Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Bundesamt für Informatik und Telekommunikation BIT
Swiss Government PKI

NICHT KLASSIFIZIERT

Klasse A: Antrag LRA-Officer

V5.0, 19.02.2019

◯ **Neuer/ Erneuerung LRAO** → Abschnitt A und B

◯ **Mutation Berechtigungen/ Pfade** → Abschnitt B

◯ **Revokation LRAO-Zertifikat** → Abschnitt C

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

☐ Schulung LRAO Klasse A besucht: 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:

Die Ausstellung von nach ZertES qualifizierten, persönlichen Zertifikaten der Klasse A (nur Signaturzertifikat) erfolgt auf der ausstellenden CA der Swiss Government PKI Regulated CA02. Die dazugehörender Root ist die Swiss Government PKI Root CA IV: Siehe dazu auch die dazugehörende CP/CPS: http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_5_0.pdf

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	

Abschnitt C) Folgende Anforderungen müssen erfüllt sein, bevor der Revokations-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. Sollte das nicht möglich sein, müssen die Unterlagen der SG-PKI zur Archivierung übergeben werden. Der LRAO 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 A- Qualifiziert». Mit seiner Unterschrift bestätigt der angehende LRA-Officer, gemäss der geltenden CP/CPS der SG-Root CA IV 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 A-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:**

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 A-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 (nach ZertES qualifizierte) und B (fortgeschrittene) Zertifikate der Swiss Government PKI, der Bundesbehörde der Schweizerischen Eidgenossenschaft

V1.1, 19.02.2019

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

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) 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 dürfen auf keinen Fall unberechtigten Dritten zugänglich gemacht werden. Der Inhaber haftet für jeden Schaden,

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

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. Dem LRA-Officer ist bekannt, dass er nicht angewiesen werden kann qualifizierte Zertifikate auszustellen, insofern die Identifizierung des Antragstellers nicht korrekt vorgenommen werden kann.

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.