Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Bundesamt für Informatik und Telekommunikation BIT
Swiss Government PKI

NICHT KLASSIFIZIERT

Klasse B: Antrag LRA-Officer

V4.5, 20.09.2019

☐ **Neuer LRAO** → Abs. A und B
☐ **Erneuerung LRAO** → Abs. A und B
☐ **Mutation Berechtigungen** → Abs. B
☐ **Revokation LRAO-Zertifikat** → Abs. B und C

Abschnitt A) Folgende Anforderungen müssen erfüllt sein, bevor der Antrag bearbeitet werden kann:

☐ Schulung besucht, Test bestanden: Kopie des Attests und Bestätigung des bestandenen Tests beigelegt

☐ AdminDir Eintrag in Gelben Seiten vorhanden

☐ LRA-Officer Informationen unter → *Abschnitt B* korrekt und vollständig ausgefüllt

Abschnitt B) Angaben zum LRA-Officer und zu den Ausstellberechtigungen:

Ausstellung Klasse B für BV:
☐ E-Mail-Adresse endet auf admin.ch (Prestaged/ Enhanced CA02)
☐ E-Mail-Adresse endet *nicht* auf admin.ch (Prestaged/ Enhanced CA01)

Ausstellung Klasse B für Extern (Non-BV):
☐ Prestaged (Enhanced CA01)
☐ *Non*-prestaged/ Standard (Enhanced CA01)

Angaben zum LRA Officer (Müssen mit dem Eintrag im AdminDir übereinstimmen; *=Pflichtfelder!)			
Nachname*:		Vorname*:	
Suffix*:		Departement*:	
Amt*:		Tel.*:	
E-Mail*:			
Adresse (Strasse, PLZ, Ort)*:			
Ausstellberechtigungen für (Dep./Amt)*:		☐ neu ☐ entziehen	
Seriennummer Auth. Zert. pers. Klasse B			
Berechtigungen für **Admin-Account** Zertifikate (A-Accounts) (auf Stufe Dep.)	☐ neu ☐ entziehen für Departement: Bitte wählen...		

Abschnitt C) Folgende Anforderungen müssen erfüllt sein, bevor der Antrag bearbeitet werden kann:

Ausführungsdatum Revokation:

Gibt es einen nachfolgenden LRA-Officer? ☐ Nein ☐ Ja, Name:

☐ LRA-Officer Informationen unter → ***Abschnitt B*** korrekt und vollständig ausgefüllt

Der noch aktive LRA-Officer verpflichtet sich, seinem Nachfolger die Kundendossiers und das Journal zu übergeben. Er ist gebeten seine LRA-Officer Smartcard zurückzusenden.

Allgemeine Nutzungsbedingungen für den LRAO

Vertraulichkeitserklärung

Der Antragsteller verpflichtet sich mit seiner Unterschrift, die Smartcard und das zugehörige Passwort vertraulich zu behandeln und die im Rahmen seiner Arbeit als LRA-Officer erhaltenen, personenbezogenen Informationen nicht an Dritte und intern nur an die Mitarbeiter weiterzugeben, welche zur Erfüllung ihrer Aufgaben unbedingt unmittelbaren Zugriff auf diese Informationen benötigen. Mitarbeiter mit LRAO-Funktion sind, soweit dies nicht bereits in ihrem Arbeitsvertrag festgelegt ist, zur Geheimhaltung zu verpflichten. Von den zu bearbeitenden Daten und Informationen sind weder vollständige noch auszugsweise Kopien anzufertigen.

Der LRA-Officer ist verpflichtet, bei Amtsaufgabe das Zertifikat revozieren zu lassen.
Die vorliegende Erklärung ist auch nach der Amtsaufgabe als LRA-Officer und nach Austritt derselben Person wirksam.

Es gelten für das LRA-Officer Zertifikat die «Benutzervereinbarung und Nutzungsbedingungen für LRA-Officer der SG-PKI» sowie die «Guidelines zu LRAO-Zertifikaten der Swiss Government PKI» (folgende Seiten) und die «Swiss Government PKI Registrierrichtlinien Klasse B». Mit seiner Unterschrift bestätigt der angehende LRA-Officer, gemäss der geltenden CP/CPS der SG-Root CA I alle in diesen Dokumenten vorhandenen Vorschriften und Verfahren, gelesen, verstanden und akzeptiert zu haben und vollständig einzuhalten. Der angehende LRA-Officer bestätigt mit seiner Unterschrift weiter mit der Ausstellung einer persönlichen LRA-Officer Smartcard zur Ausübung der LRA-Officer Tätigkeit einverstanden zu sein.

Antragsteller (Vorname, Nachname)	**Datum:** **Unterschrift/ Signatur:**

Vertrauenswürdigkeitsprüfung

Die Behörde ergreift die im gesetzlichen Rahmen erlaubten sowie ihr zumutbaren Massnahmen, um die Vertrauenswürdigkeit und Integrität des Kandidaten/ der Kandidatin zu überprüfen. Die SG-PKI empfiehlt der Behörde die Durchführung folgender Massnahmen:

- Personensicherheitsprüfung gemäss Artikel 10 der Verordnung über die Personensicherheitsprüfungen (PSPV, SR 120.4) bei der Fachstelle PSP des VBS.

  und/oder

- Vornahme eigener Massnahmen zur Überprüfung der Vertrauenswürdigkeit, wie beispielsweise:
  - Kontrolle der Identität des Kandidaten/ der Kandidatin (Pass oder Identitätskarte);
  - Überprüfung von geschäftlichen und/oder privaten Referenzen des Kandidaten/ der Kandidatin;
  - Verifizierung der Vollständigkeit und Schlüssigkeit des Lebenslaufs des Kandidaten/ der Kandidatin;
  - Kontrolle der referenzierten akademischen und beruflichen Qualifikationen;
  - Überprüfung von Betreibungs- und Strafregisterauszügen.

Bestätigung

Die unterschriftsberechtigte Person der Behörde bestätigt gegenüber der SG-PKI, die Vertrauenswürdigkeit des Kandidaten/ der Kandidatin gemäss obenstehender Empfehlung oder auf vergleichbare Art und Weise überprüft zu haben. Sie stuft den Kandidaten/ die Kandidatin als vertrauenswürdig und integer ein und bestätigt zudem, dass er/ sie über die notwendigen Kompetenzen zur Ausübung der sicherheitsempfindlichen Tätigkeit als LRA-Officer verfügt.

Unterschriften

Sofern Berechtigungspfade mehrerer Ämter beantragt werden, müssen die Unterschriftsberechtigten von jedem beantragten Amt unterschreiben. Benutzen Sie dazu das zusätzliche Listenformular unter den Klasse B-Formularen auf www.pki.admin.ch.

Unterschriftsberechtigt sind:

- auf **Amtsebene**: ISBOs, PKI-Verantwortliche der Kantone/ Polizeikorps, Sicherheitsbeauftragte von kantonalen Ämtern, sowie das SG-PKI Managementboard
- auf **Departements Ebene**: ISBDs, PKI-Verantwortliche der Kantone/ KAPOs sowie Sicherheitsbeauftragte der Kantone und Kantonspolizei

Unterschriftsberechtigte(r) Amt (Vorname, Nachname/ Funktion)	**Datum:** **Unterschrift/ Signatur:**

Für die Zuteilung von Berechtigungen für A-Accounts (nur BV-intern) ist die Unterschrift des **ISBD** einzuholen (*Berechtigung gilt immer für das gesamte Departement!*). Sofern die Berechtigungen mehrerer Departemente beantragt werden, muss das nachstehende Unterschriftsfeld von den ISBDs aller beantragten Departemente unterschrieben werden. Benutzen Sie dazu das zusätzliche Listenformular unter den Klasse B-Formularen auf www.pki.admin.ch.

Unterschriftsberechtigte(r) Departement (Vorname, Nachname) Dep/ Kt.	**Datum:** **Unterschrift/ Signatur:**

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Bundesamt für Informatik und Telekommunikation BIT
Swiss Government PKI

NICHT KLASSIFIZIERT

Benutzervereinbarung und Nutzungsbedingungen für LRA-Officer der SG-PKI

Zur Ausstellung von persönlichen Zertifikaten der Klassen A (qualifizierte und geregelte) und B (fortgeschrittene) Zertifikate der Swiss Government PKI, der Bundesbehörde der Schweizerischen Eidgenossenschaft

V1.0, 28.08.2018

Die Swiss Government PKI des BIT, in ihrer Rolle als Trust Service Provider (TSP), betreibt im Auftrag des ISB (Informatiksteuerungsorgan des Bundes) die PKI (Public-Key-Infrastruktur) der Bundesbehörden der Schweizerischen Eidgenossenschaft. Im Rahmen des Marktmodells «SD005 - Marktmodell Standarddienst: Identitäts- und Zugangsverwaltung (IAM)» werden die Zertifikate der Klasse A und B definiert. Die LRA-Officer (Local Registration Agency Officer) sind für die Ausstellung von Zertifikaten der Klasse A und B zuständig. Bezug und Nutzung der LRAO-Zertifikate der Klassen A und B unterliegen den Bestimmungen der «*Benutzervereinbarung und Nutzungsbedingungen Klasse A/B*». Diese werden durch die Swiss Government PKI (SG-PKI) jährlich den jeweils geltenden gesetzlichen Vorschriften und den normativen Anforderungen an Public Key Infrastrukturen angepasst. Letztere bilden die Basis dieser Benutzervereinbarung und Nutzungsbedingungen. Die jeweils gültige Version ist auf www.pki.admin.ch publiziert. Alle Inhaber von Zertifikaten werden über die Publikation einer aktualisierten Version der Dokumente per E-Mail informiert.
Zu beachten sind des Weiteren die «*Guidelines zu den LRAO-Zertifikaten der SG-PKI*». Diese müssen beim Bezug eines LRAO-Zertifikats ebenfalls akzeptiert werden.

Vollständigkeit und Genauigkeit der Informationen

Der Inhaber eines LRAO-Zertifikates der Swiss Government PKI (in Folge «Inhaber oder LRAO» genannt[1]) verpflichtet sich dazu, dem TSP die für den Ausstellungsprozess sowie auch für den Inhalt des Zertifikats benötigten Informationen jederzeit korrekt und vollständig zu liefern. Vor der Ausstellung des Zertifikats muss der LRAO bei persönlicher Anwesenheit anhand eines gültigen Reisedokuments identifiziert werden. Das Zertifikat ist untrennbar an diesen LRAO gebunden. Vorname(n)/ Nachname(n), Suffix und e-Mailadresse des LRAO werden immer im Zertifikat aufgeführt.

Der Inhaber verpflichtet sich ebenfalls, die Daten seiner Kunden (=Bezüger von Zertifikaten der Klassen A und/ oder B) gemäss den «*Registrierrichtlinien für die Klasse A bzw. B*» zu prüfen.

Der LRAO ist verpflichtet, den TSP zu informieren, sobald sich seine persönlichen Daten, insbesondere Vorname, Nachname, Suffix (seines Eintrages im Admin-Directory des Bundes) oder die e-Mailadresse ändern.

Schutz des privaten Schlüssels und des Zertifikats

Der LRAO verpflichtet sich dazu, alle angemessenen Vorkehrungen zu treffen, um die alleinige Kontrolle, die Vertraulichkeit und den Schutz vor Verlust und Missbrauch des privaten Schlüssels und der allfällig damit verbundenen Aktivierungsdaten (z.B. PIN/ PUK) und Medien (z.B. Smartcard), zu gewährleisten. Der private Schlüssel des Zertifikats kann und darf nur im Zusammenhang mit dem Zertifikat und nur für die im Zertifikat festgelegten Zwecke (Ausstellung/Revokation/Management von Klasse A und B Zertifikate) eingesetzt werden. Sie

[1] Die männliche Form «Inhaber» wird in diesem Dokument der besseren Leserlichkeit dienend gleichermassen für das weibliche und das männliche Geschlecht benutzt.

dürfen auf keinen Fall unberechtigten Dritten zugänglich gemacht werden. Der Inhaber haftet für jeden Schaden, der durch die Weitergabe des privaten Schlüssels und der allfällig damit verbundenen Aktivierungsdaten und Medien an Dritte entstanden ist.

Der TSP behält sich vor, das Zertifikat bereits bei einem konkreten Verdacht auf Missbrauch oder unautorisierten Zugang zum privaten Schlüssel ohne Vorinformation zu revozieren.

Nutzung des Zertifikats

Der LRAO stellt sicher, dass ihm Inhalt, Zweck und Wirkung des Einsatzes des LRAO-Zertifikates bekannt sind. Er verpflichtet sich, den auf der LRAO-Smartcard vorhandenen Zertifikat und den privaten Schlüssel nur für autorisierte Geschäfte und unter Einhaltung aller geltenden gesetzlichen Vorschriften sowie den Bestimmungen dieses Dokuments einzusetzen.

Berichterstattung und Revokation

Der LRAO verpflichtet sich dazu, das Zertifikat und den dazugehörigen privaten Schlüssel unverzüglich nicht mehr einzusetzen und beim TSP die Revokation zu verlangen, wenn:

- der konkrete Verdacht besteht, dass mit dem Zertifikat verdächtige Aktivitäten (Missbrauch der Aktivierungsdaten) unternommen wurden;
- die Informationen im Zertifikat nicht mehr korrekt oder ungenau sind oder es in naher Zukunft sein werden;

Den Anweisungen des TSP ist bei Verdacht auf Kompromittierung oder Missbrauch des Zertifikats unmittelbar Folge zu leisten.

Wenn aus Sicherheitsgründen erforderlich und aus datenschutzrechtlicher Sicht erlaubt, kann der TSP Daten über den LRAO, das Zertifikat und weitere in unmittelbarem Zusammenhang stehende Informationen an andere zuständige Stellen, TSPs, Firmen und industrielle Gruppen weiterleiten, wenn das Zertifikat oder die Person, die das Zertifikat einsetzt, als Quellen einer missbräuchlichen Verwendung identifiziert werden.

Alle Informationen betreffend die Revokation werden durch den TSP aus Gründen der Nachvollziehbarkeit archiviert.

Beendigung des Einsatzes des Zertifikats

Der LRAO verpflichtet sich dazu, den Einsatz des Zertifikats nach dessen Ablauf oder Revokation (insbesondere aufgrund einer Kompromittierung) sofort zu unterlassen.

Verantwortung / Haftung

Der LRAO ist dafür verantwortlich, dass das LRAO-Zertifikat und der zugehörige private Schlüssel nur unter Einhaltung der Bestimmungen in Abschnitt «Nutzung des LRAO-Zertifikates» dieses Dokuments eingesetzt werden. Ein Verstoss gegen diese Vorgabe hat eine Revokation und weitere administrative und gegebenenfalls juristische Massnahmen zur Folge. Der LRAO trägt die Verantwortung für alle durch ihn mit dem Zertifikat auf der LRAO-Smartcard vorgenommenen Tätigkeiten sowie für allfällig daraus resultierende Schäden und deren Folgen.

Anerkennungs- und Einverständniserklärung

Der LRAO nimmt zur Kenntnis, dass der TSP das Zertifikat bereits bei einem begründeten Verdacht eines Missbrauchs, einer Verletzung der Bestimmungen dieses Dokuments oder eines sonstigen Verstosses gegen geltende gesetzliche Bestimmungen unverzüglich revoziert.

Der LRAO bezeugt mit seiner Unterschrift im jeweiligen Anmeldeformular Klasse A/B: Antrag LRA-Officer, dass er das vorliegende Dokument «*Benutzervereinbarung und Nutzungsbedingungen für LRA-Officer der SG-PKI*» gelesen und verstanden hat und die darin aufgeführten Bestimmungen akzeptiert.

NICHT KLASSIFIZIERT

Guidelines zum LRAO-Zertifikat der Swiss Government PKI

Erläuterungen zum Bezug und Einsatz vom LRAO-Zertifikat der Klassen A und B der Swiss Government PKI

V1.0, 28.08.2018

1 Zweck des LRAO-Zertifikats

Zweck

Im Rahmen des Marktmodells «SD005 - Marktmodell Standarddienst: Identitäts- und Zugangsverwaltung (IAM)» werden die Zertifikate der Klasse A und B definiert. Die LRA-Officer (Local Registration Agency Officer) sind für die Ausstellung der Klasse A und B zuständig. Das LRAO-Zertifikat kann für folgende Zwecke verwendet werden:

- Ausstellung Revokation und Pflege von Klasse A und/oder B Zertifikate der Swiss Government PKI.

Durch erweiterte Prüf- und Sicherheitsmechanismen während des Ausstellungsprozesses der Klassen A und B Zertifikate wird die Identität des Zertifikatsinhabers auf einer hohen Sicherheitsstufe festgestellt. Die Ausgabe von Klasse A und B Zertifikaten erfolgt immer persönlich und nur nach Identifizierung des Inhabers mittels eines gültigen, für die Einreise in die Schweiz zugelassenen Reisedokumentes.

Ausgeschlossener Zweck

Das LRAO-Zertifikat erfüllt ausschliesslich die oben genannten Zwecke und gibt keinerlei weitere Aufschlüsse, Versicherungen oder Garantien. Insbesondere garantiert das LRAO-Zertifikat nicht, dass der Inhaber im Umgang mit dem Zertifikat korrekt und legal handelt.
Des Weiteren garantiert das LRAO-Zertifikat nicht, dass:

- Der im Zertifikat genannte Inhaber aktiv in die Geschäftstätigkeiten involviert ist;
- Der im Zertifikat genannte Inhaber sich an die geltenden gesetzlichen Vorschriften hält;
- Der im Zertifikat genannte Inhaber im Geschäftsumfeld seriös handelt;

2 Qualität des LRAO-Zertifikats

Die SG-PKI hält sich an die in den Registrierrichtlinien vorgegebenen Prozesse, welche die notwendigen und zumutbaren Schritte zur Bestätigung folgender Tatsachen zum Zeitpunkt der Erstausstellung eines LRAO-Zertifikates festlegen:

- **Rechtlich gültige Existenz:** Der im LRAO-Zertifikat genannte Inhaber existiert als natürliche Person und verfügt über einen persönlichen Eintrag im AdminDirectory.
- **Identität:** Der Name des im LRAO-Zertifikats genannten Inhabers stimmt mit dem Namen im AdminDirectory und im aktuell gültigen Reisedokument überein.
- **Autorisierung:** Der im LRAO-Zertifikat genannte Inhaber ist zum Bezug des Zertifikates durch die unterschriftsberechtigte Person seines Amtes autorisiert worden.
- **Richtigkeit der Daten:** Alle im Zertifikat enthaltenen Daten und Informationen sind korrekt.

- **Vereinbarung/ Nutzungsbedingungen:** Der im LRAO-Zertifikat genannte Inhaber hat die in der «*Benutzervereinbarung und Nutzungsbedingungen für LRA-Officer der SG-PKI*» beschriebenen Rechte und Pflichten gelesen, verstanden und mit der Unterschrift auf dem Antragsformular für das LRA-Officer Zertifikat der SG-PKI akzeptiert. Seine Fragen diesbezüglich wurden von der SG-PKI verständlich beantwortet.
- **Status:** Die SG-PKI stellt den Status des Zertifikats sowie Informationen über dessen Gültigkeit/ Revokation online abrufbar zur Verfügung.
- **Revokation:** Die SG-PKI kann das LRAO-Zertifikat gegebenenfalls aus den in der/n «*Benutzervereinbarung und Nutzungsbedingungen für LRA-Officer der SG-PKI*» genannten Gründen unverzüglich revozieren.

3 Policies

Alle geltenden gesetzlichen Vorgaben, Policies (inkl. der CP/CPS der SG Root CA I) und Registrierrichtlinien von Zertifikaten der SG-PKI, sowie die «*Benutzervereinbarung und Nutzungsbedingungen für LRA-Officer der SG-PKI*» und diese Guidelines sind im Internet auf der Website der SG-PKI publiziert: www.pki.admin.ch.

Der angehende LRAO verpflichtet sich mit der Unterschrift auf dem Formular: «*Klasse B: Antrag LRAO*», sich an die geltenden Richtlinien und Gesetzgebungen zu halten und seine Arbeiten danach auszuführen. Insbesondere sind dies:

- Die CP/CPS der SG Root CA I: («*Certificate Policy and Certification Practice Statement of the Swiss Government Root CA I*») (insbesondere zu erwähnen sind die in Kap. 5.3.1 und 5.5.2 beschriebenen Verpflichtungen)
- Die «*Swiss Government PKI Registrierrichtlinien Klasse B*»
- Die «*Benutzervereinbarung und Nutzungsbedingungen für LRA-Officer der SG-PKI*»
- Die «*Guidelines zum LRAO-Zertifikat der Swiss Government PKI*» (Dieses Dokument).

Inhalt

Das LRAO-Zertifikat der SG-PKI enthält Informationen betreffend:

- Herausgeber und ausstellender CA
- die Root CA der ausstellenden CA
- die angewandte Policy
- Ausstell- und Ablaufdatum des Zertifikates
- Seriennummer des Zertifikates
- Verwendungszweck des Zertifikates
- der CRL und dem OCSP
- die Auditoren der CA
- den Inhaber des Zertifikates gemäss Eintrag im AdminDirectory zum Zeitpunkt der Erstausstellung:
    1) Common Name des Inhabers
    2) E-Mail-Adresse
    3) UPN

Gültigkeit

Das LRAO-Zertifikat der SG-PKI ist max. 3 Jahre gültig. Nach Ablauf der Gültigkeit muss das LRAO-Zertifikat durch den LRAO-Officer neu bei der SG-PKI, analog dem Erstausstellungsprozess, beantragt und von der SG-PKI ausgestellt werden.

4 Bezug des LRAO-Zertifikats

Bezug

Für den Bezug des LRAO-Zertifikats der SG-PKI sind folgende Dokumente bzw. Registrierungen nötig:

- Ein gültiges, für die Einreise in die Schweiz zugelassenes Reisedokument (ID/ Pass), ausgestellt auf den Antragsteller. Die Identität wird während der obligatorischen LRAO-Schulung vom Kursleiter überprüft
- Ein persönlicher Eintrag im AdminDirectory, mit Nachname(n), Vorname(n) (gemäss Reisedokument), gültiger E-Mailadresse und optional einem UPN Eintrag (User Principal Name)

- Ein Attest, welches den erfolgreichen Besuch der obligatorischen LRA-Officer Schulung und die bestandene Prüfung bezeugt
- Ein ausgefülltes und (elektronisch) signiertes Antragsformular für LRA-Officer Zertifikate der Swiss Government PKI, in welchem
    1) der angehende LRAO
        - eine Vertraulichkeitserklärung
        - die Benutzervereinbarung und Nutzungsbedingungen für LRA-Officer der SG-PKI
        - diese Guidelines

    mit seiner Unterschrift als akzeptiert erklärt und die LRAO-Smartcard bestellt.
    2) die Unterschriftsberechtigte Person der anstellenden Behörde die Vertrauenswürdigkeit des angehenden LRA-Officer, gemäss den Vorgaben im Antragsformular unter dem Kapitel «Vertrauenswürdigkeitsprüfung», mit seiner Unterschrift bestätigt.

Identifizierung

Um die antragstellende Person zu identifizieren, wird das Reisedokument auf Gültigkeit, Richtigkeit und Echtheit während der LRAO-Schulung überprüft. Die SG-PKI Kursleiter sind zudem verpflichtet, das Bild des Dokumentes mit der vor Ihnen stehenden und am Kurs teilnehmende Person zu validieren. Ebenso wird der Antrag vor der Ausstellung eines persönlichen Zertifikates von der SG-PKI plausibilisiert (Person arbeitet tatsächlich in der im AdminDirectory Eintrag zugewiesenen Organisationseinheit und benötigt das Zertifikat im geschäftlichen Alltag; der Antragsteller ist berechtigt ein Zertifikat zu beantragen).

Verbindlichkeit

Der Antrag muss durch die zuständigen Stellen freigegeben sein. Diese Guidelines und das Dokument «*Benutzervereinbarung und Nutzungsbedingungen für LRAO der SG-PKI*» müssen vom Antragsteller verstanden und im Antragsformular für LRAO mit der (digitalen) Unterschrift akzeptiert worden sein.

5 Schutz des privaten Schlüssels und des Zertifikates

Übertragbarkeit

Das LRAO-Zertifikat ist immer persönlich und nicht übertragbar. Die persönlichen Angaben über den Inhaber werden sowohl im Zertifikat wie auch bei der SG-PKI gespeichert.

PIN/PUK

Die PIN muss unabhängig von anderen Passwörtern gewählt werden und darf für Dritte nicht zugänglich sein. Sie muss nicht regelmässig geändert werden, ausser es besteht der konkrete Verdacht, dass ein Dritter Kenntnis davon erlangt hat.

Das Zertifikat (und somit der Zertifikatsträger: Smartcard, USB-Stick, etc.) muss mit einer mind. 6-stelligen PIN gesichert werden, wobei rein numerische PINs, sowie auch gemischte PINs erlaubt sind. Um den Missbrauch der eigenen elektronischen Identität zu vermeiden, darf die PIN niemals Dritten bekanntgegeben werden.

Der PUK der Smartcard muss mindestens 8-stellig nach den oben genannten Regeln gewählt werden.

Meldepflicht

Ein allfälliger Verlust der Smartcard muss vom LRAO umgehend der SG-PKI gemeldet werden. In der Folge wird das betroffene Zertifikat gesperrt (revoziert) und die Sperrung auf einer öffentlichen elektronischen Sperrliste publiziert. Selbst wenn die Smartcard wiedergefunden werden sollte, bleibt das Zertifikat gesperrt und somit ungültig. Unmittelbar nach erfolgter Sperrung kann bei der SG-PKI die Ausstellung eines neuen LRAO-Zertifikates beantragt werden. Der Prozess der Ausstellung eines neuen LRAO-Zertifikats entspricht der Erstausstellung.

Organisationswechsel, Namenswechsel (z.B. nach Heirat) oder Änderung der E-Mail-Adresse bedingen die Ausstellung eines neuen Zertifikates (Erstausstellung).

6 Revokation

Revokationen müssen bei der SG-PKI beantragt werden. Dazu steht den befugten Personen (siehe abschliessende Liste unten) ein Formular auf der Homepage der SG-PKI www.pki.admin.ch zur Verfügung. Wird die Revokation per Telefon beantragt, wird die SG-PKI den Antragsteller mit Hilfe der Revokationspassphrase und den persönlichen Daten (Geburtstag, Geburtsort, etc.) identifizieren. Lediglich der Antragsteller selbst ist befugt, eine Revokation per Telefon zu beantragen. Weitere Personen, die eine Revokation beantragen dürfen, müssen die Anfrage schriftlich einreichen.

Befugte Personen sind:

- der Zertifikatsinhaber selbst
- der SG-PKI Verantwortliche
- SG-PKI Security Officer
- die für den Zertifikatsinhaber zuständigen:
  - Mitarbeiter des HR (Personaldienst),
  - Linienvorgesetzte
  - LRA Officer
  - ISBO
  - ISBD
  - PKI Verantwortliche der Organisation

7 Inhalt des Zertifikates

Authentifizierungszertifikat (Authentication Key)
Fingerprint (SHA-1):
Certificate Validity:
Serial #:

8 Akzept/ Bestätigung für Erhalt der Smartcard

Mit der Unterschrift auf dem Empfangsformular für LRAO-Zertifikate bestätigt der Zertifikatsinhaber nach Erhalt der LRAO-Smartcard:

- Die Korrektheit der im Zertifikat gespeicherten Daten.
- Den Erhalt der LRAO-Smartcard.
- Diese Guidelines und die Rechte und Pflichten, die aus diesen Guidelines erwachsen, verstanden und akzeptiert zu haben. Allfällige Fragen wurden von der SG-PKI verständlich beantwortet.
- Die Revokationspassphrase sowie die restlichen zur telefonischen Identifikation der Person und des Zertifikates benötigten Felder korrekt ausgefüllt zu haben.

Ausserdem verpflichtet sich der angehende LRAO, die hier beschriebenen Richtlinien, die in der CP/CPS («*Certificate Policy and Certification Practice Statement of the Swiss Government Root CA I*») beschriebenen, sowie auch die in den «*Swiss Government PKI Registrierrichtlinien Klasse B*» Anforderungen und Aufgaben zu erfüllen und umzusetzen.

Zusätzliche Fragen können an die Swiss Government PKI unter der Mailadresse pki-info@bit.admin.ch gestellt werden.