



04.03.2024 / V1.0

Proposition du nouveau LRAO canton

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

Classe B: demande d'autorisation pour officier LRA

V1.1, 06.12.2023

Nouvel officier LRA

Renouvellement des autorisations LRAO

Mutation Autorisations

Désactivation des autorisations LRAO

Ajouter une autorisation supplémentaire pour un office tiers

Confédération, avec client BAB de l'OFIT

Confédération, sans client BAB de l'OFIT

Organisations proches de la Confédération (par ex. cantons, communes, police)

CC PKI, DDPS VTG

Données de l'officier LRA (Doivent correspondre à l'entrée dans AdminDir)			
Nom:	Mustermann	Prénom:	Max
Suffix:	FG1452		
E-Mail:	max.mustermann@canton.ch		
Autorisations d'émission pour (dép. / office) (propre office et max. 1 office tiers par formulaire)	canton xy		

Conditions d'utilisation générales pour l'officier LRA

Déclaration de confidentialité

Le requérant s'engage, par sa signature, à traiter de manière confidentielle sa carte à puce et son mot de passe; il s'engage également à ne pas transmettre les informations personnelles qui lui ont été communiquées dans le cadre de son travail en tant qu'officier LRA à des tiers, mais uniquement à des collaborateurs internes qui ont impérativement besoin d'accéder à ces informations pour accomplir leurs tâches. Les collaborateurs assumant un rôle d'officier LRA sont tenus de respecter le secret de fonction, si cela n'est pas déjà imposé par leur contrat de travail. Aucune copie partielle ou complète des données et des informations à traiter ne doit être effectuée.

L'officier LRA est tenu de faire désactiver les autorisations LRAO lorsqu'il quitte ses fonctions. La présente déclaration reste valable après le départ de l'officier LRA.

Le certificat d'officier LRA est soumis au document «Convention et conditions d'utilisation pour officiers LRA de la SG PKI», aux «Directives relatives au certificat LRAO de la Swiss Government PKI» et aux «Directives d'enregistrement de la classe B de la Swiss Government PKI». Par sa signature, le futur officier LRA confirme qu'il a lu, compris et accepté toutes les règles et procédures contenues dans ces documents conformément aux CP/CPS applicables de la SG Root CA 1 et s'engage à les respecter pleinement.

1/2



Classe B: demande d'autorisation pour officier LRA NON CLASSIFIÉ

L'autorisation LRAO est explicitement accordée sur un certificat d'authentification existant issu d'un triplet valide de certificats de classe B du LRAO. C'est pourquoi, en cas de renouvellement de ses certificats de classe B, l'autorisation n'est plus valable et le LRAO doit demander un renouvellement pour que l'autorisation soit à nouveau accordée sur le nouveau certificat.

Date d'expiration du certificat de classe B à autoriser:

Suffixe BIT pour client BAB:

* Je confirme avoir lu, compris et accepté la [Convention et conditions d'utilisation pour officiers LRA de la SG-PKI](#) et les [Guidelines relatives au certificat LRAO de la Swiss Government PKI](#).

* Obligatoire

Signature du requérant

Signature électronique Signer électroniquement

* Seules les signatures de la SG-PKI sont acceptées

Contrôle de la fiabilité

L'autorité a pris les mesures autorisées par la loi et que l'on peut raisonnablement exiger d'elle afin de vérifier la fiabilité et l'intégrité du candidat ou de la candidate. La SG PKI recommande aux autorités de prendre les mesures suivantes:

- Exécution du contrôle de sécurité prévu à l'art. 10 de l'ordonnance sur les contrôles de sécurité relatifs aux personnes (OCS; RS 120.4) au service CSP du DDPS et/ou
- Prise de mesures internes de contrôle de la fiabilité, par exemple:
 - contrôle de l'identité du candidat ou de la candidate (passeport ou carte d'identité);
 - vérification des références professionnelles ou personnelles du candidat ou de la candidate;
 - vérification de l'exhaustivité et de la cohérence du curriculum vitae du candidat ou de la candidate;
 - contrôle des qualifications académiques et professionnelles référencées;
 - contrôle des extraits du registre des poursuites et du casier judiciaire.

Confirmation de l'autorité

La personne autorisée à signer pour l'autorité confirme à la SG PKI avoir vérifié la fiabilité du candidat ou de la candidate conformément à la recommandation cidessus ou selon des modalités similaires. L'autorité considère que le candidat ou la candidate est fiable et intègre, et confirme en outre qu'il ou elle dispose des compétences requises pour exercer la fonction sensible d'officier LRA.

Fonction du signataire

Signature électronique

* Seules les signatures de la SG-PKI sont acceptées

Statut : Validé
Version : V1.1, 06.12.2023 2/2

Date d'expiration de la smartcard actuelle BIT BAB

Suffixe de la smartcard BIT BAB

Il faut accepter les guidelines

Signature du requérant avec la smartcard du canton

Signature du responsable PKI ou du responsable de la sécurité du canton