Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Bundesamt für Informatik und Telekommunikation BIT
Swiss Government PKI

NICHT KLASSIFIZIERT

Administration der SG-PKI LRA-Officer und RIO

V.1.2, 17.01.2017

Klassifizierung *	Nicht klassifiziert
Status **	Freigegeben
Projektname	Administration der SG-PKI LRA-Officer und RIO
Projektabkürzung	LRAO Management
Projektnummer	
Projektleiter	SecOff SG-PKI
Auftraggeber	OM SG-PKI
Autor	Beatrice Metaj
Initiale	MetB
Bearbeitende	
Prüfende	SecOff SG-PKI
Genehmigende	SecOff SG-PKI
Verteiler	SG-PKI / LRAOs, RIO
Doc_ID	0100-RV-SGPKI-Administration der LRAOs und RIOs
Kurzbeschreibung	Dies ist die Beschreibung des Ausstellungsprozesses und Handhabung der LRAO Zertifikate für die LRAOs und wie man den RIO Prozess im Amt einführt, bzw. die eigenen RIOs definiert.
Ablageort	Certified PKI

* Nicht klassifiziert, Intern, Vertraulich
** In Arbeit, In Prüfung, Abgeschlossen

Änderungskontrolle, Prüfung, Genehmigung

Version	Datum	Beschreibung, Bemerkung	Name oder Rolle
V1.2	17.01.2017	Initial Version – Neueinbindung in Community und Korrekturen für die neuen Prozesse	Beatrice Metaj

Definitionen, Akronyme und Abkürzungen

Begriff / Abkürzung	Bedeutung
LRAO	Local Registration Authority Officer
RIO	Registration Identification Officer
SecOff	Security Officer der Swiss Government PKI
SG-PKI	Swiss Government PKI
OM	Order Management der SG-PKI
SC	SmartCard
PIN	Personal Identification Number
CMDB	OM SG-PKI interne DB
DB	Datenbank
PSP	Personensicherheitsprüfung der AIOS Fachstelle vom VBS
MLR	Marktleistungsreporting des BIT

1 Einleitung

1.1 Ausgangslage

In den Registrierrichtlinien sind Anforderungen an LRA-Officer und RIOs definiert. Die Registrierrichtlinien geben keine Auskunft über die Aktivitäten der Swiss Government PKI (SG-PKI) welche sicherstellen, dass ein gültiges LRA Zertifikat nur einem aktiven LRA-Officer zugeordnet ist. Ebenfalls wird in den Registrierrichtlinien keine Aussage über die Revokation von LRA-Officer Zertifikaten gemacht. Diese Prozesse wurden von der SG-PKI als notwendig erachtet.

1.2 Zielsetzung des Dokuments

Das vorliegende Dokument definiert die einzelnen Prozessschritte für die Verwaltung und Dokumentation der LRA-Officer und RIOs.

2 Anforderungen an LRA-Officer und RIOs

Die Registrierrichtlinien geben Auskunft über folgende Anforderungen an einen LRA-Officer:

1. *Personensicherheitsprüfung:*

   Jeder LRA-Officer ist einer Personensicherheitsprüfung zu unterziehen. Dies gilt auch für die RIOs (Registration Identification Officer). Das für die LRA-Officer bzw. RIO zuständige Amt bzw. Departement oder Kanton stellt den Antrag für die Personensicherheitsprüfung. Das Formular kann bei den Personaldiensten oder beim VBS, Fachstelle für Personensicherheitsprüfungen bezogen werden. Es ist mindestens die Grundsicherheitsprüfung 10a durchführen zu lassen. Das Resultat der Personensicherheitsprüfung muss dem Security Officer der SG-PKI zugestellt werden.

2. *Vertraulichkeit, Datenschutz:*

   Jeder LRAO hat eine Vertraulichkeitserklärung zu unterschreiben. Diese ist im Formular für die Bestellung des LRAO-Zertifikates eingebunden.

3. *Ausbildung des LRA-Officers:*

   Alle LRA-Officer müssen eine Schulung durchlaufen. Am Ende der Schulung wird mittels eines Examens festgestellt, ob der Teilnehmer genügend Kenntnisse und Fähigkeiten hat, um als LRA-Officer tätig zu sein (Zertifizierungsverfahren). Erfüllt der Teilnehmer die Bedingungen des Zertifizierungsverfahrens nicht, so erhält er keine SmartCard als LRA-Officer und darf diese Aufgaben auch nicht in Stellvertretung ausüben. Fällt der angehende LRAO durch das Examen, muss die Prüfung nach einer Besprechung der wichtigsten Punkte mit dem OM der SG-PKI wiederholt werden.

4. *Ausbildung des RIO:*

   Die RIOs müssen ebenfalls eine Schulung, jedoch mit reduziertem Umfang absolvieren. Die Schulung erfolgt grundsätzlich durch die LRA-Officer. In einzelnen Fällen kann die Schulung nach Absprache und Offerten Bewilligung durch die SG-PKI erfolgen. In der Schulung müssen zumindest die Dokumente und Prozesse zur asynchronen Ausstellung von Zertifikaten der Klasse B und die Richtlinien für den Registration Identification Officer (RIO) behandelt werden. Diese Dokumente sind im Kundenbereich der SG-PKI, in den Schulungsdokumenten zur Klasse B in der jeweils aktuellen Version vorhanden.

5. *Auffrischung der Ausbildung:*

   Der LRA-Officer ist verpflichtet, sich auf dem aktuellen Stand zu halten. Dies umfasst die Kenntnis der Registrierrichtlinien, die dort referenzierten Dokumente, und die allgemein gültigen Richtlinien und Weisungen betreffend Datensicherheit und Datenschutz. Die Aus- und Weiterbildung der LRA-Officers bezüglich allgemeinen Themen, wie beispielsweise Datenschutz, Datensicherheit, Dokumentenverwaltung oder Passwortregelungen, ist nicht Aufgabe der SG-PKI, sondern muss durch die Linie geregelt werden. Er ist verpflichtet an den durch die SG-PKI durchgeführten oder organisierten Kursen für LRAOs teilzunehmen. Stellt der LRA-Officer Mängel in seinem Wissen, Fähigkeiten oder Unklarheiten fest und kann er diese selbst nicht beheben, ist er verpflichtet, dies bei der SG-PKI zu melden. Die SG-PKI wird zusammen mit dem LRA-Officer eine Lösung suchen. Das Nichtbefolgen kann den Entzug der Berechtigung als LRA-Officer, bzw. RIO durch die SG-PKI zur Folge haben.

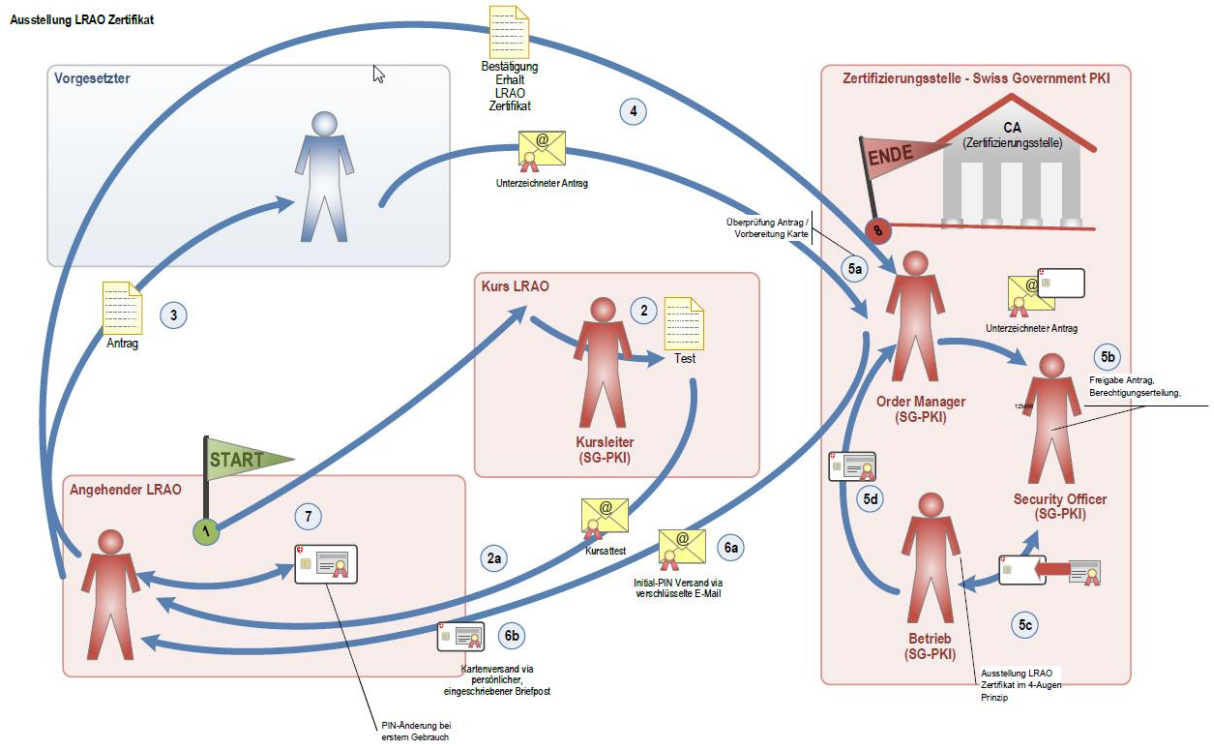
6. *Konformitätsprüfung:*

   Die SG-PKI ist verpflichtet, für die Klasse B alle 18 Monate und für die Klasse A alle 12 Monate die Durchsetzung der CPS zu überprüfen. Dazu gehört auch die Überprüfung der Einhaltung der Richtlinien der LRAs.

3 Prozesse

Die folgenden Prozesse sind gültig für die LRA-Officer der Klasse A und B. Für die Klasse A steht der RIO Prozess nicht zur Verfügung.

3.1 Neuer LRAO

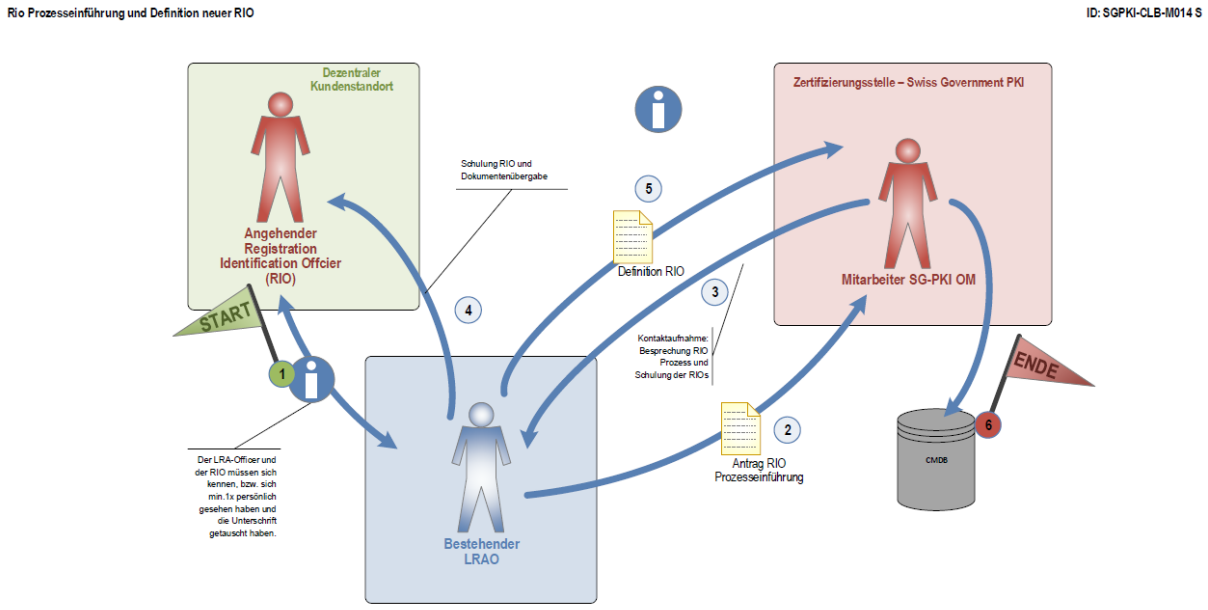


Erläuterungen

Nr.	Element	Erläuterung	Verweis, Hilfsmittel
1	1	Der Antragsteller besucht den Basiskurs für LRAOs der Klasse B oder den Weiterbildungskurs für LRAOs der Klasse A	Kursanmeldung unter: https://www.bit.admin.ch/SG-PKI/06355/index.html?lang=de
2	2	Im Kurs muss er eine Prüfung absolvieren. Das Resultat wird vom Kursleiter in den darauf folgenden Tagen dem Kursteilnehmer mitgeteilt	
2a	2a	Der Kursleiter versendet das Attest des Kurses, bzw. hat das Attest bereits im Kurs verteilt.	
3	3	Der Antrag für LRA-Officer kann nun vom angehenden LRAO ausgefüllt und dem Vorgesetzten zugestellt werden.	Antragsformular LRAO auf www.pki.admin.ch unter dem jeweiligen Zertifikatstyp und den Formularen.
4	4	Der vollständige Antrag, inkl. dem Resultat der PSP, den Kursattest und die Bestätigung der bestandenen Prüfung wird nun der SG-PKI zugeschickt. Die Anträge werden von der Post direkt dem OM der SG-PKI übergeben.	
5	5a	Nun prüft das OM den Antrag auf Vollständigkeit und bereitet die SmartCard für die Ausstellung der Zertifikate vor. Hier wird die SC initialisiert, mit PIN und PUK versehen und bedruckt.	
6	5b	Der Antrag und die vorbereitete SC wird dem SecOff zur Überprüfung und ggf. Ausstellung der Zertifikate weitergegeben.	
7	5c	Die Ausstellung der Zertifikate erfolgt im 4-Augen Prinzip zusammen mit dem Betrieb der SG-PKI. Nach der Ausstellung werden die Berechtigungen des LRAOs auf der TN-Konsole erfasst	
8	5d	Nun ist die SC beim OM bereit für den Versand.	

Nr.	Element	Erläuterung	Verweis, Hilfsmittel
9	6a	Das OM versendet die InitialPIN der SC dem Kunden via verschlüsselte Mail	
10	6b	Das OM versendet die SC und die Erhalts-Bestätigung per eingeschriebener Post dem Kunden.	
11	7	Nun kann der neue LRAO seine PIN ändern.	Die PIN kann auf der LRA-Station im SAC geändert werden.
12	8	Der Kunde muss den Empfang der LRAO SC mittels Formular bestätigen.	

3.2 RIO Prozesseinführung und Definition RIO



Erläuterungen

Nr.	Element	Erläuterung	Verweis, Hilfsmittel
1	1	Min. 1 LRAO muss im Amt bereits bestehen. Dieser muss seinen zukünftigen RIO persönlich gesehen haben und die Unterschrift von Ihm kennen.	
2	2	Der LRAO meldet der SG-PKI die Einführung des RIO Prozesses bei sich im Amt.	
3	3	Das OM der SG-PKI nimmt mit dem LRAO Kontakt auf und bespricht das Einführungsvorgehen.	
4	4	Der LRAO (alternativ kann der Auftrag auch der SG-PKI übergeben werden) schult den angehenden RIO und übergibt Ihm die nötigen Unterlagen	Terms and Conditions / Guidelines / SmartCards
5	5	Der LRAO meldet seinen neuen RIO mittels Formular der SG-PKI	
6	6	Die SG-PKI fügt den neuen RIO in der CMDB ein.	

3.3 Personensicherheitsprüfung

Das Ordermanagement der SG-PKI führt die DB mit dem Datum der Resultate der PSP. Das OM ist verantwortlich, dass die entsprechenden Einträge im MLR und beim Servicedesk nachgeführt werden.

3.4 Vertraulichkeit, Datenschutz

Der zuständige PKI Verantwortliche des Kantons, hat vom angehenden LRA-Officer welcher nicht Mitarbeiter der Bundesverwaltung ist, vor der Ausstellung der Zertifikate auf dem Antrags-Formular die

„Vertraulichkeitserklärung“ unterzeichnen zu lassen. Die Vertraulichkeitserklärung ist im Antragsformular für das LRAO-Zertifikat integriert.

3.5 Ausbildung des LRA-Officer

Die Anmeldung zu den Kursen erfolgt über die Seite: https://www.bit.admin.ch/SG-PKI/06355/index.html?lang=de . Am Ende der Schulung entscheidet der Kursleiter, ob der Teilnehmer genügend Kenntnisse und Fähigkeiten hat, um als LRA-Officer tätig zu sein. Bei einem positiven Entscheid füllt der Kursleiter für den entsprechenden Teilnehmer das Formular „Abnahme Schulung LRA-Officer“ aus. Dieses Dokument oder das Attest des Kurses sind dem Antrag beizulegen. Zusätzlich muss der neue LRAO die Prüfung im Kurs bestehen, um das Zertifikat erhalten zu dürfen. Im Fall dass der LRAO die Prüfung nicht bestanden hat, setzt sich das OM mit dem LRAO in Kontakt um die Prüfung zu besprechen und ggf. zu wiederholen. Die Prüfungsresultate werden vom OM der SG-PKI zur Nachvollziehbarkeit archiviert.

Erfüllt der Teilnehmer die Bedingungen der SG-PKI nicht, so erhält er keine SmartCard als LRA-Officer und darf diese Aufgaben auch nicht in Stellvertretung ausüben.

3.6 RIO Prozess für LRA-Officer der Klasse B

Grundlage für den Einsatz des RIO Prozesses ist ein aktiver LRA-Officer mit einer LRA-Station in einer Organisationseinheit.

Bei Aufnahme und Beendigung des Einsatzes des RIO Prozesses, stellt der LRA-Officer dem Security Officer der SG-PKI das ausgefüllte Formular „RIO Prozess für LRA-Officer der Klasse B“ zu.

Der Betrieb der SG-PKI bestätigt die Erstellung / Löschung der Berechtigungen und der Firewall-Zugriffe auf dem Formular und retourniert das Dokument zur Ablage an das OM. Das OM ist verantwortlich, dass die entsprechenden Einträge in der CMDB nachgeführt werden.

3.7 Ausbildung des RIO

Der LRA-Officer ist verpflichtet den RIO auszubilden und ihm die benötigten Formulare und Unterlagen zur Verfügung zu stellen. Er ist ebenso verpflichtet eine Liste der für ihn tätigen RIOs zu führen.

Der SG-PKI teilt der LRA den ernannten RIO mit dem Formular „Definition RIO für die Klasse B“ mit. Der RIO bestätigt mit seiner Unterschrift auf dem Formular eine Schulung erhalten zu haben. In der Schulung müssen zumindest der asynchrone Ausstellungsprozess (mit RIO, gem. https://www.bit.admin.ch/adminpki/00240/00367/00820/00822/index.html?lang=de), und die Richtlinien für den Registration Identification Officer (RIO) behandelt werden.

Das Formular stellt der LRA-Officer dem OM der SG-PKI zu. Das OM führt eine CMDB mit den nötigen Informationen und archiviert die Unterschriebenen Formulare.

3.8 Auffrischung der Ausbildung

Die SG-PKI ist verpflichtet den LRA-Officer bei neuen Versionen folgende Dokumente online zur Verfügung zu stellen:

- Registrierrichtlinien
- CP/CPS
- Benutzervereinbarung und Nutzungsbedingungen zu den Zertifikatsklassen
- Guidelines zu den Zertifikatsklassen
- Neue Formulare und Dokumente welche die Arbeit der LRA-Officer beeinflussen.
- Für LRA-Officer welche mit dem RIO-Prozess arbeiten: Richtlinien für den Registration Identification Officer (RIO)
- Dieses Dokument

3.9 Aufgabe der LRAO Tätigkeit / Revokation

Wird die LRAO-Tätigkeit auf- oder ganz abgegeben, so müssen u. A. die LRAO Zertifikate revoziert werden. Der Revokationsantrag für die LRAO-Zertifikate ist auf dem Antragsformular für LRAO Karte mitenthalten. Das Formular ist vom scheidenden LRAO auszufüllen und dem OM der SG-PKI zuzustellen.

Die Dokumentation, die der LRAO während seiner Tätigkeit gesammelt hat, muss dem nachfolgendem LRAO abgegeben werden, die Übergabe protokolliert werden, bzw. bei Abgabe der Tätigkeit, der SG-PKI übergeben werden. Eine kurze Checkliste für die Übergabe steht im Anhang zur Verfügung.

Der Prozess für die Revokation der Zertifikate ist im Abschnitt 5.3 der Registrierrichtlinien zur Klasse B dokumentiert und gilt auch für die Zertifikate der LRA-Officer. Der LRA-Officer ist verpflichtet, wenn er seine Rolle nicht mehr ausübt, dem OM der SG-PKI seine LRA-Officer SmartCard per Post zuzustellen. Dieser gibt die SmartCard an den Betrieb der SG-PKI weiter, wo die Zertifikate revoziert und die SmartCard initialisiert werden. Die Berechtigung des ehemaligen LRA-Officers wird in der LRA-Anwendung deaktiviert. Der Betrieb der SG-PKI informiert das OM über die Löschung. Dieser bestätigt die Abgabe der SmartCard in der CMDB. Und aktualisiert das MLR und den Servicedesk.

Zusätzliche Verfahren sind jedoch notwendig um LRA-Officer und die SG-PKI abzusichern. Die Kundendossiers müssen korrekt übergeben werden. Eine Checkliste (siehe Kap. 3.12) soll die Übergabe der für den Betrieb einer LRA nötigen Hilfsmittel erläutern.

3.10 Konformitätsprüfung

Die SG-PKI ist verpflichtet, für die Klasse B alle 18 Monate und für die Klasse A alle 12 Monate die Durchsetzung der CPS zu überprüfen. Dazu gehört auch die Überprüfung der Einhaltung der Richtlinien der LRAs. Die SG-PKI lässt die dezentralen Autoritäten von einer Externen Firma regelmässig auditieren.

3.11 Erneuerung des LRA-Officer Zertifikates

Die Abgelaufenen LRA-Officer Zertifikate werden nicht automatisch erneuert!

Die Erneuerung eines LRA-Officer Zertifikates wird gleichzeitig dazu benutzt, die Personensicherheitsprüfung und die Vertraulichkeitserklärung zu erneuern. Der LRA-Officer stellt für seine Erneuerungsanfrage folgende Dokumente dem Security Officer der SG-PKI zu:

- Erneuerungsantrag LRA-Officer der Klasse B
- Personensicherheitsprüfung (Resultat)
- Schulungsattest
- Resultat des Examens
- Benutzervereinbarung und Nutzungsbedingungen Klasse A/B

Sind alle Unterlagen eingetroffen werden diese vom OM eingesehen und dem SecOff übergeben. Ein neue Karte mit dem LRA-Officer Zertifikat wird gem. Kap. 3.1 erstellt und von der SG-PKI dem Besteller zugesandt.

3.12 Checkliste zur Übergabe der LRAO-Aktivität

1.	Revokationsauftrag an SG-PKI senden
2.	Ggf. Nachfolger an SG-PKI kommunizieren
3.	SmartCard an SG-PKI zurücksenden
4.	Kundendossier an Nachfolger (oder SG-PKI) übergeben
5.	Journale an Nachfolger (oder SG-PKI) übergeben

4 Anhang: Formulare

Formular für Anmeldung/ Mutation und Revokation LRAO Klasse B:

https://www.bit.admin.ch/adminpki/00240/00367/00373/index.html?lang=de

RIO Prozesseinführung und Definition RIO:

https://www.bit.admin.ch/adminpki/00240/00367/00820/00822/index.html?lang=de

Empfangsbestätigung LRAO SmartCard

https://www.bit.admin.ch/adminpki/02218/02219/index.html?lang=de (Wird mit der SmartCard mitgeliefert.)

Checkliste zur Übergabe des LRAO-Amtes:

(Siehe Kap. 3.12)