Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF

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

Retourner

16.07.2025

Classe B
Demande LRAO - Mutation autorisations

Statut: publié **V1.5**

☐ **Confédération, avec client BAB de l'OFIT**

☐ **Confédération, sans client BAB de l'OFIT**

☐ **Organisations proches à la Confédération (par ex. cantons, communes, police)**

☐ **CPK, DDPS VTG**

Employerus CPK

Officiers LRA DDPS

Officiers Key Recovery DDPS

Employeurs Helpdesk FUB

☐ **Mutation, ajouter d'autorisation**

Mutation, ajouter d'autorisation comptes d'administrateur (uniquement pour administration fédérale)

☐ **Ajouter une autorisation supplémentaire pour un office tiers**

☐ **Mutation, retirer d'autorisation ***

Mutation, retirer d'autorisation comptes d'administrateur *

* Pour supprimer l'autorisation, il suffit d'apposer sa propre signature.

Données de l'officier LRA (doivent correspondre à l'entrée dans AdminDir)			
Nom: *		Prénom: *	
Suffix: * ?			
E-Mail: *			
Tél.:			
Autorisations d'émission pour (dép. / office) (propre office et max. 1 office tiers par formulaire) *			

* Obligatoire

Conditions d'utilisation générales pour l'officier LRA

Déclaration de confidentialité

La personne requérante s'engage, par sa signature, à traiter de manière confidentielle sa carte à puce et son mot de passe; il ou elle 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 personnes collaborant en interne 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 ou elle quitte cette fonction. 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 des certificats avancés de classe B (pour les personnes physiques) de Swiss Government PKI». Par sa signature, la personne appelée à exercer la fonction d'officier LRA confirme qu'il ou qu'elle a lu, compris et accepté toutes les règles et procédures contenues dans ces documents conformément aux CP/CPS applicables de la SG Root CA I et s'engage à les respecter pleinement.

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 actuel: *

Suffixe BIT pour client BAB pas l'administration fédérale

☐ * Je confirme avoir lu, compris et accepté la Convention et conditions d'utilisation des certificats avancés de classe B (pour les personnes physiques) de Swiss Government PKI

Remarques

Signature du requérant

Signature électronique *

* Seules les signatures de la SG-PKI sont acceptées. Veuillez d'abord remplir tous les champs obligatoires ci-dessus. Une signature sans informations complètes peut entraîner un refus.

* Obligatoire

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 ci-dessus 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 de la personne signataire
Signature électronique du ou de la DSIO, du ou de la DSID ou de la personne responsable PKI *

* Seules les signatures de la SG-PKI sont acceptées

Confirmation office tiers

Si les chemins d'accès à l'autorisation sont demandés pour plusieurs offices, les personnes autorisées à signer de chacun des offices concernés doivent fournir leur signature.
Les personnes autorisées à signer sont:

- au niveau des offices: les DSIO, ainsi que les spécialistes responsables des techniques de la SG-PKI
- au niveau départemental: les DSID, ainsi que les spécialistes responsables des techniques de la SG-PKI
- au niveau cantonal, tribunaux: les responsables PKI de l'unité administrative, les préposés à la sécurité des offices, ainsi que les spécialistes responsables des techniques de la SG-PKI

La personne de l'autorité qui est autorisée à signer confirme à la SG-PKI que l'LRAO susmentionnée devrait être autorisé à délivrer des certificats pour l'office mentionné ci-dessous.

Administration ou unité administrative de la personne signataire	Fonction de la personne signataire
Signature électronique du ou de la DSIO, du ou de la DSID ou de la personne responsable PKI * (uniquement l'autorisation pour un fournisseur tiers)	

* Seules les signatures de la SG-PKI sont acceptées

Confirmation de l'autorisation du compte admin

L'autorisation pour l'émission de certificats pour les comptes d'administrateur (uniquement internes à l'administration fédérale) nécessite la signature du DSID (l'autorisation est toujours valable pour l'ensemble du département).

Le ou la DSID confirme à la SG-PKI que le ou la LRAO susmentionné doit être autorisé à délivrer des certificats d'administrateur pour le département mentionné ci-dessous.

Département
Signature électronique du ou de la DSID (uniquement pour autorisation A-Account)

* Seules les signatures de la SG-PKI sont acceptées