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

31.07.2025

Swiss Government PKI
Directives d'enregistrement de la classe B

Directives d'enregistrement de la Swiss Government PKI pour la LRA

Statut : validé V7.0

Classification *	Non classifié
Statut **	Validé
Mandante	Swiss Government PKI
Auteur	TRF
Gestionnaire	SG PKI OFIT
Vérificateur	Beatrice Metaj, Sébastien Farquet, Cornelia Enke
Approbateur	PKI Management Board
Destinataires	Officiers LRA, RIO, auditeurs
Classement	Certified PKI
Entrée en vigueur	01.08.2025

* Non classifié, interne, confidentiel

** En cours de traitement, en cours de vérification, terminé, validé

Contrôle des modifications, vérification, approbation

Version	Date	Nom ou rôle	Description, remarque
2.91	23.07.2010	Andreas Zürcher	Remplace les versions 2.x, qui sont traitées dans un document séparé pour les classes A et B
2.92		Daniel Stich	Épuration du texte et vérification de la cohérence avec le document CP/CPS, listes de contrôle avec liens vers les directives
2.93		Daniel Stich	Prise en compte des résultats de la révision avec A. Zürcher
2.94		Daniel Stich	Prise en compte des commentaires du LZPPS
3.00	23.02.2012	Daniel Stich	Version finale
3.01	23.04.2012	Daniel Stich	Modification des règles en matière de NIP
3.02	30.01.2013	Daniel Stich	PDF dans les processus RIO et émission des certificats, transmission électronique signée de documents pour le processus RIO, adaptations à la connexion à deux facteurs sur les systèmes clients de l'administration fédérale
3.03	22.04.2013	Tomaso Vasella	Prise en compte des certificats de fonction Adaptation AdminPKI-> Swiss Government PKI Adaptation de l'unité d'organisation d'après ON OFIT
3.04	11.09.2013	Daniel Stich	
3.05	15.01.2015	Daniel Stich	Précisions sur l'identification au moyen de la pièce d'identité
4.00	24.03.2015	Daniel Stich	Utilisation du nouveau modèle, enregistrement dans le système de gestion des documents
4.1	22.09.2016	Daniel Stich	Adaptation aux nouveaux assistants et processus et aux cartes à puce préparées
4.2	24.05.2017	Daniel Stich	Intégration des nouveaux formulaires et des nouvelles listes de contrôle
4.3	29.08.2017	Daniel Stich	Réglementation globale de l'archivage électronique du journal et des justificatifs
5.0	08.11.2017	Daniel Stich	Nouvelle version corrigée et validée
5.1	15.05.2019	Daniel Stich	Adaptation de l'exigence concernant le contrôle de sécurité relatif aux personnes Identification du requérant selon la disposition d'exception « livrets F »
5.2	03.09.2019	Beatrice Metaj	Plusieurs adaptations à la suite du résultat d'un audit interne
5.2	20.09.2019	Beatrice Metaj	Adaptations des formulaires de l'annexe B et des conventions d'utilisation, ajout de directives
5.3	14.10.2019	Cornelia Enke, Daniel Stich, Beatrice Metaj	Feedback / examen annuel
6.0	01.11.2019	PKI Management Board	Validation de la nouvelle version
6.1	29.11.2023	Andreas Ruckstuhl, Adrian Bärlocher	Modifications pour révision par la TRF
6.3	25.04.2024	Beatrice Metaj, Jürgen Weber	Révision de la TRF et préparation pour examen / approbation
6.4	01.05.2024	Beatrice Metaj	Compléments et corrections du Management Board, en particulier au ch. 5.2.3.6 (Vérification de la plausibilité)
6.5	02.07.2024	Sébastien Farquet	Modifications pour une formulation neutre

Version	Date	Nom ou rôle	Description, remarque
6.6	29.07.2024	Stephanie Schäfer, Silvio Pelli, Beatrice Metaj, Sébastien Farquet und Adrian Bärlocher	Compléments et correction de l'équipe de révision
6.7	14.01.2025	Beatrice Metaj, Sébastien Farquet, Cornelia Enke	Dernière révision avant publication
7.0	14.01.2025	Beatrice Metaj	Version validée pour publication

Définitions, acronymes, abréviations et références

- Glossaire
- Liste de référence

Remarque

La LRA (Local Registration Authority) et au moins un officier LRA font l'objet d'un audit, entre autres sur la base du présent document.

Table des matières

Swiss Government PKI **1**
Directives d'enregistrement de la classe B **1**
Directives d'enregistrement de la Swiss Government PKI pour la LRA 1
1. Généralités **6**
1.1 Public cible 6
1.2 Termes et abréviations utilisés 6
1.3 Documents de référence 6
1.4 But du document 6
1.5 Champ d'application 6
1.6 Certificats de classe B de la SG PKI 6
1.7 Supports de sécurité 7
2 Tâches de l'officier LRA et du Registration Identification Officer (RIO) **8**
2.1 Profil requis de l'officier LRA 8
2.2 Tâches et obligations de l'officier LRA 8
2.3 Profil requis du RIO 9
2.4 Tâches du RIO 9
2.5 Contrôle de la fiablité des officiers LRA 10
2.6 Confidentialité, protection des données 10
2.7 Formation du personnel 10
2.8 Mise à jour de la formation 11
3 Aspects généraux opérationnels **12**
3.1 Horaires de service de la LRA 12
3.2 Assistance des officiers LRA 12
3.2.1 Assistance 12
3.2.2 Dysfonctionnements 12
3.2.3 Sécurité 12
3.2.4 Commande 12
3.3 Contrôle des accès 12
3.4 Contrôle de l'accès au client LRA 12
3.5 Directives concernant les clients BAB comportant la fonction de LRA 13
3.6 Formulaires et données des clients 13
3.7 Journal 13
3.8 Délais de conservation 14
3.9 Conservation des cartes à puce préparées 15
3.10 Utilisation et protection des certificats avec autorisation d'officier LRA 15
3.11 Élimination 15
3.11.1 Clean Desk Policy 15
3.11.2 BAB 15
3.11.3 Carte à puce 15
3.12 Règles pour les NIP 15
3.13 Phrase de révocation 16
3.14 Réinitialisation du NIP et gestion de la PUK 16
4 Contrôle de conformité **17**

5 Processus de la Swiss Government PKI classe B 18
5.1 Aperçu 18
5.2 Processus d'émission d'un certificat 19
5.2.1 Qui peut demander un certificat? 19
5.2.2 Comment peut-on demander un certificat? 19
5.2.3 Émission sans RIO 20
5.2.4 Émission avec RIO 25
5.3 Processus de révocation d'un certificat 28
5.3.1 Qui peut demander une révocation ? 28
5.3.2 Comment demander une révocation ? 28
5.3.3 Les raisons d'une révocation sont notamment les suivantes : 29
5.3.4 Procédure 29
5.4 Processus de renouvellement d'un certificat 30
5.5 Processus de récupération de ses propres clés 31
5.6 Processus de récupération de clés de tiers 31
6 Formulaires et listes de contrôle 32
6.1 Formulaire de demande de certificat 32
6.1.1 Formulaire supplémentaire pour les requérants titulaires d'un livret F 32
6.2 Convention et conditions d'utilisation des certificats avancés de classe B 32
6.3 Formulaire de révocation 33
6.4 Formulaire de récupération de clés de tiers 33
6.5 Liste de contrôle pour l'émission d'un certificat sans RIO 33
6.6 Liste de contrôle pour l'émission d'un certificat avec RIO 33
6.7 Liste de contrôle RIO 33
6.8 Liste de contrôle pour la révocation d'un certificat 33
7 Violation des présentes directives 34
8 Procédure d'intervention par paliers 35
9 Propositions de modification 36
Annexe A : Historique des modifications du document 37

Liste des tableaux

Tableau 1 : nombre de points par manifestation pour officiers LRA
Tableau 2 : processus pour classe B 19
Tableau 3 : processus pour les comptes A 19
Tableau 4 : processus pour les comptes T 19
Tableau 5 : différences entre les processus avec et sans RIO 20

1. Généralités

Contenu du présent document

Le présent document contient et explique les directives et prescriptions applicables à l'émission et à l'administration des certificats de la classe B de la Swiss Government PKI (SG PKI).

1.1 Public cible

Ce document s'adresse en premier lieu aux officiers LRA (Local Registration Authority) de classe B formés et travaillant pour les offices et cantons.

1.2 Termes et abréviations utilisés

Les termes et abréviations spécifiques utilisés dans le présent document figurent dans le tableau « Définitions, acronymes et abréviations » publié sur la page www.pki.admin.ch. Ils y font l'objet de brèves explications.

1.3 Documents de référence

Les renvois aux documents de référence sont indiqués entre crochets avec l'indication du numéro correspondant, par exemple [KLB001].

Les documents de référence sont donnés dans leur version en vigueur au moment de la publication des présentes directives d'enregistrement. Les versions plus récentes, si elles existent, sont disponibles en ligne et doivent être utilisées.

1.4 But du document

Le document « Certificate Policy and Certification Practice Statement of the Swiss Government Root CA » (abrégé ci-après « CP/CPS ») [KLB001] est le règlement déterminant pour les certificats de classe B. Il vise à préciser les exigences du CP/CPS concernant la LRA.

1.5 Champ d'application

La présente directive s'applique à toutes les personnes travaillant dans le domaine de la LRA de la classe B. La SG PKI peut déléguer les tâches de la LRA de la classe B à d'autres unités d'organisation. De leur côté, celles-ci désignent le personnel exécutif.

1.6 Certificats de classe B de la SG PKI

Les certificats de classe B sont enregistrés sur un support de données sécurisé (une carte à puce ou une clé USB contenant une puce chiffrée) et sont remis au requérant une fois qu'il s'est enregistré personnellement.

Le titulaire d'un certificat de classe B est une personne physique (pas une organisation, un groupe ou une fonction). Il possède généralement trois paires de clés avec les certificats correspondants. Suivant le type de certificat (certificat de classe B ou certificat de fonction de classe B), le titulaire dispose soit d'une paire de clés pour la signature, d'une deuxième paire pour l'authentification et d'une troisième paire pour le chiffrement des clés et des données, soit d'une seule paire de clés pour l'authentification. Pour les certificats de classe B, les cartes à puce sont dotées d'emblée de trois jeux de trois paires de clés chacun, seul un jeu étant attribué simultanément aux certificats actifs.

Lors du renouvellement de cartes à puce préparées, la Certification Authority (CA) signe le trio de clés suivant. Les anciennes clés et les anciens certificats destinés à la signature et à l'authentification sont ensuite supprimés de la carte à puce. L'ancienne paire de clés destinée au cryptage des clés et des données est conservée sur la carte à puce en vue d'un décryptage ultérieur.

Un titulaire peut posséder à la fois un certificat de classe A, un certificat de classe B et un ou plusieurs certificats de fonction de classe B. Il n'est pas possible d'avoir sur le même support de données sécurisé des certificats de classe A, de classe B et de fonction. Toutefois, un support de données sécurisé peut contenir plusieurs certificats de fonction. Les noms et prénoms de la personne sont clairement identifiables et visibles dans le certificat.

1.7 Supports de sécurité

La liste et les spécifications détaillées des supports de sécurité pris en charge figurent dans la norme « A006 – Smartcard » [BV002] approuvée par le secteur Transformation numérique et gouvernance de l'informatique (TNI) ainsi que dans ses annexes.

2 Tâches de l’officier LRA et du Registration Identification Officer (RIO)

2.1 Profil requis de l’officier LRA

- Haute intégrité personnelle
- Travail précis selon les prescriptions de la SG PKI
- Fiabilité
- Contact aisé avec les clients
- Disposition à exercer une activité en veillant à sa traçabilité
- Disposition à se soumettre à un contrôle de la fiabilité, tel qu’un contrôle de sécurité relatif aux personnes au sens de l’art. 10 de l’ordonnance sur les contrôles de sécurité relatifs aux personnes (OCSP ; RS 120.4 [GV005]) ou à un contrôle similaire, exécuté par sa propre autorité (cf. ch. 2.5).
- Un officier LRA n’est pas autorisé à saisir ou à modifier les entrées de l’Admin Directory, sauf en cas de dérogations écrites confirmées par la direction de l’office concerné ou par l’officier de sécurité compétent de la SG PKI.

2.2 Tâches et obligations de l’officier LRA

L’officier LRA assume les tâches suivantes :

- vérifier la demande ainsi que les formulaires et documents complémentaires requis (cf. ch. 5.2.3.2);
- identifier le requérant (cf. ch. 5.2.3.5);
- vérifier les données de l’Admin Directory ;
- émettre un certificat ;
- révoquer un certificat ;
- informer le requérant en ce qui concerne :
  - les données d’activation ;
  - la protection des données d’activation ;
  - ses droits et ses obligations ;
  - le document « Convention et conditions d’utilisation des certificats avancés de classe B - (pour les personnes physiques) » [KLB021] ;
- le cas échéant, remplir et archiver les listes de contrôle ;
- tenir un journal des activités liées aux certificats et à la LRA ;
- gérer et conserver les dossiers des titulaires de certificats ;
- gérer et éventuellement acquérir les cartes à puce ;
- veiller à la formation et à la qualification des RIO ;
- mettre à la disposition du RIO des copies des documents « Demande RIO en vue de l’émission de certificats de classe B », « Convention et conditions d’utilisation des certificats avancés de classe B - (pour les personnes physiques) » [KLB021] et « Liste de contrôle RIO » ;
- gérer la liste des RIO ;
- valider les demandes de certificats dans le cadre du processus RIO ;
- actualiser de manière proactive ses connaissances relatives aux prescriptions, aux processus

et aux moyens techniques en relation avec les certificats de classe B ;

- conserver et gérer le matériel de la LRA en toute sécurité ;
- respecter les exigences en matière de protection des données (LPD).

2.3 Profil requis du RIO

- Haute intégrité personnelle
- Travail précis selon les prescriptions de la SG PKI et de l'officier LRA qui lui a donné le mandat
- Connaissance fondamentale de la notion de « traçabilité » et compréhension de la nécessité de sa mise en application dans ses activités en tant que RIO
- Fiabilité
- Contact aisé avec les clients
- Un RIO n'est pas autorisé à saisir ou à modifier les entrées de l'Admin Directory, sauf en cas de dérogations écrites confirmées par la direction de l'office concerné ou par l'officier de sécurité compétent de la SG PKI.

2.4 Tâches du RIO

Le RIO traite les demandes de certificats de classe B conformément aux « Directives pour le Registration Identification Officer (RIO) ». Ses tâches sont les suivantes :

- identifier le requérant ;
- informer le requérant en ce qui concerne :
  - les données d'activation ;
  - la protection des données d'activation ;
  - ses droits et ses obligations ;
  - le document « Convention et conditions d'utilisation des certificats avancés de classe B » [KLB021] ;
- vérifier la demande ainsi que les formulaires et documents complémentaires requis (cf. ch. 5.2.3.2) ;
- copier la pièce d'identité et la demande ;
- remplir la liste de contrôle ;
- transmettre à l'officier LRA qui l'a mandaté, par courrier, par coursier ou par voie électronique, la liste de contrôle dûment remplie, les éventuels formulaires complémentaires, la demande signée accompagnée d'une copie d'une pièce d'identité valable, et le document signé *Convention et conditions d'utilisation des certificats avancés de classe B* [KLB021]. S'il choisit la voie électronique : numériser les documents ci-dessus sous forme de fichiers PDF, signer ceux-ci numériquement au moyen de son certificat personnel de classe B et envoyer le tout à l'officier LRA par courrier électronique chiffré. Une fois envoyées, le RIO supprime de son propre système toutes les données qu'il a enregistrées pour être transmises ;
- conservation et gestion sécurisées des cartes à puce préparées.
- Le RIO n'est **pas** autorisé à stocker, de quelque manière que ce soit, des données de personnes pour lesquelles il a procédé à l'identification à la place d'un officier LRA. Il doit transmettre à l'officier LRA compétent, ou supprimer (version numérique) ou détruire (version papier), toutes les informations concernant des personnes dont il dispose.

Un officier LRA peut assumer le rôle d'un RIO, mais pas l'inverse.

2.5 Contrôle de la fiablité des officiers LRA

Avant toute nomination d'un officier LRA, l'autorité prend les mesures que le cadre légal lui permet et celles qui lui semblent raisonnables pour vérifier la fiabilité et l'intégrité du candidat. La SG PKI recommande aux autorités de prendre les mesures suivantes :

- contrôle de sécurité relatif aux personnes au sens de l'art. 10 OCSP [GV005], exécuté par le service spécialisé CSP du Département fédéral de la défense, de la protection de la population et des sports (DDPS)

et / ou

- suivi de mesures internes de contrôle de la fiabilité du candidat, par exemple :
  - contrôle de l'identité (passeport ou carte d'identité) ;
  - vérification des références professionnelles ou personnelles ;
  - vérification de l'exhaustivité et de la cohérence du curriculum vitæ ;
  - contrôle des qualifications académiques et professionnelles référencées ;
  - contrôle des extraits du registre des poursuites et du casier judiciaire.

La personne autorisée à signer pour l'autorité confirme ensuite à la SG PKI avoir vérifié la fiabilité du candidat conformément à la recommandation ci-dessus ou selon des modalités similaires. Elle indique qu'elle considère le candidat comme étant fiable et intègre, et confirme en outre qu'il dispose des compétences requises pour exercer sa future fonction d'officier LRA.

2.6 Confidentialité, protection des données

L'officier LRA doit signer une déclaration de confidentialité, laquelle est intégrée au formulaire « Classe B : demande LRAO ».

Les lois et ordonnances relatives à la protection des données (LPD, GPDo) [GV015, GV016] et à la sécurité de l'information (LSI, OSI) [GV003, GV014] doivent être respectées. Les travaux en tant qu'officier LRA sont effectués pour le compte de la SG PKI. L'officier LRA est personnellement responsable de respecter ces réglementations dans le cadre de son activité.

Il doit veiller en particulier à transmettre les informations concernant des données des clients ou les données importantes de la LRA sous une forme chiffrée, de même qu'à ce qu'aucun tiers non autorisé n'y ait accès.

2.7 Formation du personnel

Tous les officiers LRA doivent recevoir une formation spécifique. Au terme de celle-ci, un test écrit permet de déterminer si le participant présente des connaissances et des aptitudes suffisantes pour exercer l'activité d'officier LRA de classe B.

Si un futur officier LRA échoue au test, il n'obtient pas les autorisations. Il peut cependant suivre à nouveau la formation et repasser l'examen pour prouver qu'il dispose des aptitudes et compétences requises. Si un officier LRA constate qu'il a des lacunes ou des incertitudes dans ses connaissances ou ses aptitudes et qu'il ne peut pas y remédier lui-même, il est tenu de l'annoncer à la SG PKI. Celle-ci cherchera une solution avec lui.

Les RIO doivent suivre une formation d'envergure moindre. Celle-ci est en principe dispensée par l'officier LRA qui les mandate. Elle peut aussi être donnée par la SG PKI. La formation doit traiter au moins des documents référencés « *Vérification de l'identité des requérants, certificats de la classe B* » [KLB003], « Introduction de la procédure RIO pour les officiers LRA de classe B» [KLB027] et « *Convention et conditions d'utilisation des certificats avancés de classe B* » [KLB021].

2.8 Mise à jour de la formation

L'officier LRA est tenu de maintenir ses connaissances à jour, notamment en ce qui concerne les directives d'enregistrement. À cette fin, la SG PKI met à disposition les documents et informations actuels dans l'espace clients du site Internet Swiss Government PKI. Elle s'engage à signaler par courrier électronique les modifications importantes. L'officier LRA est tenu de lire ces informations dès qu'il reçoit le courrier correspondant.

De plus, chaque officier LRA est tenu d'obtenir un total de 20 points de perfectionnement au cours d'une période d'observation de 24 mois. Le tableau ci-après montre quelques-unes des activités qui permettent d'accumuler un nombre de points précis.

Activité	Nombre de points
Cours de base pour officiers LRA (participation)	10
Test réussi concernant le cours de base pour officiers LRA	10
LRAO Summit (1/2 journée, participation et feedback)	10
Brève séance d'information (en ligne, max. 1 heure, feedback)	5
Atelier personnalisé pour officiers LRA (min. 4 participants, sur place)	5 à 10 (selon le contenu)
Modules d'apprentissage en ligne (y c. test)	max. 5
Audit LRA (participation)	5
Sessions Q&A (en ligne, max. 1 heure, feedback)	2

Tableau 1: nombre de points par manifestation pour officiers LRA

La SG PKI propose régulièrement des cours de perfectionnement et de répétition pour les officiers LRA (ateliers ou LRAO Summit). Ceux-ci peuvent être obligés d'y prendre part s'ils ont peu de points, ou l'autorisation d'exercer la fonction d'officier LRA peut leur être retirée. Le solde de points actuel et individuel peut être demandé à la SG PKI par courrier électronique à l'adresse pki-info@bit.admin.ch. La SG PKI ne publie aucune liste de points.

3 Aspects généraux opérationnels

3.1 Horaires de service de la LRA

Les heures de service de la LRA sont fixées par les unités d'organisation responsables. Elles doivent être aménagées de manière à ce que les tâches urgentes puissent être effectuées dans un délai raisonnable (p. ex. effectuer des révocations immédiatement, au maximum dans un délai d'un jour ouvrable).

3.2 Assistance des officiers LRA

3.2.1 Assistance

Les officiers LRA peuvent demander l'assistance de l'équipe d'exploitation de la SG PKI selon les indications du catalogue des produits et services et l'accord de niveau de service (Service Level Agreement, SLA) en vigueur. Les détails sont expliqués sur le site Internet de la SG PKI.

3.2.2 Dysfonctionnements

En cas de dysfonctionnements, il convient de prendre contact avec l'équipe d'exploitation en appelant le Service Desk de l'OFIT (+41 (0)58 465 88 88). L'officier LRA peut aussi créer un ticket en utilisant le RoBIT. En cas d'urgence survenant durant les heures convenues dans l'accord de niveau de service, le Service Desk de l'OFIT (tél. +41058 465 88 88) peut mettre les officiers LRA en contact avec la SG PKI.

Tout dysfonctionnement du client BAB doit aussi être signalé au Service Desk de l'OFIT.

3.2.3 Sécurité

En cas de communications et de questions urgentes en matière de sécurité, il convient de prendre contact avec un officier de sécurité de la SG PKI par l'intermédiaire du Service Desk de l'OFIT (+41 (0)58 465 88 88). L'adresse électronique pki-secoff@bit.admin.ch peut être utilisée pour les communications ou les questions moins urgentes concernant la sécurité.

3.2.4 Commande

Les commandes et les questions générales peuvent être adressées à l'équipe MAC Manager de l'OFIT sous forme de MAC (Move/Add/Change) ou au Service Desk de l'OFIT sous forme de Service Request (+41 (0)58 465 88 88). L'adresse électronique pki-info@bit.admin.ch ne peut plus être utilisée pour ces demandes.

3.3 Contrôle des accès

Les équipements de la LRA peuvent se trouver dans un bureau individuel, mais pas dans des locaux auxquels peuvent accéder des personnes non autorisées, p. ex. des salles de réunion, des locaux d'infirmerie, etc. Les locaux devraient être facilement accessibles aux requérants et leur offrir suffisamment d'intimité pour saisir leur NIP personnel et la phrase de révocation. S'il s'agit de bureaux paysagers partagés avec des personnes n'exerçant aucune fonction de la LRA, ils doivent prévoir une section protégée ou séparée réservée aux tâches de la LRA. Les locaux en question doivent offrir des possibilités suffisantes pour mettre sous clé le matériel LRA tels que les formulaires et les données des clients, tout en offrant une sphère privée adéquate en vue de l'émission des certificats.

3.4 Contrôle de l'accès au client LRA

L'accès au client BAB comportant la fonction de LRA est protégé par une authentification à deux facteurs. Le client BAB est équipé d'un chiffrement du disque. Les applications de la LRA ne peuvent être lancées qu'avec des autorisations d'officier LRA figurant sur un certificat d'authentification de classe B. Aucune autre personne, y compris d'autres officiers LRA, n'est autorisée à accéder aux cartes à puce personnelles comprenant les autorisations d'officier LRA. La carte à puce doit toujours être emportée avec soi ou mise sous clé. Lorsque l'officier LRA ne travaille pas sur le client BAB, il doit

toujours retirer la carte à puce du lecteur et la conserver en lieu sûr ou l'avoir avec lui. Le NIP nécessaire pour la carte à puce ne peut être conservé par écrit que s'il est mis sous clé séparément de la carte à puce elle-même. Il doit être modifié immédiatement si l'on soupçonne qu'une autre personne le connaît. En cas de perte de la carte à puce, les certificats correspondants doivent être bloqués sans délai. Un officier LRA de la même unité peut généralement s'en charger. En outre, la perte doit être immédiatement signalée au Service Desk de l'OFIT et à la SG PKI.

3.5 Directives concernant les clients BAB comportant la fonction de LRA

L'utilisation du client BAB avec la fonction de LRA est soumise à des règles de sécurité strictes ainsi qu'à la loi sur la sécurité de l'information [GV003], à l'ordonnance sur la sécurité de l'information [GV004] et au document E026 - directive d'utilisation du système de poste de travail DTI-BK [BV003]. Il est strictement interdit :

- d'utiliser le client BAB pour d'autres tâches que pour celles qui sont prévues expressément ;
- d'installer ou de commander soi-même un logiciel ;
- de procéder à des modifications de la configuration logicielle ou matérielle.

Le client BAB comportant la fonction de LRA doit être protégé contre tout accès par des tiers.

3.6 Formulaires et données des clients

Les formulaires délivrés par la SG PKI doivent être impérativement utilisés et conservés dans le dossier des clients, sauf si d'autres solutions autorisées (papier ou forme électronique) sont mentionnées expressément. L'utilisation d'autres formulaires ou solutions électroniques est interdite pour des raisons de traçabilité. Les versions actuelles des formulaires sont publiées en ligne et doivent être utilisées.

Les dossiers des clients (formulaires de demande, feuilles d'information, demandes de révocation, etc.) doivent être conservés sous clé (Cleandesk Policy). Soit la pièce est verrouillée et uniquement accessible aux officiers LRA, soit les documents sont mis sous clé dans une armoire que seuls les officiers LRA peuvent ouvrir. Chaque officier LRA d'une LRA doit avoir accès à tous les dossiers des clients de la LRA.

Si les dossiers des clients sont gérés par voie électronique, les données doivent être enregistrées sur un lecteur auquel seules des personnes autorisées (officiers LRA et auditeurs) ont accès. De plus, il faut veiller au respect des conditions énoncées au ch. 3.8 « Délais de conservation ». Tous les justificatifs archivés doivent être disponibles en tant que document PDF/A et signés avec le certificat de classe B de l'officier LRA compétent ou du RIO requérant.

3.7 Journal

L'officier LRA exécutant consigne dans le journal toutes les activités de la LRA concernant l'émission et la révocation de certificats ainsi que d'autres événements importants. Les activités et événements suivants de la LRA, notamment, sont importants :

- émission de certificats ;
- révocation de certificats ;
- récupération de clés ;
- réception de nouvelles cartes à puce préparées ;
- le cas échéant, numéro de mandat interne (p. ex. numéro de ticket dans le système de saisie des mandats) ;
- changements concernant les officiers LRA (nouveaux, etc.) ;
- changement du/des site(s) de la LRA ;

- changements importants dans les processus (nouveaux formulaires, nouveau déroulement, nouvelles archives, etc.) ;
- erreurs, problèmes et particularités rencontrés dans les processus susmentionnés.

Les journaux des officiers LRA peuvent être écrits à la main (voir « Classe B : journal de l'officier LRA de la Swiss Government PKI ») ou gérés par voie électronique. Dans ce dernier cas, le journal doit être imprimé chaque soir, puis signé et classé par l'officier LRA exécutant. Comme alternative, les journaux électroniques peuvent être exportés quotidiennement dans un fichier PDF/A, signés avec le certificat de classe B de l'officier LRA et dotés de l'horodatage Time Stamping Authority (TSA) de la SG PKI. Il est également possible d'utiliser le modèle de journal PDF comprenant les entrées dont chaque ligne peut être signée numériquement. En principe, il est permis de tenir plusieurs journaux par LRA (p. ex. par officier LRA, par office, par mois, etc.), pour autant que la chronologie et l'exhaustivité restent garanties. En outre, tous les officiers LRA doivent avoir accès à tous les journaux.

Si les journaux sont gérés par voie électronique, les données doivent être enregistrées sur un lecteur auquel seules des personnes autorisées (officiers LRA et auditeurs) ont accès. De plus, il faut veiller au respect des conditions énoncées au ch. 3.8 « Délais de conservation ».

Une entrée de journal doit comporter au moins les informations suivantes :

1. Numéro d'ordre de l'inscription
2. Date
3. Client (personne demandant le certificat / personne titulaire du certificat)
4. Activité (CS : certificat standard ; CFA : certificat d'administrateur ; CFT : certificat de test ; E : émission ; R : révocation ; K : récupération des clés)
5. En cas de révocation : ancienne carte à puce retirée oui / non
6. Visa de l'officier LRA exécutant

3.8 Délais de conservation

Les formulaires, les données des clients et les journaux mentionnés aux ch. 3.6 « Formulaires et données des clients » et 3.7 « Journal » doivent être archivés dans tous les cas pendant au moins 11 ans après l'échéance du certificat. Durant ce laps de temps, les archives doivent être accessibles aux officiers LRA et la SG PKI doit pouvoir les consulter. La protection des accès à ces données doit être garantie même lorsque le dossier d'un client est géré par voie électronique (aucun accès aux données par des personnes autres que des officiers LRA).

Lorsqu'il quitte son poste, l'officier LRA est tenu de remettre tous les dossiers des clients, les journaux et le reste du matériel de la LRA à la personne qui lui succède dans l'organisation ou à la SG PKI.

Les documents papier peuvent être scannés pour être archivés, enregistrés au format PDF/A, signés et dotés de l'horodatage TSA de la SG PKI. S'il s'agit de documents isolés, la signature avec le certificat de classe B de l'officier LRA qui les a initialement exécutés suffit. Si plusieurs documents sont numérisés (p. ex. les documents d'un mois ou d'une année entière dans un seul document PDF/A), deux officiers LRA doivent signer numériquement le document PDF/A et confirmer ainsi le processus de migration correct et sans rupture du support papier vers le support électronique. Il s'agit de garantir que l'on peut retrouver des documents isolés. Le stockage électronique doit être protégé contre l'accès par des personnes autres que des officiers LRA. Après numérisation selon ces directives, les documents papier peuvent être détruits.

3.9 Conservation des cartes à puce préparées

Les cartes à puce préparées et les autres supports de données sensibles doivent être conservés en lieu sûr. Il faut soit verrouiller le local auquel seuls les officiers LRA peuvent accéder, soit ranger les cartes à puce dans une armoire dûment fermée, dont seuls les officiers LRA possèdent la clé.

3.10 Utilisation et protection des certificats avec autorisation d'officier LRA

Les certificats avec autorisation d'officier LRA ne doivent être utilisés qu'aux fins prévues et ne doivent pas être remis à des tiers. Les officiers LRA sont aussi tenus de protéger leurs clés privées et certificats se trouvant sur la carte à puce au moyen de données d'activation, conformément au ch. 3.4 « Contrôle de l'accès au client LRA ».

3.11 Élimination

3.11.1 Clean Desk Policy

Les documents papier liés aux activités de la LRA (directives, listes de contrôle, notes, etc.) ou à la clientèle (demandes de certificats, listes, etc.) qui ne sont plus utilisés doivent être éliminés à l'aide d'une déchiqueteuse ou d'un conteneur de sécurité. Les cartes à puce qui ne sont plus nécessaires doivent être perforées ou déchiquetées avant leur élimination.

Les documents dont on a encore besoin ne doivent pas être visibles de tous, ou déposés sur des tables ou dans des classeurs accessibles à quiconque, et doivent être archivés en toute sécurité.

3.11.2 BAB

Le BAB est éliminé par le service d'assistance de l'OFIT (Service Desk).

3.11.3 Carte à puce

La carte à puce doit être détruite avant d'être éliminée (p. ex. en faisant un trou dans la puce).

3.12 Règles pour les NIP

Le titulaire de certificats utilise des NIP (mots de passe) pour activer ses jetons de sécurité ou ses clés privées. Un NIP diffère en principe du mot de passe qui est utilisé par exemple pour se connecter aux applications [Guide rapide : Règles pour le code PIN des cartes à puce sous "Émission de certificats (Issuing)"]. Chaque titulaire de certificats choisit son propre NIP. Concernant ce choix, les règles sont les suivantes :

- *longueur :* le NIP doit comprendre au moins six caractères ;
- *nombre d'essais :* la carte à puce doit se bloquer automatiquement après cinq tentatives erronées ;
- *complexité* : la composition du NIP peut être définie librement (il est possible de choisir un code composé exclusivement de chiffres). Il est interdit d'utiliser des NIP faciles à deviner (p. ex. l'identifiant d'utilisateur ou 123456) ;
- *validité* : le NIP doit être changé dès que l'on soupçonne qu'un tiers en a connaissance. Lorsque le cycle de vie de la carte à puce touche à sa fin, il faut choisir un nouveau NIP pour la nouvelle carte ;
- *fonction unique* : un NIP correspond à une seule carte à puce.

On évitera d'utiliser des caractères spéciaux à cause des spécificités linguistiques des claviers.

3.13 Phrase de révocation

La phrase de révocation se compose d'une question générale et de la réponse personnelle du requérant.

La réponse à la question doit être choisie de manière à ne pas pouvoir être déduite ou devinée facilement par des tiers. En outre, le requérant doit la connaître de façon si évidente qu'il peut toujours la donner sans aucun doute ni problème.

La phrase de révocation sert à identifier le titulaire du certificat en cas de contact téléphonique avec l'officier LRA, par exemple lors d'une demande de révocation de ses certificats, ou avec le Service Desk chargé du processus de réinitialisation du NIP.

3.14 Réinitialisation du NIP et gestion de la PUK

Pour ses cartes à puce préparées, la SG PKI a développé un système électronique centralisé avec gestion des PUK. Ce système conserve la PUK de manière chiffrée sur l'un des serveurs de la SG PKI et la met à la disposition de la carte à puce en arrière-plan pendant le processus de déblocage. La PUK n'est visible à aucun moment.

Les principes suivants s'appliquent au personnel d'assistance ou aux officiers LRA :

- Pour réinitialiser un NIP, il faut faire appel à un superutilisateur compétent en la matière. Ce superutilisateur peut ouvrir un ticket interne pour la carte concernée dans une application Web, après en avoir dûment identifié le titulaire du NIP. Il peut aussi procéder à l'identification du titulaire du NIP par téléphone à l'aide de la phrase de révocation. Ensuite seulement, le titulaire pourra faire réinitialiser son NIP par un utilisateur spécialisé dans la réinitiatlisation des NIP (PIN Reset User, PRU).
- Pour débloquer une carte, il faut aussi s'adresser à un PRU. Celui-ci lance l'assistant de réinitialisation du NIP, puis confirme avoir clairement identifié la personne présente comme étant le titulaire du NIP de la carte à puce bloquée et lui donne la possibilité de réinitialiser son NIP.
- Pour ce faire, le PRU doit « prêter » son ordinateur à la personne concernée, vu que cette dernière ne peut pas effectuer la procédure d'authentification à deux facteurs sur son ordinateur du fait du blocage de sa carte à puce. La personne concernée doit être sur place avec le PRU et insérer sa carte à puce dans un second lecteur de cartes relié à l'ordinateur du PRU.
- Les fonctions de superutilisateur compétent pour la réinitialisation et de PRU ne peuvent pas être assumées simultanément par la même personne. Les autorisations s'excluent mutuellement pour conserver le principe de double contrôle inhérent à la procédure de réinitialisation du NIP.

La procédure de réinitialisation du NIP des cartes à puce préparées est exposée en détail dans le guide « Quickguide : PIN Reset ».

4 Contrôle de conformité

La SG PKI est tenue de vérifier l'application du CP/CPS [KLB001]. Fait partie de cette vérification notamment le contrôle du respect des présentes directives d'enregistrement par les officiers LRA. Le contrôle de conformité peut être effectué par la SG PKI elle-même ou par un service externe mandaté par elle. Les officiers LRA sont tenus de collaborer lors de ce contrôle et de garantir l'accès aux processus et aux documents.

S'ils ne réussissent pas le contrôle de conformité, les officiers LRA peuvent se voir retirer l'autorisation d'exercer cette fonction. En cas de manquements particulièrement graves, tous les certificats d'utilisateur délivrés par l'officier LRA concerné peuvent être révoqués.

5 Processus de la Swiss Government PKI classe B

5.1 Aperçu

Il existe plusieurs types de certificats de classe B. Les tableaux ci-après donnent une vue d'ensemble des processus applicables selon le type de certificats :

Classe B pour les comptes U ou les comptes X (compte d'utilisateur)
La carte à puce est initialisée pendant le processus de préparation de la SG PKI.
Lors de cette préparation, trois jeux de trois paires de clés (signature, authentification, chiffrement) sont générés de manière externe, puis enregistrés sur la carte à puce.
Lors de l'émission, trois certificats sont générés sur la carte (pour la signature, l'authentification et le chiffrement).
La récupération des clés sur une carte tierce (procuration) n'est pas possible.
La récupération de la clé de chiffrement privée est possible.
Un processus RIO est possible.
Un renouvellement est possible au maximum deux fois.

Tableau 2 : processus de classe B

Certificat de fonction de classe B pour les comptes A (administrateur)
La carte à puce est initialisée pendant le processus de préparation de la SG PKI.
Lors de cette préparation, trois jeux de trois paires de clés (signature, authentification, chiffrement) sont générés de manière externe, puis enregistrés sur la carte à puce.
Lors de l'émission, seul le certificat servant à l'authentification est généré sur la carte à puce.
La récupération des clés sur une carte tierce (procuration) n'est pas possible.
La récupération de la clé d'authentification privée n'est pas possible.
Aucun processus RIO n'est prévu.
Aucun renouvellement n'est autorisé.

Tableau 3 : processus pour les comptes A

Certificat de fonction de classe B pour les comptes T (test)
La carte à puce est initialisée pendant le processus de préparation de la SG PKI.
Lors de cette préparation, trois jeux de trois paires de clés (signature, authentification, chiffrement) sont générés de manière externe, puis enregistrés sur la carte à puce.
Lors de l'émission, trois certificats sont générés sur la carte (pour la signature, l'authentification et le chiffrement).
La récupération des clés sur une carte tierce (procuration) n'est pas possible.
La récupération de la clé de chiffrement privée est possible.
Un processus RIO est possible.
Un renouvellement est possible au maximum deux fois.

Tableau 4 : processus pour les comptes T

5.2 Processus d'émission d'un certificat

On distingue deux variantes du processus :

- Processus d'émission sans RIO
- Processus d'émission avec RIO

Ci-après, le processus sans RIO est appelé « émission sans RIO » et le processus avec RIO « émission avec RIO ».

Les différences entre les processus avec et sans RIO sont représentées dans le tableau ci-dessous :

Processus sans RIO	Processus avec RIO
L'officier LRA procède à l'identification personnelle du requérant. En guise de preuve, il scanne la pièce d'identité du requérant et éventuellement d'autres documents nécessaires.	Le RIO procède à l'identification personnelle du requérant. En guise de preuve, il copie la pièce d'identité sur le formulaire de demande dûment rempli et éventuellement d'autres documents nécessaires. Le RIO remplit la liste de contrôle et transmet ces documents ainsi que le formulaire signé « Convention et conditions d'utilisation des certificats avancés de classe B » [KLB021] à l'officier LRA compétent.
L'officier LRA procède à la vérification du requérant dans l'Admin Directory.	Le RIO procède à la vérification du requérant dans l'Admin Directory.
L'officier LRA instruit le requérant sur les données d'activation et leur protection.	Le RIO instruit le requérant sur les données d'activation et leur protection.
Dans l'assistant d'enregistrement (Walk-In-Wizard), l'officier LRA établit le certificat pour le requérant.	La demande est contrôlée et validée. Ensuite, l'officier LRA demande l'émission des certificats dans l'assistant d'enregistrement et envoie le numéro du ticket électronique de déblocage (code de sécurité) au requérant ou au RIO.
Le requérant saisit son NIP et les données destinées à la révocation par téléphone (phrase de révocation) à la dernière étape de l'assistant d'enregistrement.	Le requérant saisit son NIP et les données destinées à la révocation par téléphone (phrase de révocation) lors du déblocage de la carte à puce avec l'assistant d'enregistrement.

Tableau 5 : différences entre les processus avec et sans RIO

5.2.1 Qui peut demander un certificat?

Dans la demande d'autorisation pour officier LRA, la hiérarchie définit pour quelles unités d'organisation et quels collaborateurs des certificats peuvent être émis. L'appartenance organisationnelle du requérant doit concorder avec l'autorisation de l'officier LRA. Concrètement, cela signifie que l'inscription du requérant dans Admin Directory doit figurer dans le même répertoire que celui qui a été validé pour l'officier LRA ou que les répertoires autorisés doivent être enregistrés dans le compte de l'officier LRA.

Les personnes mineures (p. ex. les apprentis) peuvent également demander des certificats de classe B. Lors de l'émission de ces certificats, l'officier LRA doit veiller consciencieusement à l'obligation d'information.

Les certificats de classe B d'un officier LRA doivent être demandés à un autre officier LRA et établis par ce dernier. Un officier LRA ne peut en aucun cas se délivrer un certificat de classe B à lui-même.

5.2.2 Comment peut-on demander un certificat?

L'officier LRA ou le responsable PKI détermine de quelle manière un certificat peut être demandé (par écrit à l'aide d'un formulaire, MAC dans Remedy, etc.). En principe, le processus de commande doit être traçable jusqu'à 11 ans après l'échéance du certificat. La SG PKI met à disposition un formulaire qui comprend toutes les données requises pour la demande (« Demande de certificats personnels de classe B à la Swiss Government PKI »).

Lorsque des certificats sont commandés pour des cas exceptionnels (p. ex. lorsque le requérant peut uniquement présenter un livret F), les formulaires supplémentaires de la SG PKI prévus pour l'exception concernée doivent être complétés et annexés à la demande dans tous les cas.

5.2.3 Émission sans RIO

Le client LRA doit être utilisé conformément aux documents de formation de l'officier LRA et aux guides concernant les différents assistants. La présente directive prime en cas de contradiction.

L'officier LRA procède en suivant la « *Liste de contrôle : émission de certificats de classe B* ».

5.2.3.1 Vérifier l'entrée dans Admin Directory

Le requérant doit impérativement être enregistré dans Admin Directory pour qu'un certificat puisse être émis à son intention.

Les conditions suivantes doivent être remplies :

1. Une adresse électronique complète et plausible doit être spécifiée dans le champ « Mail ». Concernant les certificats de fonction pour les comptes A : l'adresse électronique doit être clairement identifiable au moyen du suffixe « Admin », « ADM » ou d'un suffixe similaire. Concernant les certificats de fonction pour les comptes T : l'adresse électronique doit être clairement identifiable au moyen du suffixe « Test », « TST » ou d'un suffixe similaire.
2. S'il existe plus d'une entrée dans Admin Directory (nom et prénom identiques) : l'entrée pour laquelle le certificat doit être établi peut-elle être identifiée sans équivoque à l'aide du suffixe du nom ?

Si le requérant n'est pas inscrit ou est inscrit de manière incorrecte dans l'annuaire, l'administrateur de l'Admin Directory de l'office doit ajouter ou modifier l'entrée. La procédure ne pourra continuer que lorsque le requérant sera enregistré correctement dans Admin Directory (en général, la reproduction des données dure au moins une nuit). L'officier LRA peut vérifier l'entrée saisie dans Admin Directory dans l'assistant d'enregistrement, par exemple.

5.2.3.2 Contrôler le formulaire de demande

Il faut contrôler que le formulaire de demande est complet et correct.

1. Le requérant est-il autorisé, selon le point 5.2.1, à faire une demande auprès de cet officier LRA ?
2. Les données du requérant sur le formulaire correspondent-elles à l'entrée saisie dans Admin Directory ?
3. Le formulaire est-il daté et signé correctement ?
   Au lieu de demandes individuelles, le responsable RH concerné peut aussi envoyer une liste des nouveaux collaborateurs à l'officier LRA compétent. La liste doit contenir au moins les mêmes données concernant les collaborateurs que les champs obligatoires du formulaire de demande. Au sein de l'OFIT, un MAC est disponible dans Remedy pour commander des certificats de classe B.

Il est nécessaire de remplir un formulaire de demande, qu'il s'agisse d'émettre un premier certificat ou les certificats suivants.

Le formulaire de demande peut aussi rempli et signé au moment de l'émission du certificat.

5.2.3.3 Rendez-vous pour l'émission du certificat

Une date doit être convenue avec le requérant pour l'émission du certificat. Pour ce faire, un courrier électronique est envoyé à l'adresse figurant sur la demande (exception : compte ADM sans boîte aux lettres électronique). Ce courrier doit contenir les informations suivantes :

1. Proposer une ou des date(s) pour l'émission du certificat
2. Demander au requérant de prendre avec lui une pièce d'identité valable. Celle-ci ne doit pas être échue au moment de l'inscription. Pour les dérogations, il faut apporter les formulaires et documents supplémentaires définis pour l'exception concernée (voir ch. 5.2.3.5 « Contrôler l'identité du requérant »).
3. Demander au requérant de réfléchir à un NIP, en lui rappelant les règles en matière de NIP figurant au ch. 3.17 « Règles pour les NIP ».
4. Demander au requérant de préparer une phrase de révocation.
5. Indiquer les coordonnées de l'officier LRA en cas de questions éventuelles et d'indisponibilité à la date proposée

Lors de l'entrée en fonction de nouveaux collaborateurs, la date d'émission peut aussi être fixée par le service RH compétent ou le futur supérieur hiérarchique. Dans tous les cas, les informations énumérées ci-dessus doivent être communiquées au requérant à l'avance.

5.2.3.4 Lancer le processus d'émission

Après l'arrivée du requérant, l'officier LRA lance l'assistant d'enregistrement (Walk-In Wizard) sur le client LRA et sélectionne la politique appropriée (pour les certificats de fonction de comptes A, il faut choisir celle qui sert uniquement à émettre un certificat d'authentification). Il cherche ensuite le requérant dans l'application d'émission à l'aide du nom ou de l'adresse électronique et sélectionne l'entrée adéquate. La source des données est ici Admin Directory.

5.2.3.5 Contrôler l'identité du requérant

Le requérant doit se présenter personnellement auprès de l'officier LRA en vue de son identification. L'officier LRA contrôle l'identité du requérant au moyen d'un passeport valable ou d'une carte d'identité valable pour entrer en Suisse. Le contrôle de l'identité du requérant comprend trois éléments :

1. Vérification de l'authenticité de la pièce d'identité présentée (carte d'identité, passeport). Par exemple, un badge du personnel ou un permis de conduire ne suffisent pas pour l'identification. Le contrôle doit porter sur les points suivants :
    a. La pièce d'identité est-elle encore valable (non échue à l'instant de l'enregistrement) ?
    b. Les marques de contrôle connues sont-elles présentes ? Il faut vérifier au moins quatre caractéristiques officielles de sécurité sur la pièce d'identité.
2. Identification personnelle du requérant par comparaison avec la pièce d'identité.
    a. La personne correspond-elle à la photographie de la pièce d'identité ?
    b. L'âge et la taille de la personne concordent-ils avec les indications figurant sur la pièce d'identité ?
    c. La signature sur la pièce d'identité correspond-elle à celle du formulaire de demande ?
3. Vérification que les données figurant sur la pièce d'identité correspondent à celles de la demande et à l'entrée dans Admin Directory. Il s'agit de vérifier en particulier la concordance entre le nom et le prénom inscrits sur la pièce d'identité et ceux figurant dans Admin Directory selon les règles suivantes :

Depuis le 1er janvier 2014, pour toute nouvelle entrée en fonction dans l'administration fédérale, le service RH compétent complète les champs « Nom (selon doc ID) » et « Prénom (selon doc ID) » en plus des champs nominatifs « Nom » et « Prénom ». Le contenu de ces champs s'affiche dans l'assistant d'enregistrement (Walk-In Wizard). En fonction dudit contenu, la vérification doit être exécutée selon les règles ci-après. La règle appliquée doit être cochée sur la page correspondante de l'assistant d'enregistrement. Les règles applicables sont les suivantes :

Règle 1 : les deux champs « Nom (selon doc ID) » et « Prénom (selon doc ID) » ont été complétés et sont identiques aux nom(s) et prénom(s) figurant sur la pièce d'identité présentée. À l'écran, il faut cliquer sur l'option « Identifié avec <Nom selon doc ID> / <Prénom selon doc ID> selon le document d'identité ».

Règle 2 : les champs « Nom (selon doc ID) » et « Prénom (selon doc ID) » ont été complétés, mais ne sont pas identiques à ceux figurant sur la pièce d'identité présentée. À l'écran, il faut cliquer sur l'option « Champ <Nom selon doc ID> / <Prénom selon doc ID> incorrect ». Aucun certificat n'est émis.

Règle 3 : les champs « Nom (selon doc ID) » et « Prénom (selon doc ID) » n'ont pas été complétés. Les champs « Nom » et « Prénom » correspondent cependant à ceux figurant sur la pièce d'identité présentée, compte tenu des conditions énoncées dans le document « Vérification de l'identité des requérants, certificats de la classe B » [KLB003]. À l'écran, il faut cliquer sur l'option « Identifié avec <Nom> / <Prénom>» .

Règle 4 : les champs « Nom (selon doc ID) » et « Prénom (selon doc ID) » n'ont pas été complétés. Les champs « Nom » et « Prénom » ne correspondent pas à ceux figurant sur la pièce d'identité présentée, même en tenant compte des conditions énoncées dans le document « Vérification de l'identité des requérants, certificats de la classe B » [KLB003], mais ils sont plausibles. Le requérant possédait déjà un certificat avec ces noms et prénoms (p. ex. en cas de remplacement d'une carte ou lors de l'émission d'une carte subséquente). Il faut alors demander aux ressources humaines compétentes de saisir les données dans les champs « Nom (selon doc ID) » et « Prénom (selon doc ID) ». Le requérant doit être inscrit sur la liste des certificats émis provisoirement. Le certificat peut alors être émis. À l'écran, il faut cliquer sur l'option « Émission provisoire avec ‹Nom› / ‹Prénom› ». L'officier LRA doit suivre la mutation des RH dans l'IGDP (anciennement BV+).

Règle 5 : les champs « Nom (selon doc ID) » et « Prénom (selon doc ID) » n'ont pas été complétés. Les champs « Nom » et « Prénom » ne correspondent pas à ceux figurant sur la pièce d'identité présentée. Il n'existe aucun ancien certificat du requérant.
Un nouveau certificat ne peut pas être établi. Il faut alors demander aux ressources humaines compétentes de saisir les données dans les champs « Nom (selon doc ID) » et « Prénom (selon doc ID) ». À l'écran, il faut cliquer sur l'option « <Nom> / <Prénom> invalide ».

Exception concernant les « livrets F »

Dans des cas exceptionnels, l'identification peut également être réalisée à l'aide d'un « livret F » en cours de validité. La vérification de ce dernier doit respecter les règles susmentionnées pour le contrôle d'une pièce d'identité. En cas de demandes reposant sur un « livret F », les formulaires et documents supplémentaires indiqués ci-après doivent être présentés, puis conservés dans le dossier du client :

- « Formulaire supplémentaire pour les requérants titulaires d'un livret F » entièrement complété et signé par le DSIO compétent. Celui-ci y admet que le requérant ne peut pas être identifié formellement sur la base des documents d'identité présentés, et accepte le risque correspondant pour l'organisation concernée ;
- autorisation d'exercer une activité lucrative, délivrée par l'autorité cantonale ou fédérale

compétente.

5.2.3.6 Vérification de la plausibilité de la demande

Les éléments à prendre en compte sont les suivants :

- Le requérant peut-il être identifié ?
- Travaille-t-il pour l'organisation indiquée ?
- Le service du personnel ou le supérieur hiérarchique est-il responsable du requérant ?

L'officier LRA peut refuser de délivrer un certificat s'il peut supposer que le demandeur ne sait pas comment utiliser ses certificats. Il en va de même si, en discutant avec le requérant, l'officier LRA constate que le requérant risque de ne pas respecter les directives figurant dans la convention d'utilisation.

5.2.3.7 Préparer la carte à puce

On utilise une carte à puce préparée. Elle est configurée centralement par la SG PKI en vue de son utilisation et ne doit donc pas être initialisée séparément.

5.2.3.8 Numériser les documents

Les documents utilisés pour l'identification, en particulier les pièces d'identité, doivent être numérisés pendant le processus d'émission et enregistrés dans le système. Un processus de numérisation est intégré à cet effet dans l'assistant d'enregistrement.

Pour une carte d'identité, il faut scanner le recto et le verso, et pour un passeport, la double page avec la photo et la signature. D'autres documents nécessaires à l'identification doivent aussi être scannés. Le document numérisé doit être bien lisible.

Pour obtenir de bons résultats lors du processus de numérisation, il faut utiliser les paramètres suivants :

- **Résolution :** 200 x 200 ou 300 x 300 dpi (selon les possibilités de réglage du scanner)
- **Format de fichier :** JPEG (extension de fichier : .jpg) ; PDF/A (extension de fichier : .pdf) pour la numérisation recto-verso des deux côtés de la pièce d'identité

Si aucun scanner n'est connecté au client LRA, la numérisation peut être effectuée sur un appareil multifonction et les pièces d'identité numérisées peuvent être envoyées à l'adresse électronique personnelle de l'officier LRA. L'envoi doit être crypté, si possible.

En général, la numérisation produit un résultat de taille A4. Il faut d'abord recadrer le document, de manière à n'enregistrer que la pièce d'identité proprement dite.
Le document doit être sauvegardé dans un répertoire privé du client. Après avoir émis le certificat, il convient de supprimer les documents concernés et les éventuels courriers électroniques, puis de vider la corbeille du client et celle d'Outlook.

5.2.3.9 Informer le requérant concernant le NIP et la phrase de révocation

L'officier LRA informe une nouvelle fois le requérant sur le sens et le but de la phrase de révocation. Si le requérant n'en a pas encore défini, l'officier LRA lui demande d'en préparer une conformément aux prescriptions définies au ch. 3.13 « Phrase de révocation » et lui rappelle les règles en matière de NIP figurant au ch. 3.12 « Règles pour les NIP ».

5.2.3.10 Demander des certificats et les enregistrer sur la carte à puce

La carte à puce du requérant est insérée dans le second lecteur de carte. Les certificats standard ne peuvent pas être émis sur la même carte à puce que des certificats de classe A ou des certificats de

fonction de classe B. Plusieurs certificats de fonction de classe B (p. ex. un certificat d'administrateur et plusieurs certificats de test) peuvent toutefois être enregistrés sur la même carte à puce.

À la prochaine étape, tous les documents nécessaires, qui ont été numérisés au préalable, sont enregistrés dans le système. Il s'agit au minimum de la copie d'une pièce d'identité valable. Tous les documents nécessaires à l'identification formelle et à l'enregistrement (p. ex. certificat de mariage, lettre de cautionnement, etc.) doivent être mis ensemble. Le processus correspondant est exposé au point 5.2.3.8 « Numériser les documents ».

L'assistant établit alors la demande et l'envoie au système central, où les certificats sont émis.

Le requérant est invité à saisir son NIP et sa phrase de révocation. Les certificats sont ensuite enregistrés sur sa carte à puce, laquelle est protégée par le NIP.

5.2.3.11 Demander un accusé de réception / signer la convention d'utilisation

Une fois le certificat émis, une confirmation contenant les « empreintes digitales » du certificat (numéro d'identification unique d'un certificat) s'affiche. L'impression et la remise de ce document sont facultatives. L'officier LRA doit rappeler oralement au requérant ses droits et ses obligations à l'aide des documents « Convention et conditions d'utilisation des certificats avancés de classe B » [KLB021] (but des certificats, contenu de la carte à puce, révocation des certificats, obligation de diligence concernant le NIP, phrase de révocation).

Enfin, le requérant doit signer une copie du document *« Convention et conditions d'utilisation des certificats avancés de classe B »* [KLB021] (qu'il s'agisse d'émettre un premier certificat ou les certificats suivants). Il confirme ainsi avoir lu et pris connaissance du contenu de cette notice et avoir bien reçu la carte à puce avec les certificats. L'officier LRA compare la signature apposée sur ce formulaire avec celle qui figure sur le formulaire de demande. La confirmation de réception contenant les « empreintes digitales » du certificat n'est plus nécessaire et peut être ignorée. Au lieu d'une copie papier, l'officier LRA peut remettre au requérant la convention d'utilisation sous forme électronique. Il doit cependant veiller à recevoir dans les cinq jours ouvrés la version du document signée avec un certificat de classe B et à l'archiver par voie électronique conformément aux dispositions du ch. 3.8 « Délais de conservation ». Si l'officier LRA ne reçoit pas dans ce délai la convention d'utilisation dûment signée, les certificats correspondants doivent être révoqués immédiatement.

5.2.3.12 Terminer l'émission du certificat

Enfin, le requérant se voit remettre :

- la nouvelle carte à puce,
- les copies non signées du document « Convention et conditions d'utilisation des certificats avancés de classe B » [KLB021],
- sa pièce d'identité et les autres documents requis.

5.2.3.13 Tenir un journal

Les activités effectuées doivent être consignées par l'officier LRA dans le journal LRA, conformément aux règles mentionnées au ch. 3.7.

5.2.3.14 Supprimer du système local les données enregistrées

Si la pièce d'identité a été numérisée en dehors de l'assistant d'enregistrement et enregistrée localement, le fichier doit être supprimé après l'émission des certificats. Il faut veiller en particulier à ce qu'aucune information ne soit mémorisée dans les comptes de messagerie personnel ou professionnel (cf. ch. 5.2.3.8).

Remarque : cette opération est nécessaire pour éviter de constituer un fichier de données non annoncé au sens de la loi sur la protection des données. Pendant le processus d'émission, les fichiers sont enregistrés dans la base de données de la SG PKI (qui est déclarée conformément à la LPD [GV015]).

5.2.3.15 Archivage du dossier client

La demande traitée et la copie signée du document *« Convention et conditions d'utilisation des certificats avancés de classe B »* [KLB021] sont classées dans le dossier du client. Si des formulaires supplémentaires (p. ex. en cas d'établissement avec un permis F) ou d'autres documents sont nécessaires, ils sont aussi classés dans le dossier du client.

Si le dossier est géré par voie électronique, les documents susmentionnés doivent être numérisés, enregistrés au format PDF/A, signés avec le certificat de classe B personnel de l'officier LRA, puis archivés pour que :

- la chronologie et le titulaire du certificat soient identifiables ;
- la demande puisse être trouvée à tout moment ;
- les informations éventuelles provenant des systèmes périphériques (p. ex. numéro de ticket, etc.) soient disponibles (les tickets correspondants et autres doivent être disponibles pendant au moins 11 ans après l'échéance du certificat).

5.2.4 Émission avec RIO

Dans le processus « Émission avec RIO », l'officier LRA délègue au RIO l'identification du requérant et d'autres tâches, lorsque le requérant et le RIO sont sur un site distant de celui de l'officier LRA. Cette méthode se nomme aussi processus d'émission asynchrone. Les certificats de fonction pour comptes A et T ne peuvent pas être émis en utilisant ce processus.

Les « *Directives pour le Registration Identification Officer (RIO)* » [GV003] et le « *Guide rapide Walk-In-Wizard - RIO* » (sous «RIO (Registration Identification Officers)») doivent aussi être pris en compte dans ce processus. La présente directive prime en cas de contradiction.

L'officier LRA gère l'ensemble de l'archivage des documents ; le RIO n'effectue pas d'archivage durable.

Par souci d'exhaustivité, nous décrivons ici l'ensemble du processus, y compris les opérations que le requérant exécute lui-même pour activer la carte à puce.

5.2.4.1 Établissement de la demande

Dans le formulaire « Demande du RIO en vue de l'émission de certificats de classe B », le requérant complète le paragraphe 1 en indiquant ses données personnelles ainsi que celles de son organisation et ses coordonnées, puis date et signe le paragraphe.

5.2.4.2 Identification du requérant par le RIO

L'identité du requérant doit être clairement vérifiée par un RIO. Pour ce faire, le requérant doit le contacter personnellement. Les étapes suivantes permettent d'exécuter les vérifications requises et de compléter le formulaire de demande avec les informations nécessaires :

1. Le requérant s'annonce personnellement auprès du RIO avec son moyen d'identification (passeport en cours de validité ou carte d'identité valable pour l'entrée en Suisse).
2. Le RIO procède selon la « Liste de contrôle RIO », qu'il remplit.
3. Le RIO contrôle si le visage du requérant correspond à la photo de la pièce d'identité. Si tel n'est pas le cas, il refuse de poursuivre le processus d'identification et signale l'infraction à

l'officier LRA compétent. Les autres moyens d'identification énoncés dans les dispositions d'exception et les processus à appliquer dans de tels cas figurent au ch. 5.2.3.5 « Contrôler l'identité du requérant ». La liste qui y est indiquée est exhaustive.

4. En cas de conformité, le RIO remet au requérant une nouvelle carte à puce préparée et note le numéro de série de la puce cryptée dans le champ du formulaire prévu à cet effet. Si le numéro de série ne figure pas sur la carte à puce, il peut être obtenu à l'aide de l'intergiciel de la carte ou de l'assistant de déblocage (Unseal Wizard). Le RIO précise au requérant que ce dernier doit désormais conserver la nouvelle carte à puce sous son contrôle exclusif.
5. En signant le paragraphe 2 du formulaire de demande, le RIO et le requérant confirment qu'une rencontre personnelle a eu lieu, que l'identification a été effectuée grâce à une pièce d'identité en cours de validité et que le requérant a reçu la carte à puce mentionnée.
6. Le RIO s'assure que le requérant a compris le contenu du document « *Convention et conditions d'utilisation des certificats avancés de classe B* » [KLB021] et en a reçu une copie. Le requérant doit signer la seconde copie.
7. Le RIO pose la deuxième page du formulaire de demande et la pièce d'identité sur le photocopieur de façon à ce que cette dernière et la photo du visage du requérant soient copiées dans le champ prévu à cet effet du formulaire de demande.
   Les cartes d'identité doivent être photocopiées des deux côtés ; pour les passeports, il faut effectuer une copie de la double page où figurent la photo et la signature.
8. Le RIO fait une copie de la deuxième page du formulaire de demande, de la pièce d'identité ainsi que de tous les formulaires et documents supplémentaires qui sont nécessaires à l'émission. Le requérant et le RIO signent la deuxième page. Avec la première page précédemment remplie, le formulaire de demande est maintenant complet.
9. Le RIO envoie à l'officier LRA compétent les deux documents signés (formulaire de demande et « Convention d'utilisation » [KLB021]), les copies des éventuels documents supplémentaires et la liste de contrôle dûment remplie. L'envoi peut être effectué de l'une des deux manières indiquées ci-après :
   a. Les documents signés sont envoyés par poste ou par coursier à l'officier LRA compétent.
   b. Le RIO numérise les documents au format PDF/A, les signe au moyen de son certificat personnel de classe B et les envoie par courrier électronique crypté à l'officier LRA compétent. Les conditions d'utilisation de cette procédure sont les suivantes :
      i. Le RIO est en possession d'un certificat de classe B valable.
      ii. Le RIO a accès à la clé publique de chiffrement de l'officier LRA.
      iii. Le poste de travail du RIO est équipé d'une possibilité de numérisation.
10. Si documents ont été transmis par voie électronique mais que l'officier LRA ne gère pas de dossiers de client électroniques conformément aux spécifications du ch. 5.2.4.3 « Approbation de la demande par l'officier LRA », les documents au format papier doivent être envoyés par la suite à l'officier LRA par courrier postal pour être classés dans le dossier physique du client. L'officier LRA vérifie et garantit la réception.
11. Les documents originaux qui ont été utilisés pour l'identification sont rendus au requérant. L'ensemble des copies et formulaires doivent être soit envoyés à l'officier LRA, soit détruits (déchiqueteuse). Il convient également de supprimer les copies numériques, qui se trouvent notamment dans la boîte aux lettres électronique, et de vider la corbeille. Le RIO ne conserve pas de documents et ne gère pas de dossiers des clients.

5.2.4.3 Approbation de la demande par l'officier LRA et émission des certificats

Après réception et contrôle des documents dûment remplis mentionnés au ch. 5.2.4.2 « Identification du requérant par le RIO », l'officier LRA peut approuver la demande et valider l'émission des certificats. Pour ce faire, il exécute les étapes suivantes de la liste de contrôle « Émission avec RIO » :

1. L'officier LRA vérifie si tous les documents sont joints et si le formulaire de demande est signé par un RIO autorisé. Les documents requis sont les suivants :
   - formulaire de demande « Demande RIO en vue de l'émission de certificats de classe B » signé par les personnes concernées ;
   - « Convention et conditions d'utilisation des certificats avancés de classe B » [KLB021] signée ;
   - « Liste de contrôle RIO » signée ;
   - autres documents et pièces d'identité requis en cas de situation d'exception.
2. Si les documents ont été transmis par courrier électronique, l'officier LRA vérifie :
   - qu'ils ont été envoyés chiffrés,
   - qu'ils sont dotés de la signature électronique valable du RIO.
3. Sur le client LRA, l'officier LRA lance l'assistant d'enregistrement (Walk-In Wizard) en mode RIO à l'aide de sa carte à puce. Il recherche le requérant dans le système en saisissant son nom ou son adresse électronique.
4. L'officier LRA vérifie si les données inscrites dans les formulaires de demande correspondent à celles figurant sur la copie de la pièce d'identité et à l'inscription du demandeur dans Admin Directory (cf. ch. 5.2.3.5). Si les trois sources correspondent conformément aux directives, l'approbation de la demande peut se poursuivre. Si ce n'est pas le cas, le processus doit être interrompu et une correction d'Admin Directory ou du formulaire de demande doit être demandée.
5. Les documents reçus par voie électronique peuvent être directement reliés ensemble dans l'assistant d'enregistrement.

   Si les formulaires ont été transmis sur papier, l'officier LRA numérise les copies signées du formulaire de demande et de la « Liste de contrôle RIO », ainsi que les autres documents et pièces d'identité requis en cas de situation d'exception, qu'il a reçus du RIO.

   Pour obtenir des résultats de bonne qualité, il convient d'utiliser les réglages suivants :
   - **Résolution :** 200 x 200 ou 300 x 300 dpi (selon les possibilités de réglage du scanner)
   - **Format de fichier :** JPEG (extension de fichier : .jpg) ou PDF/A (extension de fichier : .pdf)

   L'officier LRA charge ensuite les documents dans l'assistant d'enregistrement.
6. L'officier LRA saisit le numéro de série de la carte à puce remise au requérant et émet le certificat sur le serveur (en utilisant l'assistant d'enregistrement).
7. La demande validée est jointe à un ticket en arrière-plan, puis transférée à la CA pour certification. Le numéro du ticket est consigné dans un document de déblocage (Unseal Document) au format PDF, qui peut être imprimé.
8. L'officier LRA transmet le document de déblocage ou le code de déblocage (numéro de l'e-ticket) soit directement au requérant, soit au RIO.
9. L'officier LRA consigne la procédure dans le journal.
10. L'officier LRA place le document signé « Convention et conditions d'utilisation des certificats avancés de classe B » [KLB021v] dans le dossier du client. Si le dossier est géré

électroniquement, il faut classer soit la version électronique signée par le RIO, soit une version PDF/A que l'officier LRA crée à partir des documents papier. L'officier LRA signe ensuite le document avec son certificat personnel de classe B, puis le classe. Les dossiers électroniques des clients doivent respecter les exigences visées aux ch. 5.2.3.14 « Supprimer du système local les données enregistrées » et 3.8 « Délais de conservation » des présentes directives en matière de sécurité de conservation, de protection des données, de délais de conservation et de capacité de révision.

11. Les deux parties suppriment de leurs dossiers personnels toutes les copies numérisées de la carte d'identité ou du passeport (y compris de leur boîte aux lettres électronique [éléments envoyés], etc.).

5.2.4.4 Activation de la carte à puce par transfert des certificats sur la carte à puce

La dernière étape consiste à transférer les certificats sur la carte à puce du requérant.

1. Après l'émission du certificat, le requérant reçoit le document de déblocage avec le numéro de l'e-ticket par courrier électronique ou par l'intermédiaire du RIO.
2. Il lance l'assistant de déblocage (Unseal Wizard) sur un client relié au réseau et insère sa carte à puce dans le lecteur de carte. Si le client exige la connexion à deux facteurs pour Windows, un deuxième lecteur de carte doit être installé pour se connecter. Le requérant saisit le numéro de ticket reçu. L'assistant vérifie alors si la carte à puce indiquée dans le ticket correspond à celle qui est insérée dans le second lecteur de carte.
3. Si cela concorde, le requérant est invité à saisir son NIP et sa phrase de révocation.
4. L'assistant d'enregistrement sauvegarde la phrase de révocation dans la base de données centralisée, charge les certificats sur la carte à puce et protège cette dernière avec le nouveau NIP.

La carte à puce est alors activée et peut être utilisée par le requérant.

5.3 Processus de révocation d'un certificat

5.3.1 Qui peut demander une révocation ?

La liste exhaustive ci-après indique tous les rôles qui peuvent demander la révocation d'un certificat :

- la personne titulaire du certificat elle-même,
- les supérieurs hiérarchiques du titulaire du certificat,
- le responsable PKI,
- le responsable de la sécurité de la SG PKI,
- l'officier LRA compétent de la SG PKI,
- le DSIO ou le DSID, ou le responsable de la sécurité de l'information de l'organisation,
- les collaborateurs du service du personnel responsables du titulaire du certificat.

5.3.2 Comment demander une révocation ?

Le titulaire du certificat peut en demander la révocation à l'officier LRA soit personnellement, soit par courrier électronique, soit par téléphone. L'officier LRA identifie le requérant, p. ex. grâce à la phrase de révocation, et valide la plausibilité de la demande.

Les services du personnel ou les supérieurs hiérarchiques peuvent aussi envoyer des listes de demandes de révocation (p. ex. sous forme de fichiers Excel) à l'officier LRA. C'est surtout le cas lors de départs ou de changements de collaborateurs, la révocation étant intégrée dans les processus de départ prévus. L'officier LRA vérifie la compétence de l'expéditeur. L'officier LRA ne peut accepter les

demandes de révocation de tiers que par écrit (courrier électronique signé, demandes de révocation signées). Seul le titulaire du certificat peut le révoquer par téléphone.

Les officiers LRA doivent être intégrés aux processus de départ de leur unité. Il faut s'assurer que les certificats des collaborateurs qui quittent l'entreprise sont révoqués à temps. La révocation doit être effectuée immédiatement lors de la restitution de la carte à puce, ou au plus tard le premier jour ouvrable qui suit le départ.

L'officier LRA, l'officier de sécurité PKI et le responsable de la SG PKI peuvent révoquer un certificat directement dans l'assistant de révocation (Revoke-Wizard).

Quels sont les raisons d'une révocation ?

5.3.3 Les raisons d'une révocation sont notamment les suivantes :

- la carte à puce a été volée ou est introuvable ;
- la carte à puce est défectueuse ;
- la carte à puce est renouvelée ;
- la carte à puce doit être restituée (p. ex. au supérieur hiérarchique, à l'officier LRA, au service du personnel) ;
- les rapports de travail avec le titulaire du certificat prennent fin ;
- des données contenues dans le certificat ont changé (nom, adresse électronique, etc.) ;
- on soupçonne la divulgation de la clé privée (une autre personne a pu utiliser un service, p. ex. signer un courrier électronique) ;
- le titulaire n'a pas respecté des directives (p. ex. non-respect de la convention d'utilisation [KLB021]) ;
- l'officier LRA demande une révocation pour d'autres raisons.

5.3.4 Procédure

Une demande de révocation doit **toujours être traitée immédiatement**. En cas de doute sur la validité d'une telle demande (p. ex. si elle a été faite par téléphone), il faut noter qu'une révocation a pour objectif de protéger le titulaire et l'organisation contre un dommage possible suite à une utilisation abusive de leurs certificats. L'exécution d'une demande de révocation frauduleuse peut toutefois aussi causer des dommages, car les prestations ne peuvent plus être utilisées par le client concerné ou la révocation empêche un acte officiel. L'officier LRA doit donc évaluer le dommage potentiel d'une non-révocation et celui d'une révocation frauduleuse.

L'officier LRA doit procéder comme décrit ci-après.

5.3.4.1 Contrôle de la plausibilité de la demande

Éléments à prendre en compte :

- Le requérant peut-il être identifié (voix, numéro de téléphone, phrase de révocation) ?
- Le service du personnel ou le supérieur hiérarchique est-il responsable du titulaire de certificats concerné ?
- Est-ce le DSIO ou le DSID ?

5.3.4.2 Formulaire de révocation

Si une demande de révocation émane de tiers (c'est-à-dire ni de l'officier LRA, ni du titulaire du certificat ; cf. ch. 5.3.1), elle doit être formulée par écrit à l'aide du document « *Demande de révocation*

des certificats de classe B de la Swiss Government PKI ». Les services du personnel ou les supérieurs hiérarchiques peuvent aussi envoyer des listes de demandes de révocation (p. ex. sous forme de fichiers Excel) à l'officier LRA. Si la demande n'est pas présentée sur papier, il faut veiller à ce que le document ou le courrier électronique avec la pièce jointe soit signé par le requérant.

De même, un formulaire de révocation est nécessaire lorsque les informations concernant la révocation (motif, donneur d'ordre) ne figurent pas dans l'assistant de révocation ou lorsque celui-ci ne peut pas être utilisé pour la révocation. Dans de tels cas, le formulaire peut également être rempli par l'officier LRA, en particulier pour les révocations réalisées avec la console CMC et les ordres de révocation adressés à la SG PKI.

5.3.4.3 Révocation

Pour révoquer un certificat, l'officier LRA lance l'assistant de révocation sur le client LRA et y cherche le titulaire du certificat. Il sélectionne ensuite les certificats à révoquer. S'ouvre alors une page où figurent tous les documents d'identité enregistrés pour les certificats concernés. L'officier LRA vérifie l'identité du titulaire à l'aide de ces documents.

Une fois l'identification effectuée, l'officier LRA peut révoquer les certificats sélectionnés. Le titulaire reçoit automatiquement une confirmation de la révocation par courrier électronique.

Si possible, la carte à puce est retirée, détruite et éliminée conformément au ch. 3.11 « Élimination ».

5.3.4.4 Clôture administrative

Le formulaire de révocation est archivé dans le dossier du client. Si le formulaire est traité par voie électronique, les exigences fixées aux ch. 3.8 « Délais de conservation » et 5.2.3.15 « Archivage du dossier client » s'appliquent. La procédure de révocation est consignée dans le journal selon le ch. 3.7 « Journal ».

5.4 Processus de renouvellement d'un certificat

Les certificats peuvent être renouvelés par les titulaires eux-mêmes jusqu'à deux fois pendant leur période de validité. On parle alors de renouvellement (Renewal). Pour cela, la version actuelle de l'assistant de renouvellement (Renewal Wizard) doit être installée sur l'ordinateur de l'utilisateur et la mémoire disponible sur la carte à puce doit être suffisante. Étant donné que les cartes à puce préparées disposent déjà de trois jeux de clés, cette condition est généralement remplie pour ce type de carte. La procédure est la suivante :

- lancement de l'assistant de renouvellement sur la station de travail du requérant avec le certificat de classe B encore valable ;
- affichage de la carte à puce insérée dans le lecteur de carte ;
- confirmation qu'il s'agit de la bonne carte ;
- ensuite, émission de trois nouveaux certificats par l'assistant et enregistrement sur la carte à puce. Les anciens certificats de signature et d'authentification sont supprimés. Les anciens certificats de chiffrement sont conservés sur la carte à puce.

Une fois expirés, les certificats ne peuvent plus être renouvelés selon la procédure décrite ci-dessus. L'officier LRA doit alors émettre un nouveau certificat. La procédure est la même que celle régissant la première émission d'un certificat.

5.5 Processus de récupération de ses propres clés

Le titulaire d'un certificat peut demander lui-même la récupération de ses propres clés de chiffrement. La procédure est la suivante :

L'URL https://keyrecovery.pki.admin.ch/KeyRecoveryRequest/ permet de se connecter à l'application avec son certificat de classe B actuellement valable et de générer un e-ticket pour récupérer les clés. Il faut ensuite se rendre auprès de l'officier LRA ou du Key Recovery Agent (KRA) compétent avec le numéro du ticket et sa carte à puce.

Cette personne identifie le titulaire de la carte à puce et lance l'assistant de récupération des clés. Elle insère la carte à puce du titulaire dans un lecteur de carte libre et saisit le numéro de l'e-ticket. Les anciennes clés de chiffrement du titulaire s'affichent alors à l'écran. Après sélection de la clé souhaitée, celle-ci est ajoutée aux clés de chiffrement se trouvant déjà sur la carte à puce.

5.6 Processus de récupération de clés de tiers

En principe, les clés de chiffrement ne doivent figurer que sur la carte à puce du titulaire du certificat.

Dans des cas exceptionnels, il peut toutefois être nécessaire d'installer la ou les clés de chiffrement d'une personne sur une carte à puce séparée d'une personne habilitée, pour les raisons suivantes :

- le titulaire du certificat ne travaille plus pour l'office ;
- le titulaire du certificat est absent en raison d'une maladie de longue durée ;
- le titulaire du certificat est décédé ;
- cas d'ordre juridique.

Comme cette récupération permet de lire tous les courriers électroniques et documents chiffrés du titulaire du certificat (à condition que ces données chiffrées soient aussi en possession du détenteur des clés), la SG PKI et le service juridique de l'OFIT doivent évaluer chacun de ces cas séparément. À cet effet, une demande détaillée et motivée doit être soumise à la personne compétente en la matière à la SG PKI. La suite des opérations est alors définie individuellement et toujours en consultant le service juridique.

6 Formulaires et listes de contrôle

Les formulaires et les listes de contrôle ci-après ont été élaborés pour les processus susmentionnés. Tous ces documents peuvent être obtenus séparément sur le site Internet de la SG PKI.

6.1 Formulaire de demande de certificat

Avant l'émission d'un certificat dans le cadre du processus « *Émission sans RIO* » (cf. ch.5.2.3), le client doit remplir le formulaire « *Demande de certificats personnels de classe B à la Swiss Government PKI* ». Ce formulaire peut être téléchargé sur le site Internet de la SG PKI. Les clients sont libres de concevoir un formulaire propre à leur organisation pour demander des certificats. Mais au moins les données suivantes doivent y figurer :

- nom et prénom ;
- unité d'organisation ;
- adresse électronique ;
- numéro personnel unique ou suffixe.

En outre, le formulaire devrait déjà contenir des indications sur les règles à suivre pour définir le NIP et la phrase personnelle de révocation.

Il doit être remis au client à l'avance afin que celui-ci ait suffisamment de temps pour définir un NIP et une phrase de révocation. Le client signe le formulaire de demande et confirme ainsi l'exactitude des informations.

Les offices peuvent aussi commander des certificats de classe B grâce à leur système interne de saisie des mandats (p. ex. MAC dans Remedy, Gever, etc.). Il faut toutefois s'assurer que les demandes soient formellement attribuables aux certificats émis et que les documents de demande ainsi que les preuves utilisées soient disponibles jusqu'à 11 ans après l'échéance du certificat (cf. ch. 5.2.3.15 et 3.8).

Dans l'administration fédérale, la première émission d'un certificat standard fait généralement partie du processus RH « Entrée en fonction de nouveaux collaborateurs ». Les services du personnel compétents peuvent aussi annoncer les nouveaux collaborateurs à l'officier LRA en lui envoyant une liste. Ils doivent alors indiquer les données énumérées ci-dessus pour chaque nouveau collaborateur. Le formulaire « *Demande RIO en vue de l'émission de certificats de classe B* » est utilisé pour le processus « *Émission avec RIO* » (cf. ch. 5.2.4).

6.1.1 Formulaire supplémentaire pour les requérants titulaires d'un livret F

Si, en vertu des dispositions d'exception, une demande est émise pour un requérant ayant un « livret F », le « *Formulaire supplémentaire pour les requérants titulaires d'un livret F* » doit être complété en plus du formulaire de demande et signé par le DSIO compétent. Par sa signature, ce dernier confirme avoir pris acte que le requérant ne peut pas être identifié formellement avec un « livret F » et que la SG PKI ne saurait dès lors garantir l'identification correcte dudit requérant. Ce formulaire supplémentaire fait partie intégrante des documents d'émission requis lors d'un audit.

6.2 Convention et conditions d'utilisation des certificats avancés de classe B

Créé spécialement pour l'utilisateur final, le formulaire « Convention et conditions d'utilisation des certificats avancés de classe B » ne comprend que les informations les plus importantes. Des renseignements complets figurent dans les CP/CPS [KLB001]. Ce formulaire fait partie intégrante des documents d'émission requis lors d'un audit. L'actuel formulaire « Confirmation de réception de la carte à puce et directives d'utilisation » contient les empreintes digitales des certificats. À la fin du document, le numéro de la carte à puce peut être saisi, s'il est disponible. Ce numéro peut être utile en cas de problème avec la carte à puce (perte ou endommagement). Ce formulaire de confirmation ne fait pas partie intégrante des documents d'émission requis lors d'un audit.

6.3 Formulaire de révocation

Lorsqu'une révocation est exécutée avec l'assistant correspondant, le donneur d'ordre et les motifs doivent y être indiqués. Dans ces cas, il n'est pas nécessaire de remplir et d'archiver le formulaire de révocation. Dans tous les autres cas, ce formulaire fait partie intégrante des documents de révocation requis lors d'un audit (cf. ch. 5.3.4.2).

6.4 Formulaire de récupération de clés de tiers

Aucun formulaire n'est créé spécialement pour ce processus. La demande doit être envoyée, avec une justification détaillée, au responsable compétent à la PKI ou au responsable PKI de l'OFIT. Les documents nécessaires à cet effet font partie intégrante de la documentation relative à la récupération des clés qui est requise lors d'un audit.

6.5 Liste de contrôle pour l'émission d'un certificat sans RIO

La « Liste de contrôle : émission de certificats de classe B » sert d'aide à l'officier LRA lors de l'émission. Il n'est nécessaire ni de la remplir, ni de l'archiver pour chaque certificat émis.

6.6 Liste de contrôle pour l'émission d'un certificat avec RIO

La liste de contrôle « Émission avec RIO » sert d'aide à l'officier LRA lors de l'émission. Il n'est nécessaire ni de la remplir, ni de l'archiver pour chaque certificat émis.

6.7 Liste de contrôle RIO

La « Liste de contrôle RIO » est indispensable à la demande dans le processus avec RIO. Elle doit être remplie par le RIO pour chaque demande, envoyée à l'officier LRA chargé de l'approbation, puis classée par celui-ci dans le dossier du client. Cette liste de contrôle fait partie intégrante des documents d'émission requis lors d'un audit.

6.8 Liste de contrôle pour la révocation d'un certificat

La liste de contrôle « Révocation de certificats de classe B » sert d'aide à l'officier LRA lors de l'émission. Il n'est nécessaire ni de la remplir, ni de l'archiver pour chaque certificat révoqué.

7 Violation des présentes directives

En cas de violation des directives d’enregistrement, la SG PKI peut retirer les autorisations d’un officier LRA et l’empêcher ainsi d’établir de nouveaux certificats pour des utilisateurs finaux.

8 Procédure d’intervention par paliers

En cas d’incertitudes ou de questions, ou si vous rencontrez des problèmes que vous ne pouvez pas résoudre vous-même avec des clients, l’exploitation de la SG PKI ou d’autres unités d’organisation, veuillez vous adresser au responsable compétent à la PKI ou au responsable PKI de l’OFIT.

9 Propositions de modification

Veuillez envoyer vos remarques ou propositions de modification relatives à ce document ou aux formulaires à :

Product Owner Trust Frontend
Office fédéral de l'informatique et de la télécommunication OFIT
Swiss Government PKI – Trust Frontend (PS- PSC- TRU)
Eichenweg 3
CH-3052 Zollikofen
Adresse électronique : pki-info@bit.admin.ch

Annexe A : Historique des modifications du document

Version DE	Thème	Chapitre
V5.2	Définitions, acronymes et abréviations – plusieurs ajouts et corrections	Définitions, acronymes et abréviations
V5.2	Ajout des réf. [29] à [32]	Références
V5.2	Précision : les certificats de classe B sont émis uniquement pour des personnes physiques.	1.3
V5.2	Contrôle de sécurité relatif aux personnes : ce contrôle ou un contrôle équivalent de la fiabilité est exigé de l'office requérant.	2.1 / 3.13
V5.2	La LRA est désormais assistée par le Service Desk de l'OFIT ou grâce à un ticket Remedy / une demande MAC.	3.2 / 3.11 / 3.12
V5.2	Contrôle des accès : redéfinition des exigences relatives au lieu de la LRA	3.3
V5.2	Contrôle des accès : exigences relatives à la protection de l'ordinateur de l'officier LRA adaptées à celles d'un client BAB de la Confédération	3.4 / 3.5
V5.2	Formulaires et données clients : précisions sur la conservation	3.6
V5.2	Journal : nouvelles directives pour tenir un journal (électronique) et réglementation des accès	3.7
V5.2	Précisions sur la protection (électronique) des accès et les délais de conservation des documents électroniques	3.8 / 3.9
V5.2	Remplacement du certificat spécifique d'officier LRA par l'octroi d'autorisations dans les certificats personnels de classe B	3.10
V5.2	Protection des clés privées de la station LRA	Ancien ch. 3.10 – a été supprimé
V5.2	Remplacement de la station LRA par des clients BAB de la Confédération comportant des fonctions d'officier LRA	3.11 / 3.12
V5.2	Précisions sur les lois en vigueur en matière de protection des données personnelles	3.14
V5.2	Précisions sur la formation et le perfectionnement des officiers LRA, correction et autres remarques sur le nombre de points requis	3.15 / 3.16
V5.2	Réinitialisation du NIP et gestion de la PUK	Nouveau ch. 3.19
V5.2	Contrôle de la conformité : révision du texte	4
V5.2	Processus sans RIO : ajouts concernant le processus d'émission avec un « livret F »	5.2 / 5.2.3.2 / 5.2.3.7 / 5.2.4.2
V5.2	Passation d'un mandat d'émission grâce aux systèmes de saisie des mandats (MAC, Gever) et validation de l'identification à l'aide d'un « livret F », y c. le formulaire supplémentaire	5.2.2 / 5.2.3.2
V5.2	Mise en place des champs 4 et 5 (« adminGivenNameLong » et « adminSurNameLong ») dans Admin Directory et les outils LRAO, ainsi que des variantes de décision possibles pour l'émission d'un certificat	5.2.3.1
V5.2	Liaison des pièces d'identité lors de la numérisation	5.2.3.7
V5.2	Gestion des données électroniques et archivage (fichiers numérisés)	3.7/ 3.8 / 5.2.3.6 / 5.2.3.8 / 5.2.3.12 / 5.2.3.13
V5.2	Révocation : précisions sur les demandes par téléphone	5.3.2
V5.2	Formulaire de révocation : nouvelles directives en cas de révocation avec l'assistant éponyme	5.3.4.2 / 5.3.4.4 / 6.3
V5.2	Formulaires requis pour l'audit : la pertinence a été complétée dans le chapitre concerné.	6.1 ss.

Version DE	Thème	Chapitre
V5.2	Formulaire de demande : adaptation des exigences relatives aux données requises	6.1
V5.2	Nouvelles directives sur l'utilisation du formulaire *« Confirmation de réception de la carte à puce et directives d'utilisation »*	6.2
V5.2	Formulaire supplémentaire pour les requérants titulaires d'un livret F	Nouveau ch. 6.1.1
V5.2	Listes de contrôle – plusieurs corrections	Annexe A
V5.2	Formulaires – plusieurs mises à jour et corrections, nouveau formulaire pour le livret F	Annexe B
V5.2	Formulaires – ajout des formulaires LRAO, de la convention d'utilisation et des directives aux fins d'exhaustivité	Annexe B
V5.2	Historique des modifications du document, état et entrée en vigueur de celui-ci	Nouvelle annexe C
V5.2	Adaptation des listes de contrôle et formulaires	Annexe B
V5.2	Ajout du formulaire sur la réinitialisation du NIP par un superutilisateur et de la demande pour KRA dans les DE	Annexe B
V5.9	Changement de version avant validation	V5.2 DE
V5.9	Suppression du ch. 3.12 « Réparation »	Ancien ch. 3.12
V6.0	Version après validation	N° de version
V6.1	Station LRA remplacée par client LRA ou client BAB, uniquement des cartes à puce préparées	Différents chapitres
V6.1	Reformulation en langage inclusif (concerne la version allemande)	Tout le document
V6.1	Suppression des références inutiles, ajout de la LPD, de la LSI et de l'OIS	Références, ch. 3.13, différents chapitres
V6.1	Modification ou ajout de diverses définitions, acronymes et abréviations	Définitions, acronymes et abréviations
V6.1	Suppression de l'annexe A : Listes de contrôle des processus et de l'annexe B : Formulaires pour les certificats de classe B. Les documents actuels sont disponibles sur le site web de la SG PKI, références supprimées	Annexe A, annexe B
V6.1	Suppression des directives dans le document (remplacées par la convention d'utilisation élargie)	Différents chapitres
V6.1	Modification de l'assistance et la joignabilité de la SG PKI	Ch. 3.2
V6.1	Etoffement des exemples des entrées du journal nécessaires	Ch. 3.7
V6.1	Ajout d'explications sur l'archivage électronique ultérieur des documents papier	Ch. 3.8
V6.1	Responsabilité de l'officier LRA complétée	Ch. 3.13
V6.1	Modification de la liste des points liés à la formation	Ch. 3.15
V6.1	Processus d'émission légèrement modifié/complété en partie	Ch. 5.2
V6.1	Ajout de l'intégration nécessaire de l'officier LRA dans les processus de départ	Ch. 5.3.2.3
V6.4	Ajout de la directive d'utilisation du système de poste de travail (client BAB) comme nouvelle directive à respecter	Ch. 3.5
V6.4	Diverses adaptations du processus RIO, p. ex. le fait que la deuxième page du formulaire de demande ne doit pas être classée dans le dossier du client	Ch. 5.2.4 ss.
V7.0	Nouvelle version du document après diverses adaptations et compléments (selon l'historique des modifications), et langage inclusif (version allemande)	

État de la version 7.0 : 14.01.2025

Entrée en vigueur : 01.08.2025