Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF

Office fédéral de l'informatique et de la télécommunication OFIT
Swiss Government PKI

NON CLASSIFIÉ

Gestion des officiers LRA et des RIO de la SG-PKI

V1.2, 17.01.2017

Classification *	Non classifié
État **	En cours de vérification
Nom du projet	Gestion des officiers LRA et des RIO de la SG-PKI
Abréviation du projet	Gestion des officiers LRA
Numéro du projet	
Responsable du projet	SecOff SG-PKI
Client	Gestion des ordres de la SG-PKI
Auteur	Beatrice Metaj
Abréviation	MetB
Éditeurs	
Instance de vérification	SecOff SG-PKI
Instance de validation	SecOff SG-PKI
Distributeurs	SG-PKI / officiers LRA, RIO
ID du document	0100-RV-SGPKI-Gestion des officiers LRA et des RIO_FR
Description	Description de la gestion des officiers LRA, de leurs certificats, de la manière d'introduire le processus RIO dans l'office et de nommer les RIO.
Classement	Certified PKI

* Non classifié, interne, confidentiel
** En cours d'élaboration, en cours de vérification, validé, terminé

Contrôle des versions, vérification, approbation

Version	Date	Description, remarques	Nom ou fonction
V1.2	19.01.2017	Traduction de la nouvelle version 1.2 DE intégrée dans la communauté Sharepoint, avec la description des nouveaux processus	Beatrice Metaj

Définitions, acronymes et abréviations

Abréviation	Signification
LRA	Local Registration Authority
RIO	Registration Identification Officer
SecOff	Responsable de la sécurité de la Swiss Government PKI
SG-PKI	Swiss Government PKI
NIP	Numéro d'identification personnel
CMDB	Base de données de gestion de configuration (Configuration Management Database) interne à la Gestion des ordres de la SG-PKI
CSP	Contrôle de sécurité relatif aux personnes du service spécialisé Sécurité des informations et des objets du DDPS

Contenu

1 Introduction

1.1 Contexte

Les directives d'enregistrement définissent les exigences relatives aux officiers LRA et aux RIO. Elles garantissent que les certificats LRA valables sont attribués uniquement à des officiers LRA actifs. Elles ne donnent cependant aucune information concernant les activités de la Swiss Government PKI (SG-PKI). Elles ne font pas non plus mention de la révocation des certificats d'officier LRA. La SG-PKI a jugé ces processus nécessaires.

1.2 Objectif du présent document

Le présent document définit toutes les étapes du processus de gestion et de documentation des officiers LRA et des RIO.

1.3 Formulation non sexiste

Par souci de lisibilité, seule la forme masculine est utilisée dans l'ensemble du présent document pour désigner aussi bien les collaboratrices que les collaborateurs.

2 Exigences relatives aux officiers LRA et aux RIO

Les directives d'enregistrement définissent les exigences suivantes relatives aux officier LRA:

1. *Contrôle de sécurité relatif aux personnes:*

   L'officier LRA doit être soumis à un contrôle de sécurité relatif aux personnes, tout comme le RIO. L'office, le département ou le canton compétent pour l'officier LRA ou le RIO se charge de demander la réalisation du contrôle de sécurité. Le formulaire correspondant peut être obtenu auprès des services du personnel ou auprès du service du DDPS chargé du contrôle de sécurité relatif aux personnes. On fera effectuer au minimum le contrôle de sécurité de base 10a. Le résultat de ce contrôle doit être transmis au responsable de la sécurité de la SG-PKI.

2. *Confidentialité et protection des données:*

   L'officier LRA doit signer une déclaration de confidentialité qui est intégrée au formulaire de commande de certificat d'officier LRA.

3. *Formation d'officier LRA:*

   Tous les officiers LRA doivent recevoir une formation spécifique. Au terme de celle-ci, un examen permet de déterminer si le participant dispose des connaissances et aptitudes suffisantes pour exercer l'activité d'officier LRA (processus de certification). Si le participant ne remplit pas les conditions, il ne reçoit pas de carte à puce d'officier LRA et il n'est pas autorisé à exercer les tâches d'officier LRA, même en remplacement. Si le participant échoue à l'examen, il doit le repasser après avoir discuté des points importants avec le service Gestion des ordres de la SG-PKI.

4. *Formation de RIO:*

   Les RIO doivent également suivre une formation, mais de moindre envergure. Celle-ci est en principe dispensée par les officiers LRA, mais elle peut aussi, dans certains cas, être donnée par la SG-PKI après discussion et acceptation des offres. Elle doit porter au moins sur les documents et processus concernant l'émission asynchrone de certificats de classe B et les directives relatives au RIO. Ces documents sont disponibles dans l'espace clients de la SG-PKI, chaque version actuelle correspondante se trouvant dans les documents de formation relatifs aux certificats de classe B.

5. *Mise à jour de la formation:*

   L'officier LRA est tenu de se maintenir à jour, notamment dans ses connaissances sur les directives d'enregistrement, les documents qui y sont référencés ainsi que les directives et instructions en vigueur en général concernant la sécurité et la protection des données. La formation et le perfectionnement de l'officier LRA sur des thèmes généraux, comme la protection et la sécurité des données, la gestion des documents ou les règles relatives au mot de passe, ne relèvent pas de la SG-PKI mais du responsable hiérarchique. L'officier LRA doit participer aux cours spécifiques donnés ou organisés par la SG-PKI. S'il constate qu'il a des lacunes ou des incertitudes au niveau de ses connaissances ou de ses aptitudes et qu'il ne peut pas y remédier lui-même, il est tenu de l'annoncer à la SG-PKI. Celle-ci recherchera une solution avec lui. Si cette procédure n'est pas respectée, la SG-PKI peut retirer l'autorisation à l'officier LRA ou au RIO d'exercer en tant que tel.

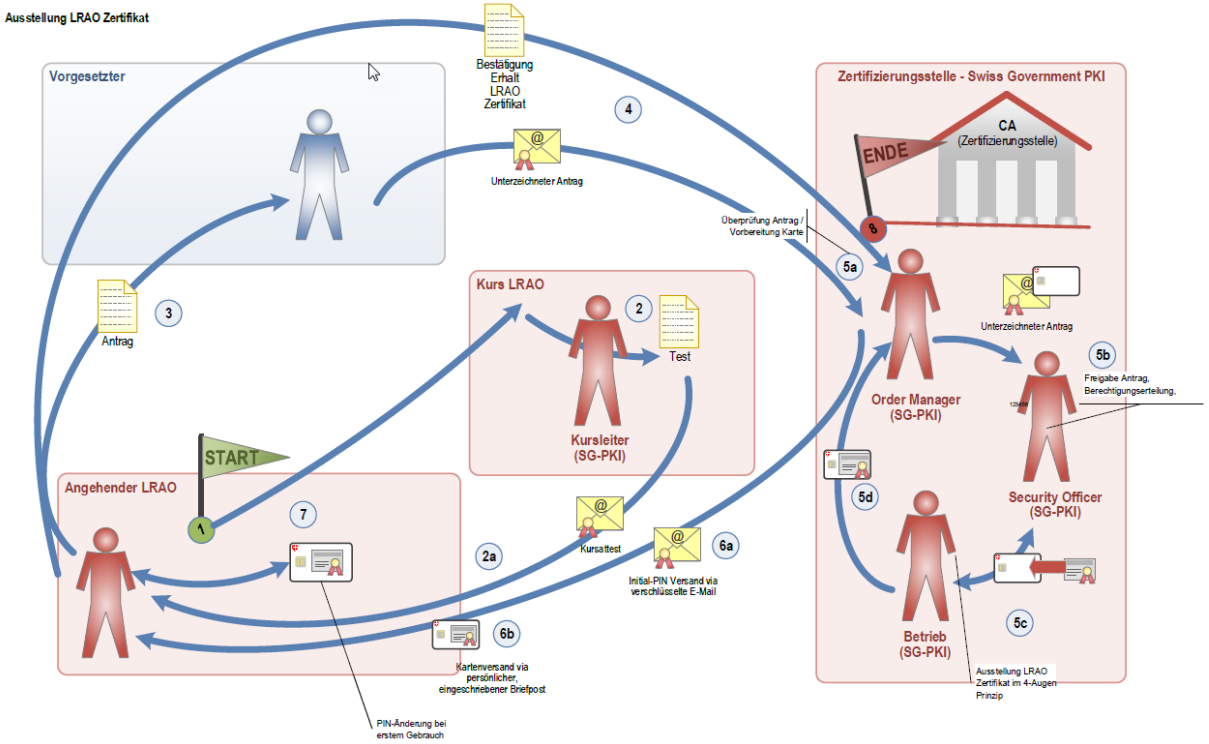
6. *Contrôle de conformité:*

   La SG-PKI est tenue de vérifier l'application du CPS tous les 18 mois pour les certificats de classe B et tous les 12 mois pour les certificats de classe A. Cela inclut le contrôle du respect des directives relatives aux LRA.

3 Processus

Les processus qui suivent sont destinés aux officiers LRA des classes A et B. Le processus RIO n'est pas disponible pour la classe A.

3.1 Nouvel officier LRA

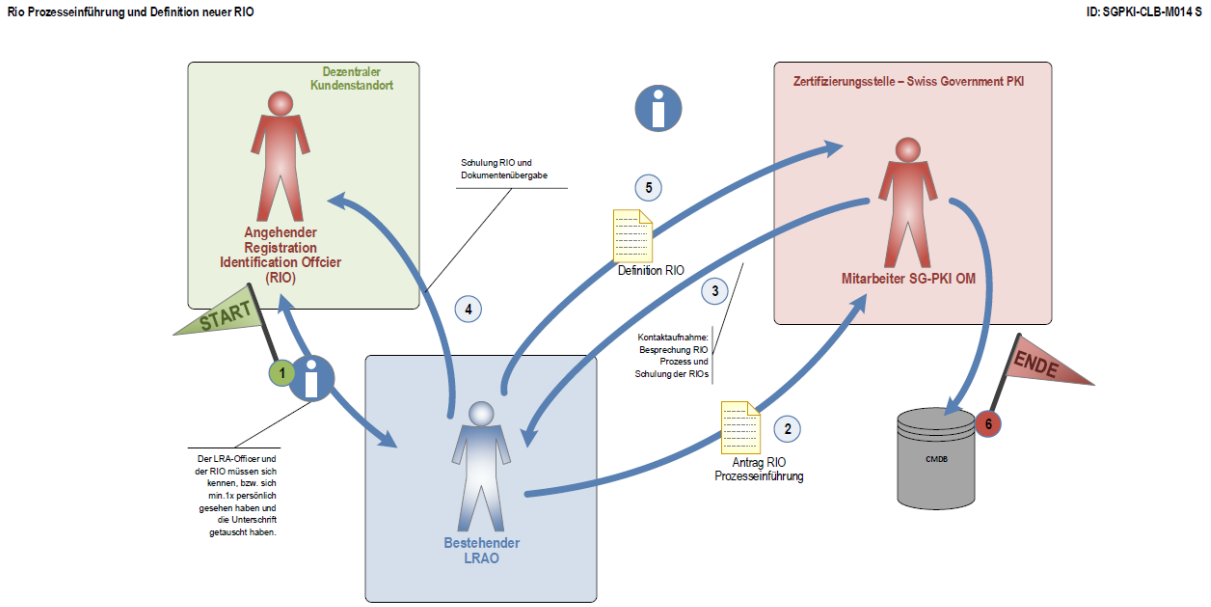


Explications

Nº	Élément	Explication	Référence, aide
1	1	L'auteur de la demande assiste au cours de base destiné aux officiers LRA de classe B ou au cours de perfectionnement destiné aux officiers LRA de classe A.	Inscription aux formations: https://www.bit.admin.ch/admin-pki/06355/index.html?lang=fr
2	2	Il est soumis à un examen à la fin de la formation. Le formateur lui communique son résultat dans les jours qui suivent.	
2a	2a	Le formateur envoie l'attestation de formation, s'il ne l'a pas déjà remise lors des cours.	
3	3	Le futur officier LRA peut désormais remplir le formulaire de demande pour devenir officier LRA et l'envoyer au responsable hiérarchique.	Le formulaire de demande pour devenir officier LRA est disponible sur www.pki.admin.ch, sous le type de certificat correspondant, puis «Formulaires».
4	4	La demande complète incluant le résultat du CSP, l'attestation de formation et la confirmation de réussite à l'examen est envoyée à la SG-PKI. Les demandes sont transmises directement par voie postale au service Gestion des ordres de la SG-PKI.	
5	5a	La Gestion des ordres vérifie si la demande est complète et prépare la carte à puce pour l'émission des certificats. La carte à puce est initialisée et dotée de codes NIP et PUK.	
6	5b	La demande et la carte à puce préparée sont transmises pour vérification au responsable de la sécurité qui, le cas échéant, autorise l'émission des certificats.	
7	5c	Les certificats sont émis selon le principe du double contrôle avec le service Exploitation de la SG-PKI. Après l'émission, les autorisations des officiers LRA sont entrées dans la console TN.	
8	5d	La Gestion des ordres peut désormais envoyer la carte à puce.	

Nº	Élément	Explication	Référence, aide
9	6a	La Gestion des ordres envoie au client le code NIP initial de la carte à puce dans un courriel crypté.	
10	6b	La Gestion des ordres envoie au client la carte à puce et le formulaire de confirmation de réception par courrier recommandé.	
11	7	Le nouvel officier LRA peut désormais modifier son code NIP.	Le code NIP peut être modifié d la station LRA dans SafeNet Authentication Client.
12	8	Le client doit accuser réception de la carte à puce d'officier LRA au moyen du formulaire de confirmation.	

3.2 Introduction du processus RIO et nomination de RIO



Explications

Nº	Élément	Explication	Référence, aide
1	1	L'office doit déjà compter au moins un officier LRA qui doit avoir déjà rencontré en personne son futur RIO et connaître sa signature.	
2	2	L'officier LRA transmet à la SG-PKI une demande d'introduction du processus RIO au sein de son office.	
3	3	Le service Gestion des ordres de la SG-PKI prend contact avec l'officier LRA et discute avec lui de la procédure d'introduction.	
4	4	L'officier LRA (ou, sur demande, la SG-PKI) forme le futur RIO et lui remet les documents nécessaires.	Conditions générales / recommandations / cartes à puce
5	5	L'officier LRA annonce à la SG-PKI la nomination de son nouveau RIO au moyen du formulaire ad hoc.	
6	6	La SG-PKI ajoute le nouveau RIO dans la base de données de gestion de configuration (CMDB).	

3.3 Contrôle de sécurité relatif aux personnes

Le service Gestion des ordres de la SG-PKI intègre la date des résultats du CSP dans la base de données. Il doit s'assurer que les entrées correspondantes sont tenues à jour dans les rapports sur les prestations de marché et par le Service Desk.

3.4 Confidentialité et protection des données

Avant l'émission des certificats, le responsable PKI compétent du canton doit faire signer le formulaire «Déclaration de confidentialité» au futur officier LRA qui n'est pas un collaborateur de l'administration fédérale. Cette déclaration de confidentialité est intégrée au formulaire de demande de certificats d'officier LRA.

3.5 Formation d'officier LRA

L'inscription à la formation s'effectue sur cette page. Au terme de la formation, le formateur décide si le participant dispose des connaissances et aptitudes suffisantes pour exercer l'activité d'officier LRA. Si c'est le cas, il remplit le formulaire «Attestation de formation d'officier LRA» pour le participant correspondant. Ce document (ou l'attestation de formation) doit être joint à la demande. Le futur officier LRA doit en outre réussir l'examen au terme de la formation afin de pouvoir recevoir le certificat. S'il échoue, le service Gestion des ordres prend contact avec lui afin d'en discuter et, le cas échéant, de lui faire repasser l'examen. Les résultats de celui-ci sont archivés par la Gestion des ordres de la SG-PKI afin d'en garder une trace.

Si le participant ne remplit pas les critères de la SG-PKI, il ne reçoit pas de carte à puce d'officier LRA et il n'est pas autorisé à exercer les tâches d'officier LRA, même en remplacement.

3.6 Processus RIO pour les officiers LRA de classe B

L'utilisation du processus RIO repose sur un officier LRA actif disposant d'une station LRA au sein d'une unité organisationnelle.

Au début et à la fin du processus RIO, l'officier LRA envoie au responsable de la sécurité de la SG-PKI le formulaire «Processus RIO pour les officiers LRA de classe B» dûment rempli.

Le service Exploitation de la SG-PKI confirme la création ou la suppression des autorisations et des accès au pare-feu dans le formulaire et retourne le document à la Gestion des ordres pour qu'elle l'archive. Cette dernière doit s'assurer que les entrées correspondantes sont tenues à jour dans les CMDB.

3.7 Formation de RIO

L'officier LRA est tenu d'assurer la formation du RIO et de mettre à sa disposition les formulaires et documents nécessaires, mais aussi de répertorier les RIO qui travaillent avec lui.

L'officier LRA indique à la SG-PKI quels sont les RIO nommés au moyen du formulaire «Nomination de RIO pour la classe B». Le RIO confirme avoir suivi une formation en signant le formulaire. La formation doit porter au moins sur le processus d'émission asynchrone des certificats (via RIO, selon https://www.bit.admin.ch/adminpki/00240/00367/00820/00822/index.html?lang=fr) et sur les directives relatives au RIO.

L'officier LRA envoie le formulaire au service Gestion des ordres de la SG-PKI. Ce dernier intègre les informations nécessaires dans la CMDB et archive le formulaire signé.

3.8 Mise à jour de la formation

En cas de sortie d'une nouvelle version, la SG-PKI est tenue de mettre à la disposition de l'officier LRA les documents suivants en ligne:

- directives d'enregistrement;
- Certificate Policy (CP) et Certification Practice Statement (CPS);
- accords et conditions d'utilisation relatifs aux classes de certificats;
- directives relatives aux classes de certificats;

- nouveaux formulaires et documents ayant une influence sur le travail des officiers LRA;
- pour les officiers LRA qui travaillent avec le processus RIO: directives relatives au RIO;
- le présent document.

3.9 Abandon des tâches d'officier LRA et révocation

Si la personne abandonne en partie ou en totalité son activité d'officier LRA, les certificats d'officier LRA doivent être révoqués. La demande de révocation de certificats d'officier LRA est comprise avec le formulaire de commande de carte à puce d'officier LRA. L'officier LRA sortant doit remplir le formulaire et l'envoyer au service Gestion des ordres de la SG-PKI.

Toute la documentation que l'officier LRA a réunie au cours de son activité doit être transmise à l'officier LRA qui lui succède; cette transmission doit être consignée dans un procès-verbal ou la documentation doit être transférée à la SG-PKI lors de la passation de l'activité. Une brève liste de contrôle pour la transmission est à disposition en annexe.

Le processus de révocation des certificats est indiqué au ch. 5.3 des directives d'enregistrement relatives aux certificats de classe B; il est également valable pour les certificats d'officier LRA. L'officier LRA est tenu de renvoyer sa carte à puce spécifique par voie postale à la Gestion des ordres de la SG-PKI lorsqu'il n'exerce plus son activité. La Gestion des ordres transmet la carte à puce au service Exploitation de la SG-PKI, qui révoque les certificats et qui initialise la carte à puce. Les autorisations de l'officier LRA sortant sont désactivées dans l'application LRA. L'Exploitation de la SG-PKI annonce cette suppression à la Gestion des ordres, qui confirme la réception de la carte à puce dans la CMDB et qui actualise la situation dans les rapports sur les prestations de marché ainsi qu'auprès du Service Desk.

Des procédures complémentaires sont toutefois nécessaires pour protéger l'officier LRA et la SG-PKI. Les dossiers des clients doivent être transmis correctement. Une liste de contrôle (voir ch. 3.12) décrit les étapes de la transmission des documents nécessaires à l'activité d'un officier LRA.

3.10 Contrôle de conformité

La SG-PKI est tenue de vérifier l'application du CPS tous les 18 mois pour les certificats de classe B et tous les 12 mois pour les certificats de classe A. Cela inclut la vérification du respect des directives relatives aux LRA. La SG-PKI charge une entreprise externe de réaliser régulièrement des audits des autorités décentralisées.

3.11 Renouvellement du certificat d'officier LRA

Les certificats d'officier LRA qui ont expiré ne sont pas renouvelés automatiquement.

Le renouvellement d'un certificat d'officier LRA constitue aussi l'occasion de renouveler le contrôle de sécurité relatif aux personnes et la déclaration de confidentialité. L'officier LRA envoie les documents suivants au responsable de la sécurité de la SG-PKI pour demander le renouvellement de son certificat:

- demande de renouvellement de certificat d'officier LRA de classe B;
- contrôle de sécurité relatif aux personnes (résultats);
- attestation de formation;
- résultat de l'examen;
- accords et conditions d'utilisation relatifs aux certificats de classes A et B.

Après réception de ces documents, le service Gestion des ordres les examine, puis les transmet au responsable de la sécurité. Une nouvelle carte avec certificat d'officier LRA est préparée selon le ch. 3.1, puis envoyée par la SG-PKI à l'auteur de la commande.

3.12 Liste de contrôle pour la transmission des activités d'officier LRA

1.	Envoyer une demande de révocation à la SG-PKI
2.	Le cas échéant, communiquer le nom du successeur à la SG-PKI
3.	Renvoyer la carte à puce à la SG-PKI
4.	Transmettre les dossiers des clients au successeur (ou à la SG-PKI)
5.	Transmettre le journal au successeur (ou à la SG-PKI)

4 Annexes: formulaires

a) Formulaire de demande / de modification et de révocation pour officiers LRA de classe B:

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

b) Introduction du processus RIO et nomination de RIO:

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

c) Confirmation de réception de carte à puce d'officier LRA:

https://www.bit.admin.ch/adminpki/02218/02219/index.html?lang=fr (est livré avec la carte à puce)

d) Liste de contrôle pour la transmission des activités d'officier LRA (voir ch. 3.12):

Formulation non sexiste

Par souci de lisibilité, seule la forme masculine est utilisée dans l'ensemble du présent document pour désigner aussi bien les collaboratrices que les collaborateurs.