellenden Staates des Reisepass bzw. Aufenthaltsausweis signiert ist, auszulesen.

1.5 Administration dieses Dokumentes

Die Verwaltung dieses Dokuments obliegt und Ansprechpartner für Fragen und Anliegen zum vorliegenden Dokument ist:

Liechtensteinische Landesverwaltung (LLV)
Ausländer- und Passamt (APA)
Städtle 38
9490 Vaduz
Fürstentum Liechtenstein

Telefon: +423 236 61 41

1.6 Definitionen und Abkürzungen

Die in diesem Dokument verwendeten Schlüsselbegriffe „MUSS“ bzw. „MÜSSEN“, „DARF NICHT“ bzw. „DÜRFEN NICHT“, „ERFORDERLICH“, „SOLLTE(N)“, „SOLLTE(N) NICHT“, „EMPFOHLEN“, „KANN“ bzw. „KÖNNEN“ und „OPTIONAL“ sind in Anlehnung an die in englischer Sprache in [IETF RFC 2119] vorliegenden Begriffe auszulegen.

Ein „Mitgliedstaat“ ist ein Land, auf welche die Verordnung (EG) Nr. 2252/2004 anwendbar ist.

„Inländisch“ bedeutet: vom Fürstentum Liechtenstein.

„Ausländisch“ bedeutet: von einem anderen Teilnehmerstaat der EAC-PKI.

Ein „gültiger Schlüssel“ ist ein Schlüssel, bei dem der gegenwärtige Zeitpunkt in den Gültigkeitszeitraum des entsprechenden Abonnentenzertifikats fällt und letzteres nicht widerrufen worden ist.

Weitere Begriffsbestimmungen und Abkürzungen dieses Textes werden in *ANLAGE A.1 BEGRIFFSBESTIMMUNGEN* und *ANLAGE A.2 ABKÜRZUNGEN* erläutert.

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

2. VERÖFFENTLICHUNGEN UND VERZEICHNISDIENST

2.1 Verzeichnisdienste

Unter folgender Website sind das gegenständliche Dokument sowie alle weiteren für den Betrieb der LI-CVCA im Kontext der EAC-PKI notwendigen Informationen über die EAC-PKI zu veröffentlichen und nach Änderung möglichst zeitnahe zu aktualisieren. Dabei ist, durch den Betreiber des Verzeichnisses ein angemessener Schutz der Integrität der veröffentlichten Informationen sicherzustellen.

ePass	http://www.llv.li/amtsstellen/llv-apa-reisepass/llv-apa-epass/llv-apa-epass-datenschutz.htm
Aufenthaltsausweis	http://www.llv.li/amtsstellen/llv-apa-aufenthaltsausweise/llv-apa-schengenausweis-2.htm

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

3. IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG

3.1 Namen

Wie unter Abschnitt A.4.1 der [BSI TR EAC] festgelegt, wird das Zertifikatsattribut „Certification Authority Reference CAR“ zur Identifizierung des öffentlichen Schlüssels herangezogen, der für die Verifizierung der Signatur der CVCA oder des DV verwendet wird.

Die Certificate Authority Reference (CAR) eines ausgestellten Zertifikats MUSS mit der Certificate Holder Reference (CHR) des ausstellenden Zertifikats übereinstimmen.

Die „Certificate Holder Reference“ eines Zertifikatinhabers MUSS einen öffentlichen Schlüssel des Zertifikatinhabers angeben. Dabei MUSS es sich im Kontext der ausstellenden Zertifizierungsstelle um einen eindeutigen Bezeichner handeln.

Die Certificate Holder Reference MUSS aus folgenden miteinander verbundenen Elementen bestehen:

1. ALPHA-2-Ländercode (gemäß ISO 3166-1) des Landes des Zertifikatinhabers;
2. eine den Zertifikatinhaber repräsentierende Mnemonik;
3. eine laufende numerische oder alphanumerische Folgenummer.

HINWEIS: Es ist nicht garantiert, dass die Certificate Holder Reference (CHR) generell eindeutig ist.

Im Kontext der LI-CVCA sind folgende Bezeichnungen definiert:

1. LI-CVCA-Zertifikat
    a. Certification Authority Reference (CAR): “LICVCA” + Folgenummer; (z.B. LICVCA00001)
    b. Certificate Holder Reference CHR: “LICVCA” + Folgenummer
2. DV-Zertifikat
    a. Certification Authority Reference CAR: CHR des ausstellenden LI-CVCA-Zertifikats
    b. Certificate Holder Reference CHR: entsprechend der Konvention der nationalen DV
3. IS-Zertifikate:

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

a. Certification Authority Reference CAR: CHR des ausstellenden DVCA-Zertifikats

b. Certificate Holder Reference CHR: entsprechend der Konvention der nationalen IS

3.2 Identitätsüberprüfung bei Neuantrag

3.2.1 LI-CVCA

Für die LI-CVCA MUSS im Verzeichnis (siehe Abschnitt 2.1) deutlich angegeben werden, wer für die Authentisierung und die Definition des Names (bzw. des CHR) der nationalen Zertifizierungsstelle zuständig ist.

3.2.2 Kommunikation zwischen CVCA und CVCA

Um Anträge von Dokumentenprüfinstanzen (F-DVCAs) prüfen zu können, muss sich die LI-CVCA die Identität der Dokumentenprüfinstanz von der F-CVCA des betreffenden Mitgliedstaats bestätigen lassen können. Daher MUSS die LI-CVCA die Identität der anderen CVCAs (F-CVCAs) überprüfen, bevor die Dokumentenprüfinstanzen Zertifikatsanträge einreichen.

Die Validierung der Identität der einzelnen CVCAs erfolgt unter Aufsicht der Europäischen Kommission. Die LI-CVCA hat der Europäischen Kommission zwecks Verteilung an die anderen teilnehmenden CVCAs folgende Informationen zu übermitteln:

a) Die nationalen Zertifikatregeln;

b) den öffentlichen Teil der Zertifizierungspraxiserklärung der Zertifizierungsstelle (falls eine solche Erklärung existiert);

c) eine Kopie des öffentlichen Schlüssels der CVCA.

Falls sich die obigen Informationen ändern, MUSS die LI-CVCAs die aktualisierten Informationen an die Europäische Kommission zwecks Verteilung an die anderen teilnehmenden CVCAs übermitteln.

3.2.3 Kommunikation zwischen DV und CVCA

Die erstmalige Übermittlung von Registrierungsinformationen durch eine DV an die LI-CVCA MUSS über einen vereinbarten vertrauenswürdigen Kanal erfolgen.

Die DV MUSS folgende Registrierungsinformationen übermitteln:

1. den öffentlichen Teil der Zertifizierungspraxiserklärung der DV;

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

2. die aktuelle Konformitätsbescheinigung über die Einhaltung der nationalen Zertifikatregeln durch die DV;

3. eine Liste der Organisationen, die von der DV zertifizierte Lesegeräte verwenden;

4. ein Zertifikatantrag gemäß Abschnitt A.4.2 der [BSI TR EAC]. Der Antrag MUSS eine äußere Signatur gemäß Abschnitt A.4.2.4 der [BSI TR EAC] enthalten, die von der übergeordneten CVCA der DVs unterzeichnet ist.

Die DV SOLLTE der LI-CVCA folgende Registrierungsinformationen übermitteln:

1. Eine Ansprechperson der DV zur Verifikation der Zertifikatsanträge und für die Rückübermittlung von Statusinformationen zu den Anträgen.

Im Falle einer nicht unwesentlichen Änderung einer der obigen Informationen MUSS die DV die betreffenden Angaben an die LI-CVCA übermitteln, damit diese prüfen kann, ob eine neue Erstüberprüfung der Identität erforderlich ist.

3.2.4 Kommunikation zwischen IS und DV

Dokumentenprüfinstanzen MÜSSEN über ein eigenes Verfahren zur Identifizierung eines authentisierten Lesegeräts verfügen. Bei der Generierung des Initialschlüsselmaterials und der Erstellung des Zertifikatantrags MÜSSEN von der DV ermächtigte Mitarbeiter anwesend sein.

3.3 Identifizierung und Authentifizierung bei einer Zertifikatserneuerung

Dafür gilt die Spezifikation [BSI TR EAC], Absatz A.4.2.

3.3.1 Kommunikation zwischen DV und CVCA

Die LI-CVCA MUSS die Gültigkeit des Antrags prüfen, indem sie die Bestätigung dafür einholt, dass

1. der Zertifikatsantrag Abschnitt A.4.2 der [BSI TR EAC] entspricht;

2. die F-CVCA des DV-Mitgliedstaats die Dokumentenprüfinstanz nach wie vor als zulässig führt;

3. die Konformitätsbescheinigung der Dokumentenprüfinstanz noch gültig ist;

4. die äußere Signatur des Zertifikatsantrags mit einem gültigen Schlüssel eines von der LI-CVCA ausgestelltes Zertifikats der betreffenden DV erstellt wurde.

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

3.3.2 Kommunikation zwischen IS und DV

Der DV DARF ein Zertifikat erst ausstellen, wenn er die Bestätigung dafür eingeholt hat, dass

1. das Lesegerät noch als in Betrieb befindlich registriert ist;

2. das Lesegerät nicht als gestohlen oder vermisst gemeldet ist.

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

4. OPERATIVE ANFORDERUNGEN IN BEZUG AUF DEN LEBENSZYKLUS VON ZERTIFIKATEN

4.1 Zertifikatantrag

4.1.1 CVCA

Für die LI-CVCA MUSS im Verzeichnis (siehe Abschnitt 2.1) deutlich angegeben werden, welche Stelle für die Genehmigung zur Einrichtung einer CVCA zuständig ist.

4.1.2 Kommunikation zwischen DV und LI-CVCA

Im Anschluss an die erfolgreiche erste Identitätsüberprüfung gemäß Abschnitt 3.2.3 MUSS die Zertifikatbeantragung durch die Dokumentenprüfinstanz gemäß Abschnitt A.4.2 der [BSI TR EAC] (Certificate Requests) und Abschnitt 2.2.2 der [BSI TR EAC] (Document Verifiers) erfolgen.

4.1.3 Kommunikation zwischen IS und DV

Kontrollinstanzen KÖNNEN Zertifikatanträge nach erfolgreichem Abschluss der ersten Identitätsüberprüfung gemäß dem obigen Abschnitt 3.2.4 einreichen.

4.2 Bearbeitung von Zertifikatanträgen

4.2.1 Von einer CVCA für sich selbst ausgestellte Zertifikate

Die LI-CVCA DARF ein selbstsigniertes CVCA-Zertifikat oder ein Linkzertifikat für ein früheres Zertifikat NUR während der Schlüsselzeremonie ausstellen, die die gegenständlichen Zertifikatregeln erfüllen muss.

Die LI-CVCAs MUSS sich vergewissern, dass der Auftrag zur Erstellung eines Zertifikates autorisiert und gültig ist (siehe Abschnitt 4.1.1).

4.2.2 Von einer CVCA für eine DV ausgestellte Zertifikate

Die LI-CVCA DARF ein Zertifikat NUR für eine DV ausstellen, die ihre eigenen nationalen DV-Zertifikatregeln einhält, d.h. letztere muss mindestens in Übereinstimmung mit der [EU CP] stehen. Die (von staatlicher und von nicht staatlicher Seite erfolgende) Verwendung von Fingerabdruckdaten im Reisedokument und in den Aufenthaltsausweisen muss nach Maßgabe von Abschnitt 1.4 dieses Dokuments erfolgen.

Die LI-CVCA MUSS sich vergewissern, dass ein Zertifikatantrag gültig ist.

Die LI-CVCA MUSS den Erhalt eines Zertifikatantrags bestätigen.

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

Die LI-CVCA MUSS den Zertifikatantrag gemäß Abschnitt 5.5.2 der Entscheidung K(2006) 2909 der Kommission vom 28.6.2006 binnen 72 Stunden bearbeiten.

Im Kontext der LI-CVCA gelten sind diese 72 Stunden (drei Werktage) aber nur im Zeitraum von Montag 7h bis Freitag 19h einer Arbeitswoche, sofern die in diesem Zeitraum liegenden Werktage nicht gesetzliche Feiertage des Fürstentums Liechtenstein oder der Republik Österreich sind.[2]

Falls die LI-CVCA für einen diese Frist überschreitenden Zeitraum außer Betrieb ist, MÜSSEN alle angeschlossenen DVs spätestens sieben Tage vor Aussetzung des Betriebs bzw., bei einem unvorhergesehen Betriebsausfall, so rasch wie möglich in Kenntnis gesetzt werden.

4.2.3 Von einer DV für ein Lesegerät ausgestellte Zertifikate

Eine DV DARF ein Zertifikat NUR für eine Kontrollinstanz ausstellen, die die nationalen IS-Zertifikatregeln einhält und die Zertifikate gemäß Abschnitt 1.4 dieses Dokuments verwendet.

DVs MÜSSEN sich vor der Ausstellung eines Zertifikats vergewissern, dass der Zertifikatantrag gültig ist.

4.3 Zertifikatsausstellung

4.3.1 Von einer CVCA ausgestellte Zertifikate

Die LI-CVCA MUSS geeignete Maßnahmen gegen die Fälschung von Zertifikaten ergreifen und dafür Sorge tragen, dass die Zertifikatausstellungsverfahren auf sichere Weise mit der entsprechenden Registrierung, Zertifikaterneuerung oder Schlüsselerneuerung (einschließlich Bereitstellung eines subjektgenerierten öffentlichen Schlüssels) verbunden werden.

Die Erstellung und Ausfertigung der Zertifikate MUSS in Übereinstimmung mit Abschnitt A.4 der [BSI TR EAC] („CV Certificates“) erfolgen.

4.3.2 Von einer DV ausgestellte Zertifikate

DVs MÜSSEN Zertifikate auf sichere Weise ausstellen, damit deren Authentizität gewahrt bleibt.

DVs MÜSSEN geeignete Maßnahmen gegen die Fälschung von Zertifikaten ergreifen und dafür Sorge tragen, dass die Zertifikatausstellungsverfahren auf sichere Weise mit der ent-

[2] D.h. Ein Antrag der am Freitag um 15h bei der LI-CVRA einlangt und bestätigt wird hat am darauf folgenden Montag noch 68 Stunden Restlaufzeit.

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

sprechenden Registrierung, Zertifikaterneuerung oder Schlüsselerneuerung (einschließlich Bereitstellung eines subjektgenerierten öffentlichen Schlüssels) verbunden werden.

Die Erstellung und Ausfertigung der Zertifikate MUSS in Übereinstimmung mit Abschnitt A.4 der [BSI TR EAC] („CV Certificates“) erfolgen.

4.4 Zertifikatsakzeptanz

Von der LI-CVCA selbstsignierte Zertifikate MÜSSEN nach ihrer Erstellung am Ende der Schlüsselimportzeremonie von der für die LI-CVCA zuständigen Stelle angenommen werden.

Bei Dokumentenprüf- oder Kontrollinstanzen GILT der Erhalt eines Zertifikats als dessen Annahme.

4.5 Verwendung des Schlüsselpaares und des Zertifikats

Die LI-CVCA, Dokumentenprüf- und Kontrollinstanzen MÜSSEN folgende Anforderungen erfüllen:

1. Sie müssen sicherstellen, dass insbesondere im Hinblick auf die Registrierung genaue und vollständige Informationen gemäß den Anforderungen dieser, und der Regeln der [EU CP] an die CVCA bzw. DV übermittelt werden.

2. Das Schlüsselpaar darf nur im Rahmen der durch diese Zertifikatregeln festgelegten Grenzen verwendet werden.

3. Sie müssen sicherstellen, dass der private Schlüssel nicht ohne Berechtigung verwendet wird.

4. Die Schlüsselgenerierung muss nach Maßgabe der [BSI TR EAC] erfolgen.

5. Sie dürfen private Schlüssel nur für Signaturen bzw. Entschlüsselungen mittels eines in Abschnitt 6.2 beschriebenen sicheren Schlüsselschpeicher verwenden.

6. Sie müssen die LI-CVCA bzw. DV unverzüglich in Kenntnis setzen, falls vor Ablauf der auf dem Zertifikat angegebenen Gültigkeitsdauer Folgendes passiert:

   a) Ein privater Schlüssel wurde verloren, gestohlen oder es bestehet der begründete Verdacht dass er kompromittiert wurde; oder

   b) infolge der Kompromittierung von Aktivierungsdaten (z.B. des PIN-Codes) oder aus anderen Gründen ist die Kontrolle über den privaten Schlüssel verloren gegangen oder

   c) Ungenauigkeiten oder Änderungen des dem Zertifikatabonnenten oder Betroffenen mitgeteilten Zertifikatinhalts;

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

7. Nach einer Kompromittierung ist die Verwendung eines privaten Schlüssels sofort und unwiderruflich zu beenden.

8. Falls mitgeteilt wird, dass der private Schlüssel der LI-CVCA oder einer LI-DVCA kompromittiert wurde, DÜRFEN die mit diesen privaten Schlüsseln signierten Zertifikate nicht mehr verwendet werden, und es MÜSSEN geeignete Maßnahmen ergriffen werden.

Die Verwendung von Schlüsselpaaren und Zertifikaten MUSS nach Maßgabe der vom Zertifikataussteller (CVCA oder DV) im Zertifikatsattribut *Certificate Holder Authorisation (CHA)* gemachten Angaben erfolgen.

Dokumentenprüf- und Kontrollinstanzen DÜRFEN den privaten Schlüssel für das erhaltene DV- bzw. IS-Zertifikat nur zu folgenden Zwecken verwenden:

1. für den in Abschnitt 1.4 („Zertifikatverwendung“) dieser Zertifikatregeln beschriebenen Zweck,

2. nach Maßgabe des Inhalts der ausgestellten Zertifikate.

4.6 Zertifikatserneuerung unter Beibehaltung des alten Schlüssels (Re-Zertifizierung)

Eine Zertifikatsverlängerung ist nicht zugelassen.

4.7 Schlüssel- und Zertifikatserneuerung (Re-Key)

Ein Zertifikatschlüssel DARF nur ausgetauscht werden, wenn

a) das DV oder das IS-Zertifikat abläuft;

b) ein DV-Zertifikat der Dokumentenprüfinstanz widerrufen wird;

c) ein IS-Schlüssel kompromittiert ist;

d) ein DV bzw. IS-Zertifikat aufgrund geänderter DV- bzw. IS-Attribute geändert werden muss.

Die LI-CVCA bzw. LI-DVCA MUSS sicherstellen, dass Anträge auf Zertifikate, die für eine zuvor registrierte DV bzw. IS ausgestellt wurden, korrekt und ordnungsgemäß autorisiert sind. Die LI-CVCA bzw. LI-DVCA

1. MUSS überprüfen, ob das Zertifikat, dessen Schlüssel ausgetauscht werden soll, existiert und gültig ist, und ob die Informationen, die für die Überprüfung der DV bzw. IS Identität und der Attribute verwendet werden, noch stimmen;

2. MUSS überprüfen ob

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

a) die kryptografische Sicherheit des Signaturschlüssels für die Gültigkeitsdauer des neuen Zertifikats ausreicht und

b) die Signatur des Betroffenen auf dem Antrag gültig ist und

c) keine Anzeichen auf Kompromittierung des für die Signatur des Betroffenen auf dem Antrag verwendete privaten Schlüssels bestehen

und darf nur nach positiver Prüfung ein neues Zertifikat ausstellen.

Die Ausstellung der Zertifikate MUSS nach Maßgabe des Abschnitts 4.3 („Zertifikatsausstellung“) erfolgen.

Wenn ein DV-Zertifikat abläuft (siehe Abschnitt 4.7 Buchstabe a), MUSS nach Maßgabe von Abschnitt A.4.2 der [BSI TR EAC] („Certificate Requests“) verfahren werden.

Wenn ein DV-Zertifikat widerrufen wird, abläuft oder geändert werden muss (siehe die Abschnitt 4.7 Buchstaben b, c und d), erfolgt ein Schlüsselaustausch wie bei der erstmaligen Beantragung eines DV-Zertifikats durch eine Dokumentenprüfinstanz.

Wenn ein privater IS-Schlüssel kompromittiert wurde oder abläuft, erfolgt ein Schlüsselaustausch wie bei der erstmaligen Beantragung eines IS-Zertifikats durch eine Kontrollinstanz.

4.8 Änderung des Zertifikats

Dieser Punkt wird in Abschnitt 4.7 („Schlüssel- und Zertifikatserneuerung (Re-Key)“) dieses Dokuments erläutert.

4.9 Widerruf und Sperrung / Suspendierung von Zertifikaten

Ein technisches System für Widerruf und Sperre von Zertifikaten gemäß [BSI TR EAC] und [EU CP] ist nicht vorgesehen.

Die LI-CVCA MUSS eine Liste von nicht mehr gültigen F-CVCAs und F-DVCAs führen. Für Widerruf- und Sperranträgen MUSS die LI-CVCA sicherstellen, dass diese Anträge von authentifizierten Quellen stammen.

Siehe Abschnitt 5.7 („Wiederherstellung nach Kompromittierung oder Katastrophen“) dieses Dokuments.

4.10 Dienst zur Statusabfrage von Zertifikaten (OCSP)

Ein OCSP-Service ist nicht vorgesehen.

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

4.11 Beendigung des Vertragsverhältnisses

Eine formelle Beendigung des Vertragsverhältnisses zwischen Zertifikatshalter und Zertifikatsaussteller ist nicht vorgesehen.

4.12 Schlüsselhinterlegung und –wiederherstellung

Eine Hinterlegung von privaten Schlüsseln außerhalb der BRZ GMBH DARF NICHT durchgeführt werden.

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

5. INFRASTRUKTURELLE, ORGANISATORISCHE, PERSONELLE SICHERHEITSMASZNAHMEN

5.1 Infrastrukturelle Sicherheitsmaßnahmen

Die LI-CVCA und jede DV MUSS den Betrieb in einer gesicherten Umgebung gewährleisten. Dies umfasst:

a) Standort und Aufbau:
CVCA bzw. DV sind in einem physisch geschützten Bereich untergebracht.

b) Zugang:
Der Zugang zur CVCA bzw. DV ist beschränkt und wird überwacht. Nur Zugangsberechtigte haben Zugang zur CVCA bzw. DV-Umgebung.

c) Datenspeicherung:
Die Datenspeicher sind gegen unbefugte oder unbeabsichtigte Nutzung und Offenlegung, unbefugten oder unbeabsichtigten Zugriff sowie Beschädigung durch Personen oder andere Gefahren (z. B. Feuer, Wasserschäden) geschützt.

d) Abfallbeseitigung:
Abfallbeseitigungsverfahren werden eingeführt, um die unbefugte Nutzung, Offenlegung sensibler Daten und den unbefugten Zugriff zu verhindern.

e) Externe Datensicherung:
Es MUSS eine externe Einrichtung für die Sicherung wichtiger Daten vorgesehen werden.

5.2 Organisatorische Sicherheitsmaßnahmen

Es MÜSSEN verfahrenstechnische Kontrollen vorgesehen werden; insbesondere sind kritische Aufgaben nach dem Vier-Augen-Prinzip auf zwei Mitarbeiter zu verteilen.

Bei CVCA, DV und Kontrollinstanz MUSS gewährleistet sein, dass nur ordnungs-gemäß ermächtigte Personen und nur, wenn nötig („need to know“-Grundsatz), Zugang zu Geräten der EAC-PKI haben. Folgende Anforderungen sind zu beachten:

a) Es MÜSSEN Maßnahmen (z. B. Firewalls) zur Abschottung der Netzwerkdomänen der CVCA/DVCA gegen externe Netzwerkdomänen, auf die Dritte Zugriff haben, vorgesehen werden.

b) Sensible Daten MÜSSEN gegen unbefugte(n) Zugriff und Änderung geschützt werden.

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

c) Sensible Daten MÜSSEN bei der Übertragung über ungesicherte Netze geschützt werden (z. B. durch Verschlüsselung und einen Mechanismus zur Gewährleistung der Datenunversehrtheit).

d) Bei CVCA, DV und Kontrollinstanz MUSS eine wirksame Verwaltung des Zugangs von Nutzern (darunter Betreiber, Systemverwalter und sonstige Nutzer, die direkten Zugang zum System haben) gewährleistet sein, damit die Systemsicherheit, darunter die Verwaltung der Benutzerkonten, Überprüfungen und die unverzügliche Änderung der Zugangsregelung oder Sperrung von Personen sichergestellt sind.

e) Bei CVCA, DV und Kontrollinstanz MUSS gewährleistet sein, dass nur Befugte Zugang zu Informationen und Funktionen des Anwendungssystems erhalten und dass die EAC-PKI-Systeme ausreichende Rechnersicherheitskontrollen für die Trennung von vertrauenswürdigen Benutzerrollen (trusted roles) vorsehen, darunter die Trennung der Funktionen der Sicherheitsbeauftragten und der Betreiber. Insbesondere ist die Nutzung von Systemwartungsprogrammen zu beschränken und streng zu überwachen. Der Zugang MUSS auf die Systemteile beschränkt werden, die für die dem Nutzer zugeteilte(n) Benutzerrolle(n) nötig sind.

f) Das CVCA , DV und IS Personal MUSS eindeutig identifiziert und authentisiert werden, bevor EAC-PKI-Anwendungen für die Zertifikatverwaltung oder den Zugang zu maschinenlesbaren Reisedokumenten verwendet werden können.

g) Das CVCA , DV und IS Personal MUSS Rechenschaft über seine Tätigkeiten ablegen, indem es beispielsweise über Ereignisse Protokoll führt (siehe Abschnitt 5.4).

h) Es MUSS dafür Sorge getragen werden, dass bei der Wiederverwendung von Datenträgern keine sensiblen Daten (z.B. gelöschte Dateien) durch Zugriff unbefugter Nutzer offengelegt werden können.

5.3 Personelle Sicherheitsmaßnahmen

Sämtliche EAC-PKI-Systeme, also LI-CVCA, DV und IS-Systeme, MÜSSEN von qualifiziertem und erfahrenem Personal betrieben werden. Im Einzelnen sind folgende Anforderungen zu erfüllen:

a) Die LI-CVCA, die DVs und Kontrollinstanzen MÜSSEN für die verschiedenen Funktionen über ausreichendes Personal verfügen, das über das Fachwissen, die Erfahrung und die Qualifikation verfügt, um die jeweiligen Dienste erbringen zu können.

b) Das Personal MUSS einer innerstaatlichen Sicherheitsüberprüfung unterzogen werden; die Sicherheitsstufe richtet sich nach den jeweiligen Benutzerrollen.

c) Verstöße gegen die Verfahrensvorschriften der LI-CVCA, die DV oder IS MÜSSEN mit entsprechenden Disziplinarmaßnahmen geahndet werden.

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

d) Sicherheitsrollen und entsprechende Zuständigkeiten, die in den Sicherheitsbestimmungen des Systems festgelegt sind, MÜSSEN in den Tätigkeitsbeschreibungen dokumentiert werden. Vertrauenswürdige Benutzerrollen, die für den Betrieb des Systems von grundlegender Bedeutung sind, MÜSSEN deutlich angegeben werden.

e) Für das gesamte Personal (fest angestellte und nicht fest angestellte Mitarbeiter) MÜSSEN Tätigkeitsbeschreibungen erstellt werden, die auf den Prinzipien der Aufgabentrennung und der möglichst eingeschränkten Zugriffsrechte beruhen.

f) Die für das Personal maßgeblichen Verwaltungsverfahren und –bestimmungen MÜSSEN in Übereinstimmung mit den in Ziffer 5.2 beschriebenen verfahrenstechnischen Kontrollen stehen.

g) Mit vertrauenswürdigen Benutzerrollen befasste LI-CVCA, die DV und IS Mitarbeiter DÜRFEN sich in keinem Interessenkonflikt befinden, der die Sicherheit des Systems beeinträchtigen könnte.

h) Mitarbeitern, die Zugang zu privaten Schlüsseln in der EAC-PKI haben, MÜSSEN von leitenden Bediensteten in aller Form vertrauenswürdige Benutzerrollen zugewiesen werden.

i) Vertrauenswürdige Benutzerrollen oder Leitungsaufgaben bei der LI-CVCA, den DVs und Kontrollinstanzen DÜRFEN NICHT Personen übertragen werden, die bekanntlich wegen eines schweren Verbrechens oder einer anderen Straftat, die sie für die Position ungeeignet macht, strafrechtlich verurteilt wurden. Das Personal DARF KEINEN Zugang zu vertrauenswürdigen Funktionen erhalten, bevor nicht die erforderlichen Überprüfungen abgeschlossen sind.

5.4 Überwachung / Protokollierung

CVCAs, DVs und Kontrollinstanzen MÜSSEN geeignete Protokollierungsverfahren anwenden, damit die ordnungsgemäße und nicht ordnungsgemäße Verwendung ihres Systems in der EAC-PKI untersucht und nachvollzogen werden kann.

Bei der LI-CVCA, DVs und Kontrollinstanzen MUSS sichergestellt werden, dass sämtliche einschlägigen Informationen über ein Zertifikat über einen angemessenen Zeitraum aufbewahrt werden, damit zumindest die in Abschnitt 8 *KONFORMITÄTSPRÜFUNG* (Compliance Audit, Assessments) genannten Überwachungsanforderungen erfüllt werden.

Die LI-CVCA und die DVs MÜSSEN sicherstellen, dass

a) die Vertraulichkeit und die Unversehrtheit der aktuellen und der archivierten Zertifikatprotokolle gewährleistet ist;

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

b) die Zertifikatprotokolle unter Wahrung ihrer Vertraulichkeit vollständig archiviert werden;

c) der genaue Zeitpunkt von Vorkommnissen, die die Umgebung, die Schlüssel und die Zertifikatverwaltung betreffen, aufgezeichnet wird;

d) sämtliche den Lebenszyklus von Schlüsseln betreffende Vorkommnisse protokolliert werden;

e) sämtliche den Lebenszyklus von Zertifikaten betreffende Vorkommnisse protokolliert werden;

f) sämtliche die Registrierung betreffende Vorkommnisse protokolliert werden;

g) sämtliche Anträge auf Widerruf, diesbezügliche Berichte und die betreffenden Folgemaßnahmen protokolliert werden;

h) die zu protokollierenden Vorkommnisse und Daten dokumentiert werden;

i) Vorkommnisse so protokolliert werden, dass die Protokolle während des Zeitraums, in dem sie aufbewahrt werden MÜSSEN, nicht ohne weiteres gelöscht oder vernichtet werden können (außer im Fall der Übertragung auf einen dauerhafteren Datenträger).

Für Protokolle von IS gilt Folgendes:

a) Über die Schlüsselverwaltung im Lesegerät MUSS so Protokoll geführt werden, dass die jeweilige DV einen Missbrauch des Systems entdecken und die geeigneten Gegenmaßnahmen einleiten kann.

b) Die Protokolle sind gegen Änderung oder Löschung zu schützen.

c) Die Aufzeichnungen MÜSSEN mindestens 3 Monate aufbewahrt werden, damit Prüfer einen etwaigen Missbrauch bestätigen können.

5.5 Archivierung

Die LI-CVCA, die DVs und Kontrollinstanzen MÜSSEN für geeignete Datenarchivierungsverfahren für das jeweilige System in der EAC-PKI sorgen. Die Verfahren MÜSSEN die Unversehrtheit, Authentizität und Vertraulichkeit der Daten sicherstellen.

Die Archive MÜSSEN so angelegt werden, dass sie während des Zeitraums, in dem sie vorhanden sein müssen, nicht gelöscht oder vernichtet werden können (außer im Fall der Übertragung auf einen dauerhafteren Datenträger).

Zugang zu den Archiven DARF nur befugten Betreibern gewährt werden.

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

Wenn die Daten nicht über den gesamten Aufbewahrungszeitraum auf den ursprünglichen Datenträgern gespeichert werden können, legt die Archivierungsstelle ein Verfahren für die regelmäßige Übertragung der archivierten Daten auf andere Datenträger fest.

Kontrollinstanzen DÜRFEN KEINE Fingerabdruckdaten aus maschinenlesbaren Reisedokumenten protokollieren oder übermitteln. Derartige Daten MÜSSEN nach dem Abgleich der Fingerabdrücke der betreffenden Person mit den Fingerabdruckdaten auf dem Reisedokument unverzüglich gelöscht werden.

Archive MÜSSEN so lange aufbewahrt werden, solange rechtliche Nachweise gemäß den geltenden Vorschriften der LLV erbracht werden müssen.

5.6 Schlüsselwechsel einer Zertifizierungsstelle

Die LI-CVCA und die DVs MÜSSEN sicherstellen, dass die Schlüssel unter kontrollierten Bedingungen nach den in Abschnitt 5.2 Organisatorische Sicherheitsmaßnahmen festgelegten Verfahren erzeugt werden.

Die LI-CVCA MUSS vollständige selbst-signierte und Link-Zertifikate ausstellen.

5.7 Kompromittierung und Wiederherstellung (disaster recovery)

Die LI-CVCA MUSS angemessene Maßnahmen zur Gewährleistung der Betriebskontinuität treffen, darunter:

a) Maßnahmen zur Verminderung der Auswirkungen von Stromversorgungsstörungen;

b) Maßnahmen zur Verminderung der Auswirkungen von Ereignissen wie Überschwemmungen oder Feuer;

c) Maßnahmen zur Verminderung der Auswirkungen des Ausfalls wichtiger Mitarbeiter.

5.7.1 Verfahren bei Vorfällen und Datenkompromittierung

Im Katastrophenfall, beispielsweise bei Kompromittierung des privaten Schlüssels eines Teilnehmers, MUSS sichergestellt sein, dass die LI-CVCA, die DVs und Kontrollinstanzen so schnell wie möglich den Betrieb wiederaufnehmen. Im Einzelnen sind folgende Anforderungen zu erfüllen:

1. LI-CVCA, DVs und Kontrollinstanzen MÜSSEN über einen festgelegten Kontinuitätsplan verfügen, auf den im Katastrophenfall zurückgegriffen wird (siehe auch Abschnitt 5.7.4).

2. Die für die Wiederaufnahme des Betriebs der LI-CVCA und der DV nötigen Systemdaten dieser Instanzen MÜSSEN gesichert und an einem sicheren Ort aufbewahrt

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

werden, damit die LI-CVCA und die DV bei Zwischenfällen bzw. Katastrophen den Betrieb schnell wiederaufnehmen können.

3. Die Sicherung und die Wiederherstellung gehören zu den vertrauenswürdigen Rollen und MÜSSEN als solche von dem dafür zuständigen Personal vorgenommen werden.

4. Der Betriebskontinuitätsplan (bzw. Datenwiederherstellungsplan) der EAC-PKI MUSS die Kompromittierung oder vermutete Kompromittierung eines privaten Schlüssels als Katastrophenfall behandeln, und es MÜSSEN entsprechende Verfahren vorgesehen sein (siehe auch Abschnitt 5.7.3).

5.7.2 Beschädigung von Rechnern, Software und/oder Daten

Ist der private Schlüssel der LI-CVCA aus nicht kritischen Gründen unbrauchbar geworden, greift das in Abschnitt 5.6 beschriebene Verfahren.

5.7.3 Verfahren bei Kompromittierung privater Schlüssel

Falls der private Schlüssel einer DV oder einer Kontrollinstanz kompromittiert oder missbraucht wurde, MUSS die Dokumentenprüfinstanz alle CVCAs, die Zertifikate für sie ausgestellt haben, umgehend informieren.

Ist ein Kontrollinstanz unauffindbar oder wurde es gestohlen, MUSS die zuständige Dokumentenprüfinstanz so schnell wie möglich (d.h. spätestens beim nächsten Zertifikatantrag) alle CVCAs, die für sie Zertifikate ausgestellt haben, von dem Zwischenfall in Kenntnis setzen.

Jedes Land SOLLTE allen anderen Ländern mitteilen, in welcher Form die beantragten Informationen zur Verfügung gestellt werden.

5.7.4 Gewährleistung der Betriebskontinuität nach einer Katastrophe

Die LI-CVCA MUSS über einen aktuellen Betriebskontinuitätsplan verfügen, in dem dargelegt ist, wie sie ihre Dienste bei den Normalbetrieb beeinträchtigenden Vorkommnissen aufrechterhält.

5.8 Einstellung des CVCA- oder DV-Betriebs

Bei der Einstellung ihres Betriebs MUSS die LI-CVCA

1. sämtliche CVCAs, bei denen sie registriert ist, in Kenntnis setzen,

2. sämtlichen CVCAs, bei denen sie registriert ist, mitteilen, welche andere CVCA gegebenenfalls die Zuständigkeit für nationale DVs übernimmt,

3. sämtliche DVs, für die sie Zertifikate ausstellt, in Kenntnis setzen,

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

4. sämtlichen DVs, für die sie Zertifikate ausstellt, mitteilen, welche andere CVCA gegebenenfalls an ihrer Stelle Zertifikate ausstellt.

5. Jede stellvertretende CVCA MUSS Zertifikate für MRTDs und Aufenthalts-ausweise erteilen, die von der ursprünglichen CVCA ausgestellt wurden.

6. Die LI-CVCA MUSS ihre privaten Schlüssel zerstören oder auf deren weitere Verwendung verzichten.

Wenn eine LI-DV den Betrieb einstellt, MUSS diese Instanz die LI-CVCA in Kenntnis setzen; diese informiert daraufhin alle CVCAs, die für die Dokumentenprüfinstanz Zertifikate ausstellen.

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

6. TECHNISCHE SICHERHEITSMASZNAHMEN

6.1 Erzeugung von Schlüsselpaaren

Die LI-CVCA und die DVs MÜSSEN sicherstellen, dass die Schlüssel der Zertifizierungsstelle unter kontrollierten Bedingungen nach den in Abschnitt 5 *INFRASTRUKTURELLE, ORGANISATORISCHE, PERSONELLE SICHERHEITSMASZNAHMEN* festgelegten Verfahren erzeugt werden.

Die Schlüssel MÜSSEN mit einem vertrauenswürdigen Gerät erzeugt werden, das die Anforderungen nach *ANLAGE B.1 ANFORDERUNGEN AN ZERTIFIZIERUNGSSTELLEN* erfüllt.

Bevor der Signierschlüssel der LI-CVCA oder einer DV ungültig wird, MUSS die LI-CVCA bzw. die DV ein neues Schlüsselpaar für die Signatur von Zertifikaten erzeugen und die nötigen Vorkehrungen treffen, um eine Störung des Betriebs der LI-CVCA bzw. der DV oder von Lesegeräten, die auf den Schlüssel angewiesen sind, zu verhindern. Der neue Schlüssel MUSS gemäß der [BSI TR EAC] und diesen Regeln erzeugt und verteilt werden.

Die LI-CVCA und die DVs MÜSSEN die Prüfbarkeit auf Integrität und Authentizität ihrer öffentlichen Schlüssel und der dazugehörigen Parameter bei der Verteilung an die Dokumentenprüf- und Kontrollinstanzen sicherstellen.

6.2 Schutz privater Schlüssel und Einsatz kryptographischer Module

Die privaten Signaturschlüssel MÜSSEN in einem vertrauenswürdigen System aufbewahrt und verwendet werden, das die Anforderungen nach *ANLAGE B.1 ANFORDERUNGEN AN ZERTIFIZIERUNGSSTELLEN* erfüllt.

Die LI-CVCA MUSS technische und sonstige Verfahren anwenden, die die Erteilung individueller Berechtigungen an vertrauenswürdige Einzelpersonen beinhalten, die sensible Operationen (wie Erzeugung, Backup, Wiederherstellung, Vernichtung und Verwendung) mit dem privaten Schlüssel der LI-CVCA durchführen.

Die DVs MÜSSEN technische und sonstige Verfahren anwenden, die die Erteilung individueller Berechtigungen an vertrauenswürdige Einzelpersonen beinhalten, die sensible Operationen (wie Erzeugung, Backup, Wiederherstellung und Vernichtung) mit dem DV-Schlüssel durchführen. Die DV muss die vertrauenswürdigen Rollen mit ihrem Hardware-Sicherheitsmodul authentisieren, um die Verwendung des DV-Schlüssels zuzulassen.

Operationen mit dem IS-Schlüssel (wie Erzeugung, Backup, Wiederherstellung, Vernichtung und Verwendung) DÜRFEN NUR von befugtem, mit dieser Benutzerrolle betrautem Personal durchgeführt werden.

Außerhalb des Signaturerzeugungsgeräts MÜSSEN private Signaturschlüssel so geschützt werden, dass das gleiche Sicherheitsniveau gewährleistet ist wie innerhalb des Signaturerzeugungsgeräts.

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

Werden private Schlüssel durch ein Backup gesichert, DÜRFEN sie nur von befugtem, mit dieser Benutzerrolle betrautem Personal abgelegt und wiederbeschafft werden, wobei mindestens eine doppelte Kontrolle in einer physisch gesicherten Umgebung durchzuführen ist. Die Zahl der für diese Aufgaben zugelassenen Mitarbeiter SOLLTE so gering wie möglich gehalten werden.

Für Sicherungskopien der privaten Signaturschlüssel MÜSSEN mindestens die gleichen strengen Sicherheitsanforderungen gelten wie für die in Verwendung befindlichen Schlüssel.

Wenn Schlüssel in einem speziellen Hardwaremodul für die Schlüsselverwaltung abgelegt werden, MUSS durch Zugriffskontrollen sichergestellt werden, dass die Schlüssel außerhalb des Hardwaremoduls nicht zugänglich sind.

Private Signaturschlüssel DÜRFEN NICHT nach Ende ihres Lebenszyklus verwendet werden, und sämtliche Kopien des Schlüssels MÜSSEN am Ende ihrer Lebensdauer vernichtet oder unbrauchbar gemacht werden.

Die Sicherheit von Verschlüsselungsgeräten MUSS während ihres gesamten Lebenszyklus sichergestellt sein; insbesondere ist dafür Sorge zu tragen, dass die Verschlüsselungshardware für die Signatur bzw. den Widerruf von Zertifikaten während des Transports oder der Aufbewahrung nicht manipuliert werden kann, im Betrieb ordnungsgemäß funktioniert und gespeicherte private Schlüssel bei der Ausmusterung des Geräts vernichtet werden.

6.3 Weitere Aspekte des Schlüsselmanagements

Die Gültigkeitsdauer gemäß Ziffer 5.5.1 der Entscheidung K(2006) 2909 der Kommission vom 28.06.2006 ist:

Stelle	Mindestgültigkeitsdauer	Höchstgültigkeitsdauer
LI-CVCA	6 Monate	3 Jahre
LI-DVCA	2 Wochen	3 Monate
LI-IS	1 Tag	1 Monat

6.4 Aktivierungsdaten

Die Anforderungen für Aktivierungsdaten SOLLTEN auf der Grundlage einer Risikoanalyse von der Dokumentenprüfinstanz selbst festgelegt werden.

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

Eine Entsperrung der Aktivierungsdaten ist MÖGLICH; das von den Aktivierungsdateien gebotene Sicherheitsniveau MUSS dabei jedoch bestehen bleiben.

6.5 Sicherheitsmaßnahmen für Computer

Die LI-CVCA, die DVs und Kontrollinstanzen MÜSSEN die Computersicherheitskontrollverfahren nach Abschnitt 5 *INFRASTRUKTURELLE, ORGANISATORISCHE, PERSONELLE SICHERHEITSMASZNAHMEN* einhalten.

Die LI-CVCA, die DV und IS-Komponenten KÖNNEN folgende Funktionen ein-schließen:

1. vorgeschriebene Verwendung authentisierter Logins für vertrauenswürdige Rollen;
2. durch den Benutzer bestimmbare Zugriffskontrolle;
3. Sicherheitsaudit (Unversehrtheitsschutz);
4. Verbot der Wiederverwendung;
5. vorgeschriebene Verschlüsselung für die Sicherheit bei Abfragen und der Datenbank;
6. vorgeschriebene Verwendung eines vertrauenswürdigen Pfades für die Identifizierung und Authentisierung;
7. Domänenisolierung für Prozesse;
8. Selbstschutz des Betriebssystems.

6.6 Sicherheitsmaßnahmen im Lebenszyklus

Von der LI-CVCA, den DVs und IS verwendete vertrauenswürdige Geräte MÜSSEN gegen Änderungen geschützt werden.

Bei der Planung und Festlegung der Anforderungen eines CVCA, DV oder IS-Systementwicklungsprojekts, das sich auf die vertrauenswürdigen Systeme oder Produkte auswirkt, MÜSSEN die Sicherheitsanforderungen analysiert werden, um sicherzustellen, dass die IT-Systeme sicher ausgelegt werden.

Es MÜSSEN Änderungssteuerungsverfahren (Change Control) vorgesehen, dokumentiert und bei jedweden Aktualisierungen, Änderungen und Notfallsoftwarereparaturen der gesamten CVCA, DV bzw. IS-Betriebssoftware verwendet werden.

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

6.7 Sicherheitsmaßnahmen für das Netzwerk

Die LI-CVCA und die DVs MÜSSEN die Netzwerk-Sicherheitsmaßnahmen nach Abschnitt 5 *INFRASTRUKTURELLE, ORGANISATORISCHE, PERSONELLE SICHERHEITSMASZNAHMEN* einhalten.

6.8 Zeitstempel

Nicht anwendbar.

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

7. PROFILE FÜR ZERTIFIKATE, SPERRLISTEN UND ONLINESTATUSABFRAGEN

7.1 Zertifikatsprofil

Die Zertifikate entsprechen dem Zertifikatsprofil gemäß [BSI TR EAC] A.4.1 („CV Certificates“).

7.2 CRL-Profil

Nicht anwendbar.

7.3 OCSP-Profil

Nicht anwendbar.

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

8. KONFORMITÄTSPRÜFUNG (Compliance Audit, Assessments)

Eine DVCA kann die Übereinstimmung mit der [EU CP] nur dann geltend machen, wenn sie nachweisen kann, dass sie nationalen Zertifikatsregeln (CP) entspricht, die wiederum den Anforderungen der [EU CP] entspricht. Die LI-CVCA MUSS prüfen, ob die nationalen Zertifikatregeln der F-CVCAs den Anforderungen der [EU CP] genügen, bevor sie für Dokumentenprüfinstanzen des jeweiligen Landes, die nach Maßgabe dieser Regeln verfahren, Zertifikate ausstellen. Bei Streitfällen MUSS ein Schiedsverfahren unter Aufsicht der Europäischen Kommission erfolgen.

Die Dokumentenprüfinstanzen MÜSSEN eine unabhängige akkreditierte Einrichtung oder Organisation („Auditstelle“) auswählen, die die Dokumentenprüfinstanz auf der Grundlage deren nationalen Zertifikatregeln und ihrer Zertifizierungspraxiserklärung prüft.

Die Auditstelle MUSS von der Akkreditierungsstelle zu diesem Zweck akkreditiert sein. Bei dem Audit MUSS nicht nur geprüft werden, ob Sicherheitskontrollverfahren vorgesehen sind, sondern auch, ob sie in der Praxis eingehalten werden. Das gilt auch für den Betrieb und die Verwaltung von Kontrollinstanzen, die DV-Zertifikate erhalten. Audits MÜSSEN mindestens alle drei Jahre durchgeführt werden.

Die Auditstelle MUSS mindestens einmal jährlich eine Überprüfung durch einen Prüfer oder ein Prüferteam vornehmen, um die Einhaltung dieser Zertifikatregeln sicherzustellen.

Der Nachweis der Konformität mit den Zertifikatregeln wird nur anerkannt, wenn die Dokumentenprüfinstanz eine von der Auditstelle ausgestellte Konformitätsbescheinigung vorlegen kann, mit der die Einhaltung der nationalen Zertifikatregeln und somit auch dieser Zertifikatregeln durch die Dokumentenprüfinstanz bescheinigt wird.

Falls bei einem Audit festgestellt wird, dass eine Dokumentenprüfinstanz gegen deren nationalen Zertifikatregeln verstößt, MUSS diese sämtliche F-CVCAs, von denen sie Zertifikate erhält, in Kenntnis setzen.

Wenn die Konformität einer F-DVCA mit deren nationalen Zertifikatregeln nicht bescheinigt wird oder die Bescheinigung ungültig wird oder abläuft, DARF die LI-CVCA keine weiteren DV-Zertifikate für diese DV mehr ausstellen.

Es wird empfohlen, dass Dokumentenprüfinstanzen für ihre Zertifizierungs- und Registrierungsfunktion ein Informationssicherheitsmanagementsystem (ISMS) gemäß ISO/IEC 27001 einführen. Das ISMS beruht auf einem ISMS-Konzept, das in den nationalen Zertifikatregeln und in der dazugehörigen Zertifizierungspraxiserklärung umrissen ist.

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

9. SONSTIGE BETRIEBLICHE ODER RECHTLICHE ASPEKTE

9.1 Gebühren

Nicht anwendbar.

9.2 Finanzielle Verantwortung

Nicht anwendbar.

9.3 Vertraulichkeit betrieblicher Informationen

Nicht anwendbar.

9.4 Vertraulichkeit personenbezogener Informationen

Kontrollinstanzen DÜRFEN keine Fingerabdruckdaten von maschinenlesbaren Reisedokumenten protokollieren oder übermitteln. Derartige Daten MÜSSEN nach dem Abgleich der vom Lesegerät bei der betreffenden Person eingeholten Fingerabdruckdaten mit den Fingerabdruckdaten auf dem maschinenlesbaren Reisedokument unverzüglich gelöscht werden.

9.5 Rechte an geistigem Eigentum

Nicht anwendbar.

9.6 Vertretung und Garantien

Nicht anwendbar.

9.7 Garantieausschluss

Nicht anwendbar.

9.8 Haftungsbeschränkung

Nicht anwendbar.

9.9 Schadenersatz

Nicht anwendbar.

9.10 Laufzeit und Kündigung

Nicht anwendbar.

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

9.11 Benachrichtigungen und Kommunikation mit den Teilnehmern

Sämtliche wesentlichen Managementaufgaben MÜSSEN über zuverlässige Kommunikationskanäle abgewickelt werden.

Die LI-CVCA und die DVs MÜSSEN in der Lage sein, eine entsprechende Kommunikation zumindest per E-Mail vorzunehmen, obgleich zusätzlich noch andere Online- oder Offline-kommunikationskanäle vereinbart werden KÖNNEN.

Die LI-CVCA MUSS, falls ihre üblichen Kommunikationskanäle gestört sind, den DVs, die Zertifikate erhalten, alternative Kanäle für die Übermittlung von Zertifikatanträgen mitteilen. Diese Benachrichtigung MUSS möglichst rasch erfolgen, damit das Risiko, dass Zertifikate erlöschen, möglichst gering gehalten wird.

E-Mail-Mitteilungen MÜSSEN nach dem folgenden Format aufgebaut sein, und etwaige Anlagen MÜSSEN dem MIME-Standard entsprechen.

9.11.1 Register

Betr.: Register
Text: URLs für diesen Staat
Anlagen: keine

9.11.2 CVCA-Zertifikat

Betr.: CVCA-Zertifikat
Text: nicht spezifiziert
Anlagen: CVCA-Linkzertifikat(e)

9.11.3 DV-Zertifikatantrag

Betr.: DV-Zertifikatantrag
Text: nicht spezifiziert
Anlagen: Zertifikatantrag bzw. -anträge

9.11.4 Empfangsbestätigung für DV-Zertifikatanträge

Betr.: Empfangsbestätigung für DV-Zertifikatanträge
Text: nicht spezifiziert
Anlagen: Zertifikatantrag bzw. -anträge

9.11.5 DV-Zertifikat

Betr.: [Bescheid betreffend] DV-Zertifikatantrag
Text: Grund für die Nichterteilung eines DV-Zertifikats

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

Anlagen: DV-Zertifikat (wenn mindestens eines ausgestellt wurde)

9.11.6 Aussetzung des CVCA-Dienstes

Betr.: {Länder} Aussetzung des CVCA-Dienstes
Text: Beginn und Ende der Aussetzung des CVCA-Dienstes
Anlagen: nicht spezifiziert

9.12 Änderungen

Die gegenständliche Zertifikatsregeln [LI CVCA CP] kann jederzeit überarbeitet und geändert werden.

Rechtschreibfehler oder typografische Korrekturen, die den Inhalt der [LI CVCA CP] nicht ändern, sind ohne vorherige Meldung an andere Mitgliedsstaaten und die Europäische Kommission erlaubt.

Bevor eine Änderung der [LI CVCA CP] durchgeführt wird, die in der Sicherheit eine wesentliche Veränderung bedeutet, MUSS dies der Europäischen Kommission und den anderen Mitgliedsstaaten, für deren DVs Zertifikate der LI-CVCA ausgestellt wurden, gemeldet werden.

Die LI-CVCA wird die Absicht, die [LI CVCA CP] zu modifizieren, innerhalb von drei Monaten, bevor der Modifizierungsprozess an der EAC-CP vorgenommen wird, anderen Mitgliedsstaaten und der Europäischen Kommission und CVCA/DVs, melden.

Die Objektbezeichner (OIDs) der Zertifikatsregeln werden geändert, wenn die LI-CVCA feststellt, dass eine Änderung der Zertifikatsregeln Einfluss auf die Vertrauenswürdigkeit der Zertifikatsregeln hat.

9.13 Streitbeilegungsverfahren

Nicht anwendbar.

9.14 Anwendbares Recht

Nicht anwendbar.

9.15 Einhaltung geltender Rechtsvorschriften

Nicht anwendbar.

9.16 Ergänzende Bestimmungen

Nicht anwendbar.

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

9.17 Sonstige Bestimmungen

Nicht anwendbar.

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

10. ANLAGE A.1 BEGRIFFSBESTIMMUNGEN

1. Zertifizierungsstelle – Instanz, die Zertifikate ausstellt

2. Sperrliste – Verzeichnis widerrufener Zertifikate

3. Zertifikatregeln – Sicherheitsleitlinien einer Zertifizierungsstelle, die die Anwendbarkeit eines Zertifikats auf einen bestimmten Anwendungsbereich und/oder eine Anwendungsklasse mit gemeinsamen Sicherheitsanforderungen beschreiben

4. Zertifizierungspraxiserklärung – Erklärung über die Praktiken, die eine Zertifizierungsstelle bei der Ausstellung, der Verwaltung, dem Widerruf und der Erneuerung von Zertifikaten und beim Schlüsselaustausch verwendet

5. Einheitliche Zertifikatregeln (Common Certificate Policy) – von der Kommission veröffentlichtes Rahmenwerk für Zertifikatregeln, das bestimmte Mindestanforderungen vorsieht, denen die nationalen Zertifikatregeln der Mitgliedstaaten genügen müssen, bevor sie in die EAC-PKI aufgenommen werden können

6. Gemeinsame Kriterien - gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik („Common Criteria for Information Technology Security Evaluation“), Titel einer Reihe von Dokumenten, in denen bestimmte Kriterien für die Evaluierung der IT-Sicherheit beschrieben sind

7. Public-Key-Infrastruktur für die erweiterte Zugriffskontrolle (EAC-PKI) – Infrastruktur, die für die Kontrolle des Zugriffs auf in Pässen und Reisedokumenten gespeicherte Fingerabdruckdaten mit Hilfe der erweiterten Zugriffskontrolle erforderlich ist

8. Dokumentensignierer – Stelle, die das Originaldokument signiert, in diesem Fall die Stelle, die das maschinenlesbare Reisedokument ausstellt

9. Dokumentenprüfinstanz (DV) – Instanz innerhalb der EAC-PKI, die von einer CVCA Zertifikate anfordert und auf deren Grundlage Zertifikate für Kontrollinstanzen ausstellt

10. Prüftiefe – Einstufung eines IT-Systems oder Produkts nach Maßgabe der Bewertung seiner Sicherheit nach den gemeinsamen Kriterien für die Bewertung der Sicherheit von Informationstechnik

11. Kontrollinstanz – System (einschließlich des hoheitlichen Lesegeräts) für das Auslesen von Fingerabdruckdaten aus maschinenlesbaren Reisedokumenten

12. Internationale Zivilluftfahrt-Organisation – Sonderorganisation der Vereinten Nationen, die sich mit der Planung und Entwicklung des internationalen Luftverkehrs

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

befasst; in diesen Zusammenhang legt sie internationale Standards für maschinenlesbare Reisedokumente fest

13. Schlüsselimportzeremonie – Verfahren, bei dem ein Schlüsselpaar mit Hilfe eines Sicherheitsmoduls erzeugt und der öffentliche Schlüssel zertifiziert wird

14. Linkzertifikat – Zertifikat, das ohne Austausch eines neuen vertrauenswürdigen, selbstsignierten Zertifikats der Wurzelzertifizierungsstelle („out-of-band“) die Betriebskontinuität gewährleistet

15. Maschinenlesbares Reisedokument – internationales Reisedokument, das neben direkt zu entnehmenden Informationen auch Daten enthält, die nur mit Geräten ausgelesen werden können

16. Nationale Zertifikatregeln – Zertifikatregeln eines Mitgliedstaats für die Erteilung von Zertifikaten an andere Mitgliedstaaten bzw. für den Erhalt von Zertifikaten anderer Mitgliedstaaten;

17. Objektbezeichner – einmalig zugeordnete Zahlenreihe, anhand derer ein Dokument eindeutig identifiziert werden kann;

18. Öffentlicher Teil der Zertifizierungspraxiserklärung – Teil der Bestimmungen einer Zertifizierungspraxiserklärung, die von einer Zertifizierungsstelle veröffentlicht wird

19. Registrierungsstelle – Stelle, die die Antragsverfahren für Zertifikate festlegt, die Identität der Antragsteller überprüft und diese authentisiert, Anträge auf Widerruf von Zertifikaten stellt oder weiterleitet und Anträge auf Erneuerung von Zertifikaten oder auf Austausch der Schlüssel im Namen der Zertifizierungsstelle genehmigt

20. Vertrauenswürdiger Zertifizierungspfad – Kette von Zertifikaten, die zur Validierung eines Zertifikats, das den erforderlichen öffentlichen Schlüssel enthält, benötigt wird. Eine Zertifikatkette besteht aus mindestens einem CVCA-Zertifikat, gegebenenfalls Linkzertifikaten, einem DV-Zertifikat und dem IS-Zertifikat.

Aus Abschnitt 1.6 der [EU CP] werden folgende Definitionen übernommen:

- Ein „Mitgliedstaat“ ist ein Land, auf welche die Verordnung (EG) Nr. 2252/2004 anwendbar ist.

- „Inländisch“ bedeutet: vom Fürstentum Liechtenstein.

- „Ausländisch“ bedeutet: von einem anderen Teilnehmerstaat der EAC-PKI.

- Ein „gültiger Schlüssel“ ist ein Schlüssel, bei dem der gegenwärtige Zeitpunkt in den Gültigkeitszeitraum des entsprechenden Abonnentenzertifikats fällt und letzteres nicht widerrufen worden ist.

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

11. ANLAGE A.2 ABKÜRZUNGEN

CA	Certification Authority (Zertifizierungsstelle)
CC	Common Criteria (Gemeinsame Kriterien für die Bewertung der Sicherheit von Informationstechnik)
CP	Certificate Policy (Zertifikatregeln)
CPS	Certification Practice Statement (Zertifizierungspraxiserklärung)
CRL	Certificate Revocation List (Sperrliste)
CSCA	Country Signing Certification Authority (nationale Wurzelzertifizierungsinstanz im Kontext der Ausstellung von Reisedokumenten)
CSPKI	Country Signing Public Key Infrastructure (nationale Public-Key-Infrastruktur für die Ausstellung von Reisedokumenten)
CVRA	Country Verifying Registration Authority (Registrierungsstelle der nationalen Wurzelzertifizierungsstelle im Kontext Berechtigung von Kontrollinstanzen zum Zugriff auf sensitive Daten)
CVCA	Country Verifying Certification Authority (Zertifizierungsstelle der nationalen Wurzelzertifizierungsinstanz im Kontext Berechtigung von Kontrollinstanzen zum Zugriff auf sensitive Daten)
EAC-PKI	Extended Access Control Public Key Infrastructure (Public-Key-Infrastruktur für die erweiterte Zugriffskontrolle)
DV	Dokumentenprüfinstanz
EAC	Extended Access Control (erweiterte Zugriffskontrolle)
EAL	Evaluation Assurance Level (Prüftiefe)
ICAO	International Civil Aviation Organisation (Internationale Zivilluftfahrt-Organisation)
IS	Inspection System (Kontrollinstanz - Lesegerät)
MRTD	Machine Readable Travel Document (maschinenlesbares Reisedokument)
OID	Object Identifier (Objektbezeichner)
RA	Registration Authority (Registrierungsstelle)

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

CR	Certificate Request (Zertifikatsantrag)
DVCA	Document Verifing Certification Authority (CA einer Dokumentenprüfinstanz)
F-CVCA	Fremde (ausländische) CVCA
F-DVCA	Fremde (ausländische) DVCA
F-SPOC	Fremder (ausländische) SPOC
HSM	Hardware Security Module (Hardware Sicherheitsmodul)
LI-CVCA	Liechtensteinische CVCA
LI-CVRA	Liechtensteinische Registrierungsstelle
LI-SPOC	Liechtensteinischer SPOC
LLV/APA	Das Ausländer- und Passamt der Liechtensteinischen Landesverwaltung
OCSP	Online Certificate Status Protokoll; eine Möglichkeit zu prüfen, ob ein Zertifikat widerrufen wurde
SPOC	Single Point of Contact (zentraler, singulärer Ansprechpartner)
USB-Token	Ein Datenträger mit USB-Anschluss

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

12. ANLAGE B.1 ANFORDERUNGEN AN ZERTIFIZIERUNGSSTELLEN

Die von den Zertifizierungsstellen verwendeten Sicherheitsmodule MÜSSEN nach folgenden Standards bewertet und zertifiziert werden:

1. FIPS PUB 140-1 Stufe 3 oder höher [3]
2. FIPS PUB 140-2 Stufe 3 oder höher [4]
3. PP-SSCD [5] [6] [7]
4. BSI Cryptographic Modules Security Level “Enhanced” [8]

[3] Security Requirements for Cryptographic Modules (FIPS PUB 140-1)
[4] Security Requirements for Cryptographic Modules (FIPS PUB 140-2)
[5] BSI-PP-0004-2002T Protection Profile – Secure Signature-Creation Device Type 1, Version 1.05
[6] BSI-PP-0005-2002T Protection Profile – Secure Signature-Creation Device Type 2, Version 1.04
[7] BSI-PP-0006-2002T Protection Profile – Secure Signature-Creation Device Type 3, Version 1.05
[8] BSI-PP-0036-2008: Cryptographic Modules Security Level "Enhanced" Version 1.01

AUSLÄNDER- UND PASSAMT
FÜRSTENTUM LIECHTENSTEIN

13. ANLAGE C. REFERENZDOKUMENTE

[BSI TR EAC]	Advanced Security Mechanisms for Machine Readable Travel Documents; https://www.bsi.bund.de/cln_165/ContentBSI/Publikationen/TechnischeRichtlinien/tr03110/index_htm.html	BSI; V 1.11; 21.02.2008
[EU CP]	Entscheidung der Kommission vom 22. Dezember 2008 über Zertifikatsregeln entsprechend der Vorgabe in den technischen Spezifikationen der Normen für Sicherheitsmerkmale und biometrischen Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten und zur Aktualisierung der Verweise auf Normen und Standards	EU Kommission K(2008) 8657; 22.12.2008
[IETF RFC 2119]	Key words for use in RFCs to Indicate Requirement Levels; http://tools.ietf.org/html/rfc2119	IETF; 03.1997