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

Directives d'enregistrement de la classe B de la Swiss Government PKI

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

V6.0, 01.11.2019

Classification *	Non classifié
Statut **	Validé
Nom du projet	
Nom abrégé du projet	
Numéro du projet	
Chef de projet	
Mandant	Swiss Government PKI
Auteur	Daniel Stich
Initiales	
Gestionnaires	Daniel Stich, Jürgen Weber, Beatrice Metaj
Vérificateurs	Michael von Niederhäusern
Approbateurs	PKI Management Board
Destinataires	Officiers LRA, auditeurs
ID du document	0002-RV-Directives d'enregistrement de la Swiss Government PKI pour la LRA
Description succincte	
Classement	Certified PKI

* Non classifié, interne ou confidentiel

** En traitement, en vérification, terminé

Contrôle des modifications, examen, approbation

Version	Date	Description, remarque	Nom ou rôle
2.91	23.07.2010	Remplace les versions 2.x, qui sont traitées dans un document séparé pour les classes A et B	Andreas Zürcher
2.92		Réduction du texte et vérification de la cohérence avec le document CP/CPS, listes de contrôle avec liens vers les directives	Daniel Stich
2.93		Prise en compte des résultats de la révision avec A. Zürcher	Daniel Stich
2.94		Prise en compte des commentaires du LZPPS	Daniel Stich
3.00	23.02.2012	Finalisation	Daniel Stich
3.01	23.04.2012	Adaptation des règles relatives au NIP	Daniel Stich
3.02	30.01.2013	PDF dans les processus RIO et établissement des certificats, transmission électronique signée de documents pour le processus RIO, adaptations à la connexion à 2 facteurs sur les systèmes clients de l'administration fédérale	Daniel Stich
3.03	22.04.2013	Prise en compte des certificats de fonction Adaptation AdminPKI-> Swiss Government PKI Adaptation de l'unité d'organisation après ON OFIT	Tomaso Vasella
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	Feed-back / examen annuel
6.0	01.11.2019	PKI Management Board	Validation de la nouvelle version

Définitions, acronymes et abréviations

Terme / Abréviation	Signification
Admin Directory	Annuaire de l'administration fédérale où sont enregistrés, entre autres, des certificats de cryptage et les listes de certificats révoqués, auxquels peuvent accéder les utilisateurs finaux. Il s'agit d'un annuaire conformément à la recommandation X.500 [18].
AdminPKI	Ancienne désignation de la Swiss Government PKI. Est encore souvent utilisée comme synonyme de celle-ci.
Agent habilité à la récupération des clés (Key Recovery Agent, KRA)	Utilisateur doté d'une autorisation spéciale pour exécuter l'assistant de récupération des clés. L'autorisation KRA fait partie intégrante de la fonction d'officier LRA. En cas de demande spécifique, elle peut également être accordée à d'autres collaborateurs.
Application d'enregistrement	(Voir client LRA)
Autorité d'enregistrement locale (Local Registration Agency, LRA)	Unité d'organisation chargée par la SG PKI d'exécuter en son nom l'identification des requérants ainsi que la commande et la gestion des certificats. Les tâches de la LRA sont assumées par l'officier LRA. Cela englobe non seulement le matériel (ordinateur portable) et le logiciel (client LRA) utilisés pour le traitement des certificats, mais aussi les locaux dans lesquels les clients sont identifiés, les certificats établis, les dossiers clients archivés et les ordinateurs de la LRA (client LRA) exploités.
Autorité de certification (CA)	Service digne de confiance qui émet et gère des certificats ainsi que des listes de certificats révoqués selon les recommandations X.509 [19]. Les CA de la classe B sont communément appelées *Swiss Government Enhanced CA 01* et *Swiss Government Enhanced CA 02.*
Autorité de certification racine (Root CA)	Autorité de certification suprême de l'administration fédérale suisse pour les certificats émis en vertu de la SCSE ainsi que pour les certificats de classe B. Elle est communément appelée Swiss Government Root CA I.
Cartes à puce non préparées	Cartes à puce non soumises au processus des cartes à puce préparées de la SG PKI. Elles doivent être initialisées préalablement pour émettre un certificat. De plus, leurs données de chiffrement pour la signature et l'authentification sont générées directement au niveau de la puce.
Cartes à puce préparées	Cartes à puce soumises, avant leur utilisation, au processus éponyme de la SG PKI. La préparation consiste à les initialiser, à les doter de trois jeux de trois paires de clés chacun et à les sécuriser à l'aide d'une PUK et d'un NIP. Le numéro de série de la carte à puce est enregistré de manière centralisée avec les identifiants des clés, les clés de chiffrement, la PUK et le NIP.
Certificat	Un certificat contient la clé publique d'un titulaire de certificat ainsi que d'autres indications sur celui-ci. L'information complète est signée numériquement au moyen de la clé privée de l'autorité de certification qui émet le certificat. Le format est conforme à la recommandation X.509 [19].
Certificat de fonction de classe B	Un compte d'administration ou de test valable est nécessaire pour l'obtention d'un certificat de fonction. Le requérant doit se présenter personnellement muni d'une pièce d'identité valable devant une autorité d'enregistrement locale. Contrairement à un certificat standard de classe B et à un certificat pour un compte T, seul un certificat d'authentification est émis (sur une carte à puce ou une clé USB) pour un compte A.
Certificat standard de classe B	Produit standard de la SG PKI – voir Définition des produits. Les certificats sont délivrés sur une carte à puce non préparée ou sur une clé USB.
Certificate Policy / Certificate Practice Statement (CP/CPS)	Certificate Policy (directives de certification) / Certificate Practice Statement (dispositions d'exécution de la SG PKI): document décrivant les processus d'établissement et de gestion des certificats émis par la CA concernée.
Certificate Service Provider (CSP)	Certificate Service Provider (fournisseur de services de certification): organisation exploitant une infrastructure PKI (p. ex. la Swiss Government PKI).
Classes de certificats	La Swiss Government PKI émet des certificats de classe A, B, C et D de différentes CA [16].
Client de bureautique	Poste de travail de la Confédération (station de travail de l'OFIT)

Terme / Abréviation	Signification
Client LRA	Anciennement appelé station LRA, le client LRA englobe le matériel (ordinateur portable ou de bureau, scanneur, imprimante) et les logiciels correspondants (application d'enregistrement, pare-feu, chiffrement du disque, etc.) utilisés par l'officier LRA pour émettre et révoquer des certificats.
Co-certificat	Certificat servant à établir une relation de confiance entre deux autorités de certification. Est aussi appelé certificat croisé.
Données d'activation	Données que doit entrer un utilisateur pour activer un module cryptographique (p. ex. carte à puce). Les clés privées ne font pas partie des données d'activation.
Identificateur d'objet OID	Identificateur alphanumérique unique enregistré conformément aux normes internationales en la matière pour désigner un objet ou une classe d'objets spécifique.
Infrastructure à clé publique (PKI)	Ensemble complet des directives, processus, environnements serveurs, logiciels et postes de travail servant à l'administration des clés et des certificats y relatifs.
Liste des autorités de certification révoquées (Authority Revocation List, ARL)	Liste des certificats d'émetteur qui ont été révoqués.
Liste des certificats révoqués (Certificate Revocation List, CRL)	Liste contenant les numéros de série des certificats révoqués avant leur échéance. Cette liste est tenue à jour et publiée par l'autorité de certification.
Livret F	Livret pour les étrangers admis provisoirement. Ceux-ci font l'objet d'une décision de renvoi de Suisse, mais l'exécution dudit renvoi s'est révélée illicite (violation du droit international public), inexigible (mise en danger concrète de l'étranger) ou matériellement impossible (pour des motifs techniques d'exécution).
Numéro d'identification personnel (NIP)	Le NIP permet à l'utilisateur d'accéder au contenu du support de données sécurisé.
Officier LRA	L'officier LRA est une personne qui exerce les fonctions de la LRA (p. ex. identification du client, émission ou révocation d'un certificat) sur mandat de la SG PKI.
Personal Unblock Key (PUK)	Clé personnelle de déblocage. Elle est utilisée pour débloquer une carte bloquée suite à la saisie trop fréquente d'un NIP erroné et pour lui attribuer un nouveau NIP.
Politique de sécurité (PS)	Une politique de sécurité comprend l'ensemble des directives et des prescriptions élaborées sur la base d'une analyse des risques. Elle a pour but la réduction de dommages possibles par des dispositions préventives et la correction d'irrégularités au moyen de mesures adéquates. La politique de sécurité sert à protéger l'intégrité, la disponibilité et les données du prestataire de services de certification. Les spécifications de la politique de sécurité définissent le niveau de sécurité visé pour un système d'information et pour chaque composante de l'architecture de sécurité.
Publication (d'un certificat)	Opération consistant à mettre un certificat à la disposition de tiers pour leur permettre de crypter des informations.
Registration Identification Officer (RIO)	Le RIO procède à l'identification personnelle du requérant sur la base de sa pièce d'identité en cours de validité et de sa demande dûment remplie (*Demande RIO en vue de l'émission de certificats de classe B*). Il remet au requérant une carte à puce préparée, copie la pièce d'identité sur la demande et transmet à l'officier LRA mandant, par courrier, par coursier ou par courriel crypté, sous forme de fichiers numérisés et signés, le document dûment signé, la liste de contrôle RIO et le formulaire signé *Convention et conditions d'utilisation des certificats de classe B*. Le RIO travaille toujours sur mandat d'un officier LRA déterminé.
Renouvellement d'un certificat	Un certificat est émis à la demande d'un titulaire de certificat. La paire de clés sous-jacentes est à nouveau définie. Un nouveau certificat est donc établi pour le titulaire concerné. La génération d'un nouveau certificat après une révocation n'est pas un renouvellement.
Requérant	Un requérant est une personne demandant un certificat. Une fois celui-ci émis, cette personne est appelée titulaire de certificat.
Signature numérique	Résultat du codage d'un message à l'aide d'un système cryptographique utilisant des clés, de telle sorte que la personne qui reçoit le message initial puisse déterminer: 1. si la clé qui a servi au codage du message est bien celle du signataire; 2. si le message a été modifié depuis le moment de son codage.

Terme / Abréviation	Signification
Swiss Government Enhanced CA 01	Tous les certificats standard de classe B ainsi que les certificats de classe B des cartes à puce préparées des cantons et des offices qui ne font pas partie des périmètres 1 et 2 de l'administration fédérale sont émis avec cette autorité de certification.
Swiss Government Enhanced CA 02	La Swiss Government Enhanced CA 02 sert exclusivement à émettre des certificats de l'administration fédérale sur des cartes à puce préparées.
Swiss Government PKI (SG PKI)	Par Swiss Government PKI ou SG PKI (autrefois AdminPKI), on entend l'infrastructure de l'OFIT pour les classes de certificat proposées comme service standard (ancienne prestation transversale).
Titulaire de certificat	Les titulaires de certificat de la Swiss Government PKI classe B sont des collaborateurs ou des unités administratives de l'administration fédérale suisse, de l'administration cantonale ou de l'administration communale. Dans le certificat - selon X.509 -, il est appelé subject (sujet).
Utilisateur de certificat	Un utilisateur de certificat est une personne utilisant un certificat d'un titulaire. Un utilisateur de certificat peut aussi être une unité d'organisation de l'administration fédérale, un système informatique, une application informatique ou un titulaire de certificat d'une autre PKI ainsi que d'un client ou d'un fournisseur.
Utilisateur pouvant réinitialiser des NIP (PIN Reset User, PRU)	Utilisateur pouvant exécuter sur son poste de travail l'assistant de réinitialisation des NIP pour une autre personne. Chaque utilisateur peut être un PRU si son poste de travail dispose de deux lecteurs de carte à puce.
Valeur de hachage, empreinte digitale	Une valeur de hachage est une valeur numérique définie grâce à un algorithme de hachage à partir de données saisies. Étant donné qu'un bon algorithme génère une valeur de hachage différente pour des données distinctes, celle-ci sert notamment d'«empreinte digitale» pour garantir l'envoi non falsifié des documents. En cas de falsification, la valeur de hachage calculée par le destinataire ne concorderait plus avec celle envoyée par l'expéditeur. La valeur de hachage cryptée avec la clé secrète de l'expéditeur est appelée signature numérique.

Références

Identification	Titre, source
[1]	**Swiss Government PKI - Root CA I CP/CPS** Certificate Policy and Certification Practice Statement of the Swiss Government Root CA I Version V2.8 du 15.5.2019 Source: Swiss Government PKI (http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf)
[2]	**Convention et conditions d'utilisation des certificats de classe B** Pour l'obtention de certificats personnels avancés de la Swiss Government PKI des autorités fédérales de la Confédération suisse Version 1.1 du 31.3.2017 Source: Swiss Government PKI
[3]	**Directives relatives aux certificats de classe B de la Swiss Government PKI** Explications concernant l'obtention et l'utilisation des certificats de classe B de la Swiss Government PKI Version 1.0 du 9.3.2017 Source: Swiss Government PKI
[4]	**Vérification de l'identité des requérants, certificats de la classe B** Prescriptions contraignantes et détaillées concernant la vérification de l'identité des requérants de certificats de la classe B de la Swiss Government PKI, dérogations comprises Version 1.2 du 14.11.2017 Source: Swiss Government PKI
[5]	**Formulaire supplémentaire pour les requérants titulaires d'un livret F** Document à remplir en plus du formulaire de demande lorsque le requérant n'a pas de pièce d'identité en cours de validité, mais présente uniquement un livret F. Version 1.0 du 20.9.2019 Source: Swiss Government PKI

Identification	Titre, source
[6]	**Quickguide WALK-IN SYNCHRON** Guide d'émission des certificats de classe B (standard et prestaged) Version 1.1 de janvier 2017 Source: Swiss Government PKI
[7]	**Quickguide PIN Reset** Guide de réinitialisation du NIP de la carte à puce Version 1.1 de janvier 2017 Source: Swiss Government PKI
[8]	**Quickguide Rekeying (Renewal)** Guide de renouvellement des certificats de classe B Version 1.1 de janvier 2017 Source: Swiss Government PKI
[9]	**Quickguide Key Recovery** Guide de restauration des certificats de cryptage Version 1.1 de janvier 2017 Source: Swiss Government PKI
[10]	**Quickguide Revoke** Guide de révocation des certificats de classe B Version 1.0 du 3.6.2016 Source: Swiss Government PKI
[11]	**Quickguide Register Smartcard** Guide d'enregistrement de la carte à puce Version 1.0 du 28.12.2016 Source: Swiss Government PKI
[12]	**Quickguide: changement de langue dans les Wizards** Description pour changer la langue dans les Wizards Version 1.0 du 26.1.2017 Source: Swiss Government PKI
[13]	**Directives pour le Registration Identification Officer (RIO)** Version 2.0 du 1.2.2017 Source: Swiss Government PKI
[14]	**Quickguide WALK-IN ASYNCHRON** (en allemand uniquement) Quickguide zur Ausstellung von Zertifikaten Klasse B (Standard und Prestaged) mit RIO Version 1.1 de janvier 2017 Source: Swiss Government PKI
[15]	**Quickguide Token Unseal** Guide de déblocage des cartes de type préparé (émission des certificats par le RIO, indications pour le client final) Version 1.0 du 6.6.2016 Source: Swiss Government PKI
[16]	Public Key Infrastruktur (PKI) in der Bundesverwaltung: Positions- und Strategiepapier, Version 1.1, vom 7. April 2004 (Infrastructure de clé publique dans l'administration fédérale: document de positionnement et de stratégie, version 1.1 du 7 avril 2004)
[17]	Ordonnance du 4 mars 2011 sur les contrôles de sécurité relatifs aux personnes (OCSP)
[18]	ITU-T X.500, L'annuaire: Vue d'ensemble des concepts, modèles et services
[19]	ITU-T X.509, L'annuaire: Cadre d'authentification

Identification	Titre, source
[20]	RFC 5280, Infrastructure de clés publiques X.509 Internet, Certificat et profil LRC; septembre 2005
[21]	RFC 3647, Infrastructure de clés publiques X.509 Internet, Protocoles de gestion des certificats, novembre 2003
[22]	Directive technique n° 20 (DT20), Structure Admin Directory, Office fédéral de l'informatique et de la télécommunication, 1er juin 1999
[23]	RFC 2526, Public Key Infrastructure Certificate Policy and Certificate Practices Framework, March 1999
[24]	W002 - Directives du Conseil fédéral concernant la sécurité informatique dans l'administration fédérale
[25]	Norme A006 «Smartcard» de l'UPIC, version 2.1, et annexe (avec les composants autorisés)
[26]	Énoncé des pratiques de certification de l'autorité de certification Admin-CA3, 30.3.2005
[27]	Whitepaper concernant les exigences de complexité des NIP des cartes à puce https://intranet.isb.admin.ch/dam/isb_kp/de/dokumente/themen/sicherheit/technologiebetrachtungen/
[28]	Ordonnance sur le traitement des données personnelles liées à l'utilisation de l'infrastructure électronique de la Confédération (RS 172.010.442) du 22 février 2012 (état le 1er avril 2012) Entrée en vigueur: 1er avril 2012 Source: https://www.admin.ch/opc/fr/official-compilation/2012/947.pdf
[29]	Loi fédérale sur la protection des données (LPD; RS 235.1) du 19 juin 1992 (état le 1er mars 2019) Entrée en vigueur: 1er juillet 1993 Source: https://www.admin.ch/opc/fr/classified-compilation/19920153/201903010000/235.1.pdf
[30]	Ordonnance concernant la protection des informations (OPrI; RS 510.411) du 4 juillet 2007 (état le 1er janvier 2018) Entrée en vigueur: 1er août 2007 Source: https://www.admin.ch/opc/fr/official-compilation/2007/3401.pdf
[31]	Ordonnance sur l'informatique dans l'administration fédérale (OIAF; RS 172.010.58) du 9 décembre 2011 (état le 1er avril 2018) Entrée en vigueur: 1er janvier 2012 Source: https://www.admin.ch/opc/fr/official-compilation/2011/6093.pdf

Table des matières

Table des tableaux

1 Généralités

Contenu du présent document

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

Public cible

Ce document s'adresse en premier lieu aux officiers LRA de classe B formés et travaillant pour les offices et cantons. Il sert également de support aux organes externes chargés des audits de la LRA dans les organisations.

Termes et abréviations utilisés

Les termes et abréviations spécifiques utilisés dans le présent document figurent dans le tableau «Définitions, acronymes et abréviations», page 3, où ils font l'objet de brèves explications.

Documents référencés

Les renvois aux documents de référence sont indiqués entre crochets contenant l'indicateur correspondant, par exemple [1]. Les documents figurant dans le tableau «Références», page 5, renferment le cas échéant des compléments d'information au présent document.

Formulation non sexiste

Par souci de lisibilité, seule la forme masculine est utilisée dans l'ensemble de ce document pour désigner aussi bien des personnes de sexe féminin que des personnes de sexe masculin.

1.1 But du document

Le document «Certificate Policy and Certification Practice Statement of the Swiss Government Root CA I» (abrégé ci-après par «CP/CPS») [1] est le règlement déterminant pour les certificats de classe B. Il vise à préciser les exigences du CP/CPS concernant la LRA.

1.2 Champ d'application

La présente directive s'applique à tous les collaborateurs travaillant dans le domaine de la LRA (Local Registration Authority) de la classe B. La Swiss Government 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.

1.3 Certificats de classe B de la Swiss Government PKI

Les certificats de la classe B sont enregistrés sur un support de données sécurisé (une carte à puce ou une clé USB contenant une puce chiffrée) et ne sont remis au requérant qu'après son enregistrement personnel.

Le titulaire d'un certificat de classe B est une personne physique (pas une organisation, un groupe ou une fonction). Il possède généralement une ou trois paires de clés avec les certificats correspondants. En effet, suivant le type de certificat (certificat standard 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 pour l'authentification et d'une troisième pour le chiffrement des clés et des données, soit d'une seule paire de clés pour l'authentification. Pour les certificats de classe B de type préparé, 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.

Pour les organisations ayant leur propre gestion des PUK, l'initialisation du support de sécurité est exécutée avec l'outil du fournisseur de cartes et ne fait pas partie de l'application d'enregistrement. Les cartes à puce qui

utilisent la gestion des PUK de la Swiss Government PKI sont initialisées soit lors de leur configuration (cartes à puce préparées), soit directement lors de l'émission à l'aide de l'assistant d'enregistrement (Walk-In Wizard), soit grâce à l'assistant d'enregistrement de la carte à puce (Register Smartcard Wizard; cartes à puce non préparées).

Lors du renouvellement de cartes à puce préparées, la CA signe le prochain trio de clés. Si les cartes à puce ne sont pas préparées, l'application génère un nouveau jeu de paires de clés et les fait signer par la CA. Les anciennes clés et les anciens certificats destinés à la signature et à l'authentification sont ensuite supprimés de la carte. L'ancienne paire de clés destinée au cryptage des clés et des données est conservée sur la carte en vue d'un décryptage ultérieur.

Un titulaire peut posséder à la fois un certificat de classe A, un certificat standard 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.

1.4 Supports de sécurité

La liste et les spécifications détaillées des supports de sécurité pris en charge figurent dans la norme «A006 – Smartcard» [25] approuvée par l'Unité de pilotage informatique de la Confédération (UPIC) ainsi que dans son annexe.

2 Tâches de l'officier LRA et du RIO

2.1 Profil requis de l'officier LRA

- Haute intégrité personnelle
- Travail précis selon les prescriptions de la Swiss Government 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 OCSP (RS 120.4) ou à un contrôle similaire, exécuté par la propre autorité (cf. chap. 3.12)
- Un officier LRA n'est pas autorisé à saisir ou à modifier les entrées de l'Admin Directory.

2.2 Tâches de l'officier LRA classe B

L'officier LRA assume les tâches suivantes:

- vérifier la demande ainsi que les formulaires et documents complémentaires requis (cf. point 5.2.3.2 «Contrôler le formulaire de demande»);
- identifier le requérant (cf. point 5.2.3.5 «Contrôler l'identité du requérant»);
- vérifier les données de l'Admin Directory;
- établir le certificat;
- révoquer le certificat;
- informer le client en ce qui concerne:
  - les données d'activation;
  - la protection des données d'activation;
  - ses droits et ses obligations;
  - «Convention et conditions d'utilisation des certificats de classe B» [2];
  - «Directives relatives aux certificats de classe B de la Swiss Government PKI» [3];
- le cas échéant, remplir et archiver les listes de contrôle;
- tenir un journal des activités liées aux certificats;
- tenir et conserver les dossiers des titulaires de certificats;
- gérer, voire acquérir et initialiser 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 de classe B», «Directives relatives aux certificats de classe B de la Swiss Government PKI» 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 les connaissances relatives aux prescriptions, aux processus et aux moyens techniques en relation avec les certificats de classe B.

2.3 Profil requis du RIO

- Travail précis selon les prescriptions de la Swiss Government 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

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 client en ce qui concerne:
  - les données d'activation;
  - la protection des données d'activation;
  - ses droits et ses obligations;
- vérifier la demande ainsi que les formulaires et documents complémentaires requis (cf. point 5.2.3.2 «Contrôler le formulaire de demande»);
- copier la pièce d'identité et la demande;
- remplir la liste de contrôle;
- transmettre à l'officier LRA mandant, par courrier, par coursier ou par voie électronique, la liste de contrôle dûment remplie, les éventuels formulaires complémentaires, la copie signée de la demande accompagnée d'une copie d'une pièce d'identité en cours de validité ainsi que le formulaire signé *Convention et conditions d'utilisation des certificats de classe B* [2]. S'il choisit la voie électronique: numérisation des documents ci-dessus sous forme de fichiers PDF, signature numérique de ceux-ci au moyen de son certificat personnel de classe B et envoi de l'ensemble à l'officier LRA par courriel chiffré.

Un officier LRA (LRAO) peut assumer le rôle d'un RIO, l'inverse n'étant pas possible.

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.

3.2 Soutien de la LRA

La LRA peut demander le soutien de l'équipe d'exploitation de la Swiss Government PKI selon les indications du catalogue des produits et services et le Service Level Agreement (SLA) en vigueur.

En cas de dysfonctionnements, l'équipe d'exploitation peut être contactée par l'intermédiaire du Service Desk de l'OFIT (+41 (0)58 465 88 88).

En cas de communications et de questions urgentes en matière de sécurité, il convient de prendre contact avec un officier de sécurité de la Swiss Government PKI également 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. 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 reste à disposition pour obtenir des conseils.

3.3 Contrôle des accès

Aucune exigence particulière n'est posée aux locaux de la LRA. Les équipements de celle-ci peuvent se trouver dans un bureau normal. Ne sont toutefois pas admis les locaux auxquels peuvent accéder des personnes non autorisées, à l'instar des salles de réunion, des locaux d'infirmerie, etc. Les locaux en question devraient être facilement accessibles aux requérants et leur offrir suffisamment d'intimité pour saisir leurs NIP/PUK personnels, ainsi que la phrase de révocation. S'il s'agit de bureaux paysagers partagés avec des collaborateurs n'exerçant aucune fonction de la LRA, il doit y avoir une section protégée/séparée réservée aux tâches de la LRA. Le local devra 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 d'accès au client LRA

L'accès au client de bureautique (poste de travail de la Confédération) comportant les fonctions du client LRA est protégé par une authentification à deux facteurs (certificat de classe B). Le client LRA est équipé d'un chiffrement du disque. Les applications LRA ne peuvent être lancées qu'avec des autorisations d'officier LRA figurant sur une carte LRAO distincte ou avec un certificat « ordinaire » de classe B lors d'une authentification à deux facteurs. 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 doit toujours être emportée avec soi ou mise sous clé. Lorsque l'officier LRA ne travaille pas sur le client de bureautique, 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. Toute perte de la carte à puce doit être déclarée sans délai au Service Desk de l'OFIT et à la Swiss Government PKI, qui bloquent immédiatement ladite carte.

3.5 Directives concernant les clients LRA

Les clients de bureautique comprenant une fonction LRA et leurs utilisateurs sont soumis à des prescriptions de sécurité strictes ainsi qu'aux directives du Conseil fédéral concernant la sécurité informatique dans l'administration fédérale [24] et à l'OIAF [31]. Il est absolument interdit:

- d'y installer un logiciel de manière autonome,
- d'y raccorder du matériel qui n'est pas fourni par l'OFIT,
- de procéder à des modifications de la configuration logicielle ou matérielle,
- d'utiliser les clients LRA pour d'autres tâches que pour les tâches expressément prévues.

3.6 Formulaires et données clients

Les formulaires délivrés par la SG PKI et indiqués dans la présente directive doivent être utilisés impérativement, 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 dossiers clients (formulaires de demande, feuilles d'information, demandes de révocation, etc.) doivent être conservés sous clé (principe du cleardesk). Soit la pièce est verrouillée et uniquement accessible à l'officier LRA, soit les documents sont mis sous clé dans une armoire que seul l'officier LRA peut ouvrir.

Si les dossiers 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

Toutes les activités de la LRA concernant l'émission, la révocation et la récupération de clés de certificats ainsi que d'autres événements importants sont consignées dans le journal. Les activités suivantes de la LRA sont notamment importantes:

- émission de certificats;
- révocation de certificats;
- remplacement/réparation/déplacement temporaire d'un client LRA;
- réception de nouvelles cartes à puce vierges;
- réception d'une nouvelle carte à puce pour l'officier LRA;
- demandes de réinitialisation du NIP (si le système correspondant de la SG PKI n'est pas utilisé);
- le cas échéant, numéro de mandat interne (p. ex. numéro de ticket dans le système de saisie des mandats).

Les journaux des officiers LRA peuvent être tenus manuellement (cf. «Journal de la Swiss Government PKI pour les certificats de classe B») ou 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 de la Time Stamping Authority de la SG PKI (TSA SG PKI). Il est permis de tenir plusieurs journaux par LRA (p. ex. par LRAO, par office, par mois, etc.), pour autant que la chronologie et l'exhaustivité restent garanties. Un enregistrement local des données du journal sur le client LRA ne peut être que temporaire. Celles-ci doivent ensuite être transférées sur un support/lecteur où l'archivage est garanti conformément au ch. 3.8 «Délais de conservation» et aux dispositions de la LPD et protégé contre un accès par des tiers non autorisés.

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

1. le numéro d'ordre de l'inscription,
2. la date,
3. le nom de l'officier LRA exécutant,
4. le nom du client (requérant / titulaire du certificat),
5. l'activité (préfixe: CS: certificat standard, CFA: certificat d'administrateur, CFT: certificat de test, E: émission, R: révocation, K: récupération de la clé, PR: réinitialisation du NIP).

3.8 Délais de conservation

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

3.9 Conservation des cartes à puce vierges

Les cartes à puce vierges, enregistrées et préparées ainsi que 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 tenus de protéger leurs clés privées/certificats se trouvant sur la carte à puce au moyen de données d'activation, conformément au ch. 3.4.

3.11 Élimination

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

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

3.12 Contrôle de la fiabilité

Avant toute nomination d'un officier LRA, l'autorité prend les mesures autorisées par le cadre légal 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 (RS 120.4), exécuté par le service spécialisé CSP du Département fédéral de la défense, de la protection de la population et des sports (DDPS) [17]

et/ou

- prise de mesures internes de contrôle de la fiabilité, par exemple:
  - contrôle de l'identité du candidat (passeport ou carte d'identité);
  - vérification des références professionnelles ou personnelles du candidat;
  - vérification de l'exhaustivité et de la cohérence du curriculum vitæ du candidat;

- 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 considère que le candidat est fiable et intègre, et confirme en outre qu'il dispose des compétences requises pour exercer la fonction sensible d'officier LRA.

3.13 Confidentialité, protection des données

L'officier LRA doit signer une déclaration de confidentialité, qui est intégrée dans le formulaire de demande.

Les lois et ordonnances relatives à la protection des données (LPD) [29] ainsi que l'ordonnance concernant la protection des informations (OPrI) [30] doivent être respectées.

Il faut veiller en particulier à transmettre les données clients ou les données importantes de la LRA ou de la CA sous une forme chiffrée et à ce qu'aucun tiers non autorisé n'y ait accès.

3.14 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 de 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 au niveau de ses connaissances ou de ses aptitudes et qu'il ne peut pas y remédier lui-même, il est tenu de l'annoncer à la SG PKI. Celle-ci recherchera une solution avec lui.

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.

Les RIO doivent également suivre une formation, mais de moindre envergure. Celle-ci est en principe dispensée par l'officier LRA qui leur donne leur mandat. 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*» [4], «*Directives pour le Registration Identification Officer (RIO)*» [13] , «*Convention et conditions d'utilisation des certificats de classe B*» [2] et «*Directives relatives aux certificats de classe B de la Swiss Government PKI*» [3].

3.15 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 http://www.pki.admin.ch. Elle s'engage à signaler par courriel les modifications importantes. De son côté, l'officier LRA est tenu de lire les informations mises en ligne par la SG PKI dans l'espace clients de son site dès qu'il a reçu le courriel 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 18 mois. Le tableau ci-après indique quelles activités permettent d'accumuler un nombre de points précis.

Activité	Nombre de points
Formation de base	10
Test de la formation de base	10
LRAO Summit (1/2 journée)	10
Atelier LRAO (1/2 journée)	5 à 10 (selon le contenu)
Atelier personnalisé LRAO (au moins 4 participants, sur place)	5 à 10 (selon le contenu)
Réunion préparée / téléconférence (sur un thème précis)	5

Tableau 1: Nombre de points par manifestation LRAO

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

3.16 Règles pour les NIP

Les titulaires de certificats utilisent des NIP (mots de passe) pour activer leurs cartes à puce ou leurs clés privées. Ce NIP diffère en principe du mot de passe qui est utilisé par exemple pour se connecter aux applications [27]. Tout titulaire de certificat choisit ses propres NIP. Concernant ce choix, nos règles sont les suivantes:

- *longueur:* le NIP doit comprendre au moins six caractères;
- *nombre d'essais:* la carte doit se bloquer automatiquement après 5 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 triviaux (p. ex. votre identifiant d'utilisateur ou 123456);
- *validité*: le NIP doit être changé dès qu'on soupçonne qu'un tiers en a pris 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.

3.17 Phrase de révocation

La phrase de révocation sert à identifier l'utilisateur 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. Elle est composée d'une question et de la réponse correspondante.

La réponse à la question doit être choisie de manière à ne pas pouvoir être déduite ou devinée facilement par des tiers. Elle doit, d'autre part, être bien connue par le requérant, de manière qu'il puisse toujours répondre à la question sans problème ni doute.

3.18 Réinitialisation du NIP et gestion de la PUK

En principe, une procédure de déblocage à l'aide de la PUK doit être prévue pour chaque carte à puce bloquée. La gestion des PUK relève toutefois de la compétence de l'autorité, dans la mesure où la carte préparée de la SG PKI n'est pas utilisée. Cette dernière a développé pour ses cartes préparées un système électronique centralisé avec gestion des PUK, dans lequel la PUK est conservée de manière chiffrée sur l'un des serveurs de la SG PKI et mise à la disposition de la carte en arrière-plan pendant le processus de déblocage. La PUK n'est à aucun moment visible.

Si un autre système est utilisé pour gérer les PUK des cartes non préparées (Scamiad, Privacy PUK ou autres), l'office doit veiller à ce que:

- les PUK soient uniquement mises à la disposition des personnes autorisées (collaborateurs des Service Desks, officiers LRA) sous une forme électronique ou par écrit (sur papier, sous enveloppe, etc.);
- les PUK ne puissent être consultées par les officiers LRA ou le personnel du Service Desk compétent qu'avec le consentement exprès du titulaire de la carte (en raison du blocage de celle-ci, p. ex.);
- la consultation d'une PUK soit dûment documentée (p. ex. à l'aide d'un système de saisie des mandats, d'un ticket, d'une entrée de journal, etc.);
- la même PUK ne serve pas pour plusieurs cartes;
- les PUK ne puissent pas être «devinées» (p. ex. numéro personnel, numéro de carte, etc.);
- une description du système utilisé (procédures, activités, rôles, lieux d'archivage, etc.) soit disponible et approuvée par l'office.

Si une carte préparée de la SG PKI est utilisée, les principes suivants s'appliquent au personnel d'assistance ou à l'officier LRA:

- Il faut faire appel à un PIN Reset Superuser pour réinitialiser le NIP. Ce superutilisateur peut ouvrir dans une application Web un ticket interne pour la carte concernée, après en avoir dûment identifié le titulaire. L'identification peut également être réalisée par téléphone à l'aide de la phrase de révocation. Ensuite seulement, le titulaire pourra faire réinitialiser son NIP par un PIN Reset User (PRU).
- Le déblocage d'une carte nécessite un PRU, qui est chargé de «prêter» son ordinateur au titulaire de la carte et de lancer pour lui l'assistant de réinitialisation du NIP, car le blocage de la carte empêche l'authentification à deux facteurs du titulaire. Pour ce faire, l'utilisateur concerné doit être avec le PRU et insérer sa carte dans un second lecteur de cartes relié à l'ordinateur du PRU.
- Les fonctions «PIN Reset Superuser» et «PRU» ne peuvent pas être assumées simultanément par une seule et 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 préparées est exposée en détail dans le guide «PIN Reset» [7].

4 Contrôle de conformité

La SG PKI est tenue de vérifier tous les 18 mois l'application du CPS. En fait partie 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.

Les autorisations de l'officier LRA concerné peuvent être révoquées si celui-ci échoue à ce contrôle de conformité. En cas de manquements particulièrement graves, le responsable PKI ou le responsable de la sécurité PKI peut également demander la révocation de tous les certificats d'utilisateur émis par l'officier LRA fautif.

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, type préparé
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.
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 (*rekeying*) est possible au maximum deux fois.

Tableau 2: Processus de classe B, type préparé

Classe B, type non préparé
La carte à puce est initialisée: • lorsque les certificats sont émis avec l'assistant d'enregistrement (Walk-In Wizard), ou • lors de son enregistrement avec l'assistant éponyme (Register Smartcard Wizard), ou • par l'officier LRA en dehors du processus, à l'aide du système de gestion des PUK spécifique à l'organisation.
Lors de l'établissement des certificats, trois paires de clés (signature, authentification, chiffrement) sont générées sur la carte.
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 (*rekeying*) est autorisé au maximum deux fois.

Tableau 3: Processus de classe B, type non préparé

Certificat de fonction de classe B pour comptes A (administrateur)
L'officier LRA initialise la carte à puce lors de l'établissement du certificat à l'aide de l'assistant d'enregistrement (Walk-In Wizard).
Seule la paire de clés destinée à l'authentification est générée sur la carte lors de l'établissement.
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 4: Processus pour les comptes A

Certificat de fonction de classe B pour comptes T (test)
L'officier LRA initialise la carte à puce lors de l'établissement du certificat à l'aide de l'assistant d'enregistrement (Walk-In Wizard).
En général, une paire de clés (authentification) est générée sur la carte lors de l'établissement. Si nécessaire, des clés de signature et de chiffrement sont également autorisées.
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.
Aucun renouvellement n'est autorisé.

Tableau 5: Processus pour les comptes T

L'officier LRA et le participant disposent de plusieurs assistants pour les processus avec et sans RIO. Voir à ce sujet les références [6], [7], [8], [9], [10], [11], [12], [14] et [15].

5.2 Processus d'émission d'un certificat

On distingue deux variantes du processus d'émission:

- processus d'émission sans RIO (Registration Identification Officer),
- processus d'émission avec RIO.

Ci-après, nous appelons le processus sans RIO «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
Identification personnelle du requérant effectuée directement par l'officier LRA. Comme preuve, celui-ci scanne la pièce d'identité du requérant. Lorsque le requérant bénéficie d'une dérogation, les pièces d'identité et les documents définis pour celle-ci doivent être contrôlés et numérisés. Ils sont mentionnés pour chaque exception au point 5.2.3.5 «Contrôler l'identité du requérant».	Identification personnelle du requérant effectuée directement par le RIO. À titre de preuve, le RIO copie la pièce d'identité en cours de validité et le formulaire de demande dûment rempli. Lorsque le requérant bénéficie d'une dérogation, les pièces d'identité et les documents définis pour celle-ci doivent être contrôlés et numérisés. Ils sont mentionnés pour chaque exception au point 5.2.3.5 «Contrôler l'identité du requérant». Le RIO remplit la liste de contrôle et transmet ces documents ainsi que le formulaire signé «Convention et conditions d'utilisation des certificats de classe B» [2] à l'officier LRA sur mandat duquel il agit.
Vérification du requérant dans l'Admin Directory par l'officier LRA	Vérification du requérant dans l'Admin Directory par le RIO
Instruction du participant concernant les données d'activation et leur protection par l'officier LRA	Instruction du participant concernant les données d'activation et leur protection par le RIO
L'officier LRA génère la demande pour le participant. Lors de la dernière étape de l'assistant d'enregistrement (Walk-In Wizard), le participant saisit son NIP et les données destinées à la révocation par téléphone (phrase de révocation).	Validation de la demande par l'officier LRA
	Le participant 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 correspondant (Unseal Wizard).

Tableau 6: 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.

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.). Le processus de commande doit, dans tous les cas, être traçable et pouvoir être audité, pendant 11 ans après l'échéance du certificat. La SG PKI met à disposition un formulaire qui comprend toutes les données requises pour la demande (cf. en annexe).

Lorsque des certificats sont commandés dans 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, dans tous les cas, être complétés et annexés à la demande.

5.2.3 Émission sans RIO

La LRA doit être utilisée conformément aux documents de formation de l'officier LRA et aux guides concernant les différents assistants [6], [7], [8], [9], [10], [11], [12], [14] et [15]. La présente directive prime en cas de contradiction.

L'officier LRA procède selon la «Liste de contrôle: émission de certificats de classe B

Processus de classe B «Émission sans RIO» (point 5.2.3 des directives d'enregistrement**)**.

5.2.3.1 Vérifier l'inscription 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».
   En cas de certificats de fonction pour comptes A: adresse électronique du titulaire du compte.
   En cas de certificats de fonction pour comptes T: adresse électronique du compte T. Elle doit être identifiable au moyen du suffixe «test», «TST» ou d'un suffixe similaire.
2. S'il existe plus d'une inscription dans Admin Directory: l'inscription 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, il faut demander son enregistrement ou la modification de l'entrée par l'administrateur de l'Admin Directory de l'office. La procédure ne pourra continuer que lorsque le requérant sera enregistré correctement dans Admin Directory (en général, la reproduction des données dure au minimum une nuit). L'officier LRA peut effectuer la vérification dans l'assistant d'enregistrement (Walk-In Wizard), par exemple.

5.2.3.2 Contrôler le formulaire de demande

Contrôler l'intégrité et l'exactitude du formulaire de demande.

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'enregistrement dans Admin Directory?
3. Le formulaire est-il correctement daté et signé?

Depuis l'introduction de la connexion à deux facteurs pour les systèmes clients de l'administration fédérale, le responsable RH concerné peut aussi envoyer une liste des nouveaux collaborateurs à l'officier LRA compétent. La liste doit contenir, pour chaque collaborateur, les mêmes données que le formulaire de demande. Au sein de l'OFIT, un MAC est disponible dans Remedy pour commander des certificats de classe B.

5.2.3.3 Accord pour une date d'émission

Une date doit être convenue avec le requérant pour l'émission du certificat. À cet effet, un courriel est envoyé à l'adresse électronique figurant sur la demande. Ce courriel doit contenir les informations suivantes:

1. Proposition de date(s) pour l'émission du certificat
2. Demande au requérant de prendre avec lui une pièce d'identité valable. Celle-ci ne doit pas être échue à l'instant de l'enregistrement. Pour les dérogations, il faut apporter les formulaires et documents supplémentaires définis pour l'exception concernée (voir point 5.2.3.5 «Contrôler l'identité du requérant»).
3. Demande au requérant de préparer un NIP. Lui rappeler les règles en vigueur pour les NIP selon le point 3.16 «Règles pour les NIP».
4. Demande au requérant de préparer une phrase de révocation.
5. 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. Les informations énumérées ci-dessus doivent être communiquées dans tous les cas au requérant.

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). Ensuite, l'utilisateur est recherché dans l'application d'émission à l'aide de son nom ou de son adresse électronique, l'entrée adéquate étant sélectionnée. Admin Directory est ici la source des données.

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. Celle-ci doit être réalisée au moyen d'un passeport valide ou d'une carte d'identité valable pour l'entrée en Suisse. Le badge du personnel ne suffit pas pour l'identification. 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.
    c. Les indications figurant sur la pièce d'identité concordent-elles avec celles de la demande?
    d. La signature sur la pièce d'identité correspond-elle à celle du formulaire de demande?

2. Identification personnelle du requérant par comparaison avec la photographie se trouvant sur 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?

3. Vérification que les données figurant sur le document correspondent à celles de la demande et à l'inscription dans Admin Directory. En particulier, la concordance entre les nom et prénom inscrits dans le document et ceux d'Admin Directory est attestée selon les critères suivants:

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

- **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» [4]. 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» [4], mais ils sont plausibles. Le requérant possédait déjà un certificat avec ces noms/prénoms (p. ex. en cas de remplacement d'une carte ou lors de l'émission d'une carte subséquente). Il convient dès lors de 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 établi. 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, même en tenant compte des conditions énoncées dans le document «Vérification de l'identité des requérants, certificats de la classe B» [4]. Il n'existe aucun ancien certificat du requérant. Un nouveau certificat ne peut pas être établi. Il convient dès lors de 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 correspondre aux 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:·

- «formulaire supplémentaire pour les requérants titulaires d'un livret F» [5] 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 son organisation;
- autorisation d'exercer une activité lucrative, délivrée par l'autorité cantonale ou fédérale compétente.

5.2.3.6 Préparer la carte

L'administration fédérale utilise de manière stratégique une carte à puce préparée, qui est configurée centralement par la SG PKI en vue de son utilisation et ne doit donc pas être initialisée séparément. Les cartes à puce non formatées et non préparées qui utilisent la gestion des PUK de la SG PKI sont initialisées pendant le processus d'établissement grâce à l'assistant d'enregistrement (Walk-in Wizard) ou à l'assistant d'enregistrement de la carte à puce (Register Smartcard Wizard).

Si le système de gestion des PUK d'autres fabricants (p. ex. Privacy PUK ou SCAMIAD) est utilisé, on procédera conformément aux directives internes de l'unité d'organisation, la carte à puce étant initialisée au préalable avec le produit tiers selon les prescriptions énoncées au point 3.18 des présentes directives.

5.2.3.7 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 (Background Server). Un processus de numérisation est intégré à cet effet dans l'assistant d'enregistrement (Walk-In Wizard).

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

Couleurs:	**TrueColor**
Résolution:	**200 x 200** ou 300 x 300 (suivant les possibilités de réglage du scanner)
Format:	**JPEG** (extension: .jpg)
	PDF (extension: .pdf) pour numériser en recto verso les deux côtés de la carte d'identité

En général, la numérisation produit un résultat de taille A4. Recadrez d'abord le document, de manière à n'enregistrer que la pièce d'identité proprement dite.
Enregistrez le document dans un répertoire privé de votre client. Après avoir émis le certificat, vous êtes tenu de supprimer ces fichiers et les éventuels courriels, puis de vider la corbeille du client et celle d'Outlook.

Attention: les cartes d'identité doivent être numérisées **des deux côtés**, car la date de validité apparaît uniquement au verso.

5.2.3.8 Information au requérant concernant le NIP et la phrase de révocation

On informera une nouvelle fois le requérant sur le sens et le but de la phrase de révocation et, s'il n'en a pas encore défini, on lui demandera d'en préparer une conformément aux prescriptions définies au point 3.17. De même, on lui rappellera les règles de définition du NIP selon le point 3.16.

5.2.3.9 Demander des certificats et les enregistrer sur la carte

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 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 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 en cours de validité. Tous les documents nécessaires à l'identification formelle et à l'enregistrement (p. ex. certificat de mariage, lettre de cautionnement, etc.) doivent être liés. Le processus correspondant est exposé au point 5.2.3.7 «Numériser les documents».

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

L'utilisateur est invité à saisir son NIP et sa phrase de révocation. Les certificats sont ensuite enregistrés sur sa carte à puce, qui est protégée par le NIP.

5.2.3.10 Demander un accusé de réception/signature de la convention d'utilisation

Après la délivrance des certificats, une page contenant leurs «empreintes digitales» (numéro d'identification unique d'un certificat) sera imprimée. Il faut rappeler oralement au requérant ses droits et ses obligations à

l'aide des documents «*Convention et conditions d'utilisation des certificats de classe B*» [2] et «*Directives relatives aux certificats de classe B de la Swiss Government PKI*» [3] (but des certificats, contenu de la carte à puce, révocation des certificats, obligation de diligence concernant le NIP et phrase de révocation).

Enfin, le requérant doit signer une copie du document «*Convention et conditions d'utilisation des certificats de classe B*» [2]. 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 copie des empreintes digitales sera agrafée à l'exemplaire signé de la convention d'utilisation. Au lieu d'une copie papier, l'officier LRA est libre de 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 point 3.8. Si l'officier LRA ne reçoit pas la convention d'utilisation dûment signée, les certificats correspondants doivent être révoqués.

5.2.3.11 Finalisation de l'émission

Pour finir,

- la nouvelle carte à puce,
- les copies non signées des documents «*Convention et conditions d'utilisation des certificats de classe B*» [2] et «*Directives relatives aux certificats de classe B de la Swiss Government PKI*» [3];
- la pièce d'identité et les autres documents requis

sont remis au requérant.

5.2.3.12 Tenir un journal

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

5.2.3.13 Supprimer du système local les données enregistrées

Si la pièce d'identité a été numérisée en dehors de l'assistant d'enregistrement (Walk-In Wizard) et enregistrée localement, le fichier doit être supprimé après la délivrance des certificats. Il faut veiller en particulier à ce qu'aucune information ne soit mémorisée dans les comptes de messagerie personnel ou professionnel (cf. également point 5.2.3.7 «Numériser les documents»).

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 toutefois enregistrés dans la base de données de la SG PKI (qui est déclarée conformément à la LPD [29]).

5.2.3.14 Classement du dossier client

La demande traitée, la copie signée du formulaire et le document *«Convention et conditions d'utilisation des certificats de classe B»* [2] seront archivés dans le dossier client.

Si ce 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 soit identifiable;
- 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 Registration Identification Officer (RIO) l'identification du requérant et d'autres tâches. Ce dernier et le RIO sont sur un site distant de celui de l'officier LRA.

En l'espèce, on parle également de processus d'émission asynchrone. Les certificats de fonction pour comptes A ne peuvent pas être émis en utilisant ce processus.

Les «Directives pour le Registration Identification Officer (RIO)» [13] et le «Quickguide Walk-In asynchron» [14] doivent également être pris en compte dans ce processus. La présente directive prime en cas de contradiction.

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 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 le date et le signe.

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 ou carte d'identité en cours de validité).
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 point 5.2.3.5 «Contrôler l'identité du requérant». La liste correspondante est exhaustive.
4. En cas de conformité, le RIO remet au requérant une nouvelle carte à puce enregistrée 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 à l'utilisateur que ce dernier doit désormais conserver la nouvelle carte 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 de classe B*» [2] et en a reçu une copie. Le requérant doit signer la seconde copie.
7. Le RIO pose le 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 pour la confirmation de la demande.
   Les cartes d'identité doivent être copiées des deux côtés.
8. Le RIO fait une copie 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 copie désormais complétée du formulaire de demande. Le formulaire ne comportant pas la pièce d'identité copiée peut être détruit.
9. Le RIO envoie à l'officier LRA compétent les deux documents signés (formulaire de demande et «*Convention d'utilisation*» [2]), les copies des éventuels documents supplémentaires et la liste de contrôle dûment remplie. L'envoi peut être effectué selon l'un des deux modes indiqués ci-après:
   a. Les documents signés sont envoyés par poste ou par coursier à l'officier LRA compétent.
   b. Le RIO numérise les documents en format PDF/A, les signe au moyen de son certificat standard de classe B. Il envoie ensuite les documents ainsi préparés, par courriel 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 standard 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 les documents sont transmis par voie électronique, les documents au format papier doivent être envoyés ensuite par courrier postal à l'officier LRA pour être classés dans le dossier client si aucun dossier client électronique conforme aux spécifications mentionnées au point 5.2.4.3 «Acceptation de la demande par l'officier LRA» n'est tenu.

5.2.4.3 Acceptation de la demande par l'officier LRA

Après réception et contrôle des documents dûment remplis mentionnés au point 5.2.4.2 «Identification du requérant par le RIO», l'officier LRA peut approuver la demande et valider l'émission des certificats. À cet effet, il procède aux opérations 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 signé;
   - formulaire signé «*Convention et conditions d'utilisation des certificats de classe B de la Swiss Government PKI*» [2];
   - «liste de contrôle RIO» signée;
   - autres documents et pièces d'identité requis en cas de disposition d'exception.

   Si les documents ont été transmis par courriel, l'officier LRA vérifie

   - qu'ils ont été envoyés chiffrés,
   - qu'ils sont dotés de la signature électronique valable du RIO.

2. 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.

3. Si les formulaires ont été transmis sur papier, l'officier LRA numérise les copies signées du formulaire de demande, de la « convention d'utilisation » et de la «*liste de contrôle RIO*» et les autres documents et pièces d'identité requis en cas de disposition d'exception, qu'il a reçus du RIO. Les paramètres suivants permettent d'obtenir de bons résultats qualitatifs:

Couleurs:	TrueColor
Résolution:	200 x 200 ou 300 x 300 (suivant les possibilités de réglage du scanner)
Format:	JPEG (extension: .jpg) ou PDF/A (extension .pdf)

   Les documents reçus par voie électronique peuvent être liés directement. L'officier LRA les charge ensuite dans l'assistant d'enregistrement (Walk-In Wizard).

4. L'officier LRA vérifie si les données inscrites dans le formulaire de demande correspondent à celles figurant sur la copie de la pièce d'identité et à l'inscription du requérant dans Admin Directory (voir directives au point 3 du chap. 5.2.3.5 «Contrôler l'identité du requérant»).

5. Si les indications nécessaires concordent, l'officier LRA saisit le numéro de série de la carte à puce remise à l'utilisateur et valide la demande.

6. La demande validée est jointe à un ticket, puis transférée à la CA pour certification. Le numéro du ticket est consigné dans un document de déblocage (Unseal Document) au format PDF.

7. L'officier LRA transmet le document de déblocage ou le code de déblocage (numéro de l'e-ticket) soit directement à l'utilisateur, soit au RIO.

8. Il consigne la procédure dans le journal.

9. Il archive le formulaire signé «*Convention et conditions d'utilisation des certificats de classe B*» [2] dans le dossier client.

Si le dossier est géré électroniquement, il faut classer soit la version électronique signée par le RIO ou une version PDF/A que l'officier LRA réalise à partir des documents papier, auquel cas il la signera avec son certificat de classe B avant de l'archiver. Les dossiers clients électroniques doivent respecter les exigences visées aux points 5.2.3.13 et 3.8 des présentes directives en matière de sécurité de conservation, de protection des données, de délais de conservation et de capacité de révision.

5.2.4.4 Installation du certificat sur la carte à puce du requérant

En dernier lieu, le certificat doit encore être installé sur la carte à puce du requérant:

1. Après l'émission du certificat, le requérant reçoit par courriel ou par l'intermédiaire du RIO le document de déblocage avec le numéro de l'e-ticket.
2. Il lance l'assistant de déblocage (Unseal Wizard) sur un système client relié au réseau et insère sa carte à puce dans le lecteur de carte. Si le système client exige la connexion à 2 facteurs pour Windows, un deuxième lecteur de carte doit être installé pour ce faire. L'utilisateur 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. En cas de concordance, l'utilisateur est invité à saisir son NIP et sa phrase de révocation.
4. L'assistant enregistre 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.

5.3 Processus de révocation d'un certificat

5.3.1 Qui peut demander une révocation?

La liste exhaustive ci-après mentionne tous les rôles pouvant demander la révocation d'un certificat:

- le titulaire du certificat lui-même,
- les collaborateurs des RH compétentes (services du personnel),
- les supérieurs hiérarchiques,
- le responsable de la Swiss Government PKI,
- l'officier de sécurité PKI,
- l'officier LRA compétent,
- le DSIO de l'office.

5.3.2 Comment demander une révocation?

Le titulaire du certificat peut en demander la révocation à l'officier LRA soit personnellement, soit par courriel, soit par téléphone. L'officier LRA contrôle la plausibilité de la requête, par exemple en se servant de la phrase de révocation.

Des services RH ou des supérieurs hiérarchiques peuvent aussi envoyer des listes de demandes de révocation (p. ex. sous forme de fichiers Excel) à l'officier LRA, ce qui est surtout le cas lors de départs ou de changements de collaborateurs. L'officier LRA vérifie la compétence de l'expéditeur. L'officier LRA ne peut accepter les demandes de révocation de tiers que par écrit (courriel signé, demandes de révocation signées). Seul le titulaire du certificat peut le révoquer par téléphone.

L'officier LRA, l'officier de sécurité PKI et le responsable de la Swiss Government PKI peuvent révoquer directement un certificat dans l'application LRA.

5.3.3 Quels sont les motifs d'une révocation?

Les raisons d'une révocation sont notamment les suivantes:

- la carte à puce a été volée ou ne peut plus être retrouvée,
- la carte à puce est défectueuse,
- la carte à puce est renouvelée,

- le client a oublié le NIP de sa carte à puce et il n'existe aucun système d'administration des PUK pour réinitialiser le NIP,
- la carte à puce a été bloquée suite à un trop grand nombre de tentatives erronées et il n'existe aucun système d'administration des PUK pour débloquer la carte,
- les rapports de travail avec le titulaire du certificat ont pris 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 courriel),
- le client ne respecte pas les directives (non-observation du CP/CPS p. ex.),
- 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), on observera qu'une révocation a pour objectif de protéger le client contre un dommage possible suite à une utilisation abusive de ses 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 elle 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 procède comme suit:

5.3.4.1 Contrôle de la plausibilité de la demande

Bases:

- Le requérant peut-il être identifié (voix, numéro de téléphone, phrase de révocation)?
- Le service RH ou le supérieur hiérarchique est-il compétent pour les titulaires de certificats concernés?

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. point 5.3.1 à ce sujet), elle doit être formulée par écrit à l'aide du document «*Demande de révocation des certificats de classe B de la Swiss Government PKI*». Lorsque la demande n'est pas présentée sur papier, il faut veiller à ce que le document ou le courriel avec la pièce jointe soit signé par le requérant.

De même, un formulaire de révocation est nécessaire lorsque les informations sur cette dernière (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 la révocation, il convient de lancer l'assistant éponyme (Revoke Wizard) sur la station LRA et de rechercher le titulaire du certificat. Ensuite, les certificats à révoquer seront sélectionnés. L'officier LRA pourra alors consulter une page avec tous les documents d'identité enregistrés pour un certificat. Il vérifiera l'identité du titulaire du certificat à l'aide de ces documents.

Une fois l'identification effectuée, les certificats sélectionnés seront révoqués. Leurs titulaires recevront automatiquement une confirmation de la révocation par courriel.

5.3.4.4 Clôture administrative

Le formulaire de révocation physique est archivé dans le dossier client. Lorsque celui-ci est géré par voie électronique, les exigences visées aux points 3.8 et 5.2.3.14 s'appliquent. La procédure de révocation est consignée dans le journal selon le point 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) ou de redéfinition des clés (Rekeying). Pour cela, la version la plus récente de l'assistant de renouvellement (Renewal Wizard) doit être installée sur l'ordinateur de l'utilisateur et l'espace mémoire disponible sur la carte à puce doit être suffisant. 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 (Renewal Wizard) sur le client de bureautique de l'utilisateur 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. Un nouveau certificat doit alors être établi par l'officier LRA. 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 suffit ensuite de 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 l'utilisateur et lance l'assistant de récupération de clé. Il insère la carte à puce de l'utilisateur dans un lecteur de carte libre et saisit le numéro de l'e-ticket. Les anciennes clés de chiffrement de l'utilisateur 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 de l'utilisateur. Dans des cas exceptionnels, il peut toutefois être nécessaire d'installer la ou les clés de chiffrement d'une personne sur la carte d'un autre utilisateur pour les raisons suivantes:

- le collaborateur ne travaille plus pour l'office,
- le collaborateur est absent pour cause de maladie de longue durée,
- le collaborateur est décédé.

Comme cette récupération permet de lire tous les courriels et documents chiffrés du titulaire du certificat (à condition que ces données chiffrées soient aussi en possession du détenteur des clés), chacun de ces cas nécessite une évaluation séparée. À cet effet, une demande détaillée et motivée doit être soumise au responsable PKI. La suite des opérations est alors définie individuellement et toujours en relation avec 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 auprès du responsable PKI ou 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. point 5.2.3), le client doit remplir le formulaire suivant: « Demande de certificats personnels de classe B à la Swiss Government PKI »

NON CLASSIFIÉ

Demande de certificats personnels de classe B à la Swiss Government PKI

Certificats avancés

V2.3, 20.09.2019

Ce formulaire permet de demander un certificat de classe B à la Swiss Government PKI. On opère une distinction entre les certificats standard (avec authentification, signature et chiffrement) et les certificats de fonction pour les comptes d'administrateur et de test (authentification seulement pour les comptes d'administrateur).

Vous avez besoin d'une carte d'identité ou d'un passeport valables pour votre identification auprès de votre centre d'enregistrement.

**Champs obligatoires*

Nom et prénom(s)*:	
N° de pièce d'identité*:	Valable jusqu'au*:
Unité d'organisation*:	
Type de certificat*: Certificat standard de classe B	
Adresse électronique*:	
Adresse professionnelle*:	
Lieu d'origine:	Date de naissance:
N° de carte à puce:	

Lieu et date*: **Signature*:**

_____ _____

Ce formulaire peut être téléchargé sur le site Internet de la Swiss Government PKI. Les clients sont libres de concevoir à cette fin un formulaire propre à leur organisation. Les données suivantes doivent au moins 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 de définition du NIP et de 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 l'exactitude des informations.

Les offices ont également la possibilité de 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 émissions et qu'elles soient archivées et puissent être auditées pendant 11 ans à compter de l'échéance du certificat (cf. points 5.2.3.14 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 nouveaux collaborateurs peuvent être annoncés à l'officier LRA par les services RH compétents au moyen des listes. Les données énumérées ci-dessus doivent alors être mentionnées pour chaque nouvelle arrivée.
Le formulaire «*Demande RIO en vue de l'émission de certificats de classe B*» est utilisé pour le processus «*Émission avec RIO*» (cf. point 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. En signant, 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 de classe B

Créé spécialement pour l'utilisateur final, le formulaire «Convention et conditions d'utilisation des certificats de classe B» [2] ne comprend que les informations les plus importantes. Des renseignements complets figurent dans les CP/CPS [1]. 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 se trouve le numéro de la carte à puce, si disponible. Ce numéro peut être utile en cas de problème avec la carte à puce (perte ou endommagement). Ce formulaire 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 le motif doivent y être indiqués. Dans ce 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. point 5.3.4.2 à ce sujet).

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 PKI. 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. Elle ne doit être ni remplie ni archivée pour chaque certificat établi.

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. Elle ne doit être ni remplie ni archivée pour chaque certificat établi.

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 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. Elle ne doit être ni remplie ni archivée pour chaque certificat établi.

7 Procédure d'intervention par paliers

En cas d'incertitudes ou de questions ou si vous avez 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 PKI de l'OFIT.

8 Propositions de modification

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

Responsable du service Swiss Government PKI
Office fédéral de l'informatique et de la télécommunication
Monbijoustrasse 74
CH-3003 Berne
Adresse électronique: pki-info@bit.admin.ch

Annexes

Annexe A: Listes de contrôle des processus – classe B

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF

Office fédéral de l'informatique et de la télécommunication OFIT
Exploitation
Exploitation des services frontaux
PKI

Liste de contrôle: émission de certificats de classe B

Processus de classe B «Émission sans RIO» (point 5.2.3 des directives d'enregistrement)

V2.1, 20.09.2019

N°	Description	Référence DE [1]
Préparation pour l'émission des certificats		
1.	Contrôler la demande:	
	a) Le requérant est-il enregistré dans Admin Directory? Avec son nom correct, y c. suffixe et adresse électronique?	5.2.3.1
	b) Le requérant est-il autorisé à obtenir un certificat de la classe B? Se trouve-t-il dans la branche de l'Admin Directory pour laquelle l'officier LRA est compétent?	5.2.1
	c) L'adresse électronique figurant dans la demande concorde-t-elle avec l'inscription dans Admin Directory?	5.2.3.2
	d) Les indications figurant dans la demande sont-elles complètes et plausibles?	5.2.3.2
2.	Fixer un rendez-vous pour l'établissement du certificat via l'adresse électronique indiquée par le requérant. Indiquer que seuls le passeport ou la carte d'identité sont acceptés comme moyens d'identification. Il est également utile de demander au requérant de se préparer au choix du NIP et de la phrase de révocation.	5.2.3.3
3.	Préparer la carte à puce: une initialisation distincte est nécessaire uniquement lorsqu'un logiciel tiers est utilisé pour gérer les PUK. Toutes les autres cartes ont déjà été préparées lors du processus correspondant ou seront d'abord formatées par l'assistant d'enregistrement (Walk-in Wizard) lors du traitement.	5.2.3.6
Émission des certificats		
4.	Contrôler l'identité	5.2.3.5
	a) Type de la pièce d'identité: s'agit-il d'un passeport ou d'une carte d'identité? Ou le requérant peut-il être identifié avec une autre pièce d'identité en vertu d'une disposition d'exception? La pièce d'identité est-elle authentique (vérifier au moins quatre caractéristiques de sécurité)?	

[1] Directives d'enregistrement de la classe B de la Swiss Government PKI

	b) La pièce d'identité est-elle encore en cours de validité?	
	c) Les indications de la demande concordent-elles avec celles de la pièce d'identité et d'Admin Directory, en particulier le nom et le prénom du requérant?	
	d) Comparer le visage du requérant avec la photo de la pièce d'identité. S'agit-il bien de la même personne?	
5.	Numériser et enregistrer la pièce d'identité et les éventuels autres documents requis.	5.2.3.7
6.	Informer le requérant sur le choix du NIP et de la phrase de révocation *(peut déjà figurer dans le courriel d'invitation).*	5.2.3.8
7.	Émettre la carte à puce à l'aide de l'assistant d'enregistrement (Walk-In Wizard). L'utilisateur doit définir lui-même le NIP et la phrase de révocation.	5.2.3.9
8.	Informer le requérant de ses obligations en vertu des documents «*Convention et conditions d'utilisation des certificats de classe B*» et «*Directives relatives aux certificats de classe B*» et discuter avec le client.	5.2.3.10
9.	Joindre le formulaire «*Confirmation de réception de la carte à puce et directives d'utilisation*» aux documents signés (facultatif) et faire signer une copie de la convention d'utilisation.	5.2.3.10
10.	La signature sur le formulaire «*Convention et conditions d'utilisation des certificats de classe B*» concorde-t-elle avec celle figurant sur la pièce d'identité?	
11.	Remettre au requérant la carte à puce, la pièce d'identité, d'autres documents éventuels et l'exemplaire non signé des documents «*Convention et conditions d'utilisation des certificats de classe B*» et «*Directives relatives aux certificats de classe B*».	5.2.3.11
12.	Remplir le journal.	5.2.3.12
13.	Supprimer le fichier de la pièce d'identité créé à l'étape 5 ainsi que les courriels éventuellement utilisés pour l'envoyer.	5.2.3.13
14.	Classer l'exemplaire signé du formulaire «*Convention et conditions d'utilisation des certificats de classe B*» et, si elle a été faite sur papier, la demande avec les empreintes digitales des certificats dans le dossier client et éventuellement dans les archives électroniques.	5.2.3.14

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF

Office fédéral de l'informatique et de la télécommunication OFIT
Exploitation
Exploitation des services frontaux
PKI

Liste de contrôle: émission de certificats de classe B avec RIO

Processus de classe B «Émission avec RIO», points à vérifier par l'officier LRA (point 5.2.4 des directives d'enregistrement)

V2.1, 20.09.2019

Description	Référence DE [1]
Établissement de la demande	
Le requérant/RH/supérieur hiérarchique remplit la première partie du formulaire «Demande de certificats via RIO et Wizard» et informe le RIO (et le client) de la nouvelle émission de certificats: https://www.bit.admin.ch/bit/fr/home/subsites/generalites-concernant-la-swiss-government-pki/types-de-certificats/classe-b--standard-/formulaires.html	5.2.4.1
Identification du requérant et transmission de la demande par le RIO	
Le RIO procède selon la liste de contrôle pour RIO, y documente les étapes effectuées et transmet les documents à l'officier LRA. Il est important à cet égard que le numéro de série de la carte à puce soit inscrit sur le formulaire de demande et que les copies/documents numérisés soient complets et lisibles.	5.2.4.2
Approbation par l'officier LRA de l'émission des certificats	
Examen de la demande:	5.2.4.3
a) Tous les documents requis sont-ils disponibles (formulaire de demande [avec le numéro de série de la carte], liste de contrôle, copie signée du formulaire «Convention et conditions d'utilisation des certificats de classe B», le cas échéant les autres copies nécessaires en vertu d'une disposition d'exception)? **En cas de transmission électronique**: tous les documents ont-ils été transmis sous forme chiffrée?	
b) La confirmation de la demande est-elle signée par un RIO autorisé? **En cas de transmission électronique**: la signature électronique du RIO est-elle valable?	
c) Numériser et enregistrer la pièce d'identité et les éventuels autres documents requis. **En cas de transmission électronique**: enregistrement de la confirmation signée de la demande	
d) Comparer les données dans le système avec les indications figurant sur le formulaire de demande: l'utilisateur est-il saisi correctement dans Admin Directory?	
Émission des certificats grâce à l'assistant d'enregistrement (Walk-In Wizard): utiliser la «RIO Policy»	

[1] Directives d'enregistrement de la classe B de la Swiss Government PKI

e) Ajouter les documents numérisés. La demande validée est jointe à un ticket, puis transférée à la CA pour certification. Le numéro du ticket est consigné dans un document de déblocage (Unseal Document) au format PDF.	
f) Envoyer le document de déblocage avec le code d'activation à l'adresse privée du client (autre solution: les données d'activation peuvent être adressées au RIO dans un courriel chiffré et signé).	
g) Classer les documents mentionnés au point a) (forme papier) dans le dossier client et, en cas de **transmission électronique**, dans le dossier client électronique.	
h) Remplir le journal.	5.2.4.3, 3.7
Récupération du certificat par le requérant	
1) Ouvrir l'assistant de déblocage de smartcard (Token Unseal Wizard) chez le RIO ou un collègue possédant un deuxième lecteur de carte.	
2) Insérer la carte dans le lecteur (le système la reconnaît automatiquement).	
3) À l'invitation de l'assistant, saisir le code d'activation → Les certificats sont enregistrés.	
4) Saisir ensuite le NIP et la phrase de révocation → La carte peut désormais être utilisée.	

Liste de contrôle: révocation de certificats de classe B

Processus de classe B «Révocation d'un certificat» (point 5.3 des directives d'enregistrement)

V2.1, 20.09.2019

N°	Description	Référence DE [1]
Contrôler la demande		
1.	Contrôler la plausibilité de la demande.	5.3.4.1
2.	Remplir si nécessaire le formulaire de révocation si cela n'a pas déjà été fait par le requérant.	5.3.4.2
Révoquer le certificat		
3.	Chercher le certificat correspondant dans l'assistant de révocation (Revoke Wizard).	5.3.4.3
4.	Identifier le titulaire du certificat à l'aide des documents d'identité enregistrés.	
5.	Révoquer le certificat.	
Clore le processus		
6.	Archiver le formulaire de révocation (s'il est disponible en fonction de l'application/du processus choisi)	5.3.4.4
7.	Remplir le journal.	5.3.4.4, 3.7

[1] Directives d'enregistrement de la classe B de la Swiss Government PKI

Liste de contrôle RIO

V2.1, 20.09.2019

N°	Description de la tâche	Résultat (OK / NOK)	**Date**
1	Examiner la demande et en contrôler la plausibilité (cette personne est autorisée à recevoir des certificats de classe B de la Swiss Government PKI et est enregistrée dans Admin Directory).		
2	Contrôler l'identité en comparant la pièce d'identité valable avec le formulaire de demande (seuls sont admis une carte d'identité ou un passeport en cours de validité).		
	Nom: _____		
	Type de pièce d'identité selon le formulaire de demande (seuls sont admis une carte d'identité ou un passeport en cours de validité) Numéro de série du document: _____ Validité de la pièce d'identité: _____	☐ Carte d'identité ☐ Passeport ☐ Autres _____	
	Comparer le visage du requérant avec la photo de la pièce d'identité.		
3	Remettre la carte à puce préenregistrée (ou de type préparé); informer le client de son obligation de veiller à ce qu'aucune autre personne n'ait accès à sa carte. Numéro de série de la carte à puce: _____		
4	Remplir la partie 2 du formulaire de demande, y c. les signatures.		
5	Expliquer au client le contenu des documents «Convention et conditions d'utilisation des certificats de classe B» et «Directives relatives aux certificats de classe B de la Swiss Government PKI».		
6	Remettre au client les documents «Convention et conditions d'utilisation des certificats de classe B» et «Directives relatives aux certificats de classe B de la Swiss Government PKI»; lui faire signer une copie de la convention d'utilisation et la récupérer.		
7	Copier la pièce d'identité (des deux côtés) au verso de la demande. Copier tous les documents.		
8	Signer toutes les pages comprenant une copie et faire signer le client.		
9	Signer la liste de contrôle.		
10	Envoyer les documents à l'officier LRA («Convention et conditions d'utilisation des certificats de classe B», le formulaire de demande dûment complété, la présente liste de contrôle). En cas de transmission électronique: envoyer à l'officier LRA compétent, par courriel chiffré, les documents signés.		

Nom / prénom du RIO:	Unité d'organisation:	Lieu et date:

Signature du RIO: _____

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF

Office fédéral de l'informatique et de la télécommunication OFIT
Exploitation
Exploitation des services frontaux
PKI

Annexe B: Formulaires pour certificats de classe B

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF

Office fédéral de l'informatique et de la télécommunication OFIT
Exploitation
Exploitation des services frontaux
PKI

NON CLASSIFIÉ

Demande de certificats personnels de classe B à la Swiss Government PKI

Certificats avancés

V2.3, 20.09.2019

Ce formulaire permet de demander un certificat de classe B à la Swiss Government PKI. On opère une distinction entre les certificats standard (avec authentification, signature et chiffrement) et les certificats de fonction pour les comptes d'administrateur et de test (authentification seulement pour les comptes d'administrateur).

Vous avez besoin d'une carte d'identité ou d'un passeport valables pour votre identification auprès de votre centre d'enregistrement.

**Champs obligatoires*

Nom et prénom(s)*:	
N° de pièce d'identité*:	Valable jusqu'au*:
Unité d'organisation*:	
Type de certificat*: Certificat standard de classe B	
Adresse électronique*:	
Adresse professionnelle*:	
Lieu d'origine:	Date de naissance:
N° de carte à puce:	

Lieu et date*: **Signature*:**

_____ _____

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF
Office fédéral de l'informatique et de la télécommunication OFIT
Swiss Government PKI

NON CLASSIFIÉ

Classe B: formulaire supplémentaire pour les requérants titulaires d'un livret F

V1.1, 20.09.2019

Ce formulaire fait partie intégrante de la demande de certificat de classe B de la Swiss Government PKI lorsque le requérant ne possède aucune pièce d'identité en cours de validité, hormis un «livret F».

Il doit être remis avec une demande de certificat de classe B de la Swiss Government PKI qui est dûment complétée et munie d'une signature valable.

Le DSIO compétent doit signer le présent formulaire. Il confirme ainsi avoir pris acte que l'identité du requérant ne peut pas être établie formellement sur la base d'un «livret F» et que la SG PKI décline dès lors toute responsabilité en la matière.

Nom:	Prénom:
N° de pièce d'identité:	
Unité d'organisation:	
Type de certificat: Certificat standard ☐ Certificat de fonction: Administrateur ☐ Test ☐	
Adresse électronique[1]:	
Adresse professionnelle:	
Lieu d'origine:	Date de naissance:
☐ Collaborateur interne ☐ Collaborateur externe	

[1] Adresse électronique du titulaire du compte s'il s'agit d'un «certificat de fonction pour administrateur».

DSIO:

Nom, prénom: _____
(en lettres majuscules)

Lieu, date: _____

Signature: _____

Requérant:

N° pièce d'identité: _____

Lieu, date: _____

Signature: _____

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

Demande RIO en vue de l'émission de certificats de classe B

Formulaire pour communiquer les informations du requérant à l'officier LRA

V1.1, 20.09.2019

1 Données du requérant (à remplir par cette personne et à remettre au RIO)

Par la présente, le requérant commande une carte à puce de type préparé pour l'émission de certificats de classe B de la Swiss Government PKI:

Nom, prénom:

Département, canton, office:

Adresse électronique:

Numéro de téléphone:

Lieu, date: Signature: _____

2 Identification et remise de la carte (à remplir conjointement par le RIO et le requérant, et à remettre à l'officier LRA)

Le requérant reçoit du RIO une carte à puce de type préparé. Après que l'officier LRA a approuvé la demande, le requérant peut débloquer sa carte à puce à l'aide du code de sécurité qui lui a été communiqué ou envoyé.

Le RIO transmet au requérant la carte à puce avec
les numéros d'identification suivants: **numéro de série** (obligatoire):_____
numéro de carte ou LegicID (optionnel): _____

Le RIO et le requérant confirment, par leur signature, qu'il y a eu rencontre personnelle, remise de la carte à puce avec le numéro de série susmentionné et procédure d'identification à l'aide d'une pièce d'identité valable:

RIO:	**Requérant:**
Nom, prénom: _____ (en lettres majuscules)	N° pièce d'identité: _____
Lieu, date: _____	Lieu, date: _____
Signature: _____	Signature: _____

3 Convention et conditions d'utilisation

Le RIO s'assure que le requérant a compris le contenu de la convention et des conditions d'utilisation et qu'il en a reçu une copie. Un deuxième exemplaire doit être signé par le requérant et remis par le RIO à l'officier LRA, accompagné du présent document dûment rempli et d'une copie de la pièce d'identité.

4 Copie de la pièce d'identité

Une copie de la pièce d'identité valable du requérant doit figurer au dos de ce document. Les cartes d'identité doivent être obligatoirement photocopiées des deux côtés. Les copies de passeports doivent toujours inclure les pages comprenant la photo, la signature et la date de validité. Le verso de ce document ainsi que les pages requises supplémentaires doivent être complétés par les deux parties avec le lieu, la date et la signature. Le dos de ce document sert de support aux copies.

[Déposer ici une copie des documents d'identité]

RIO:

Lieu, date: _____

Signature: _____

Requérant:

Lieu, date: _____

Signature: _____

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF
Office fédéral de l'informatique et de la télécommunication OFIT
Swiss Government PKI

NON CLASSIFIÉ

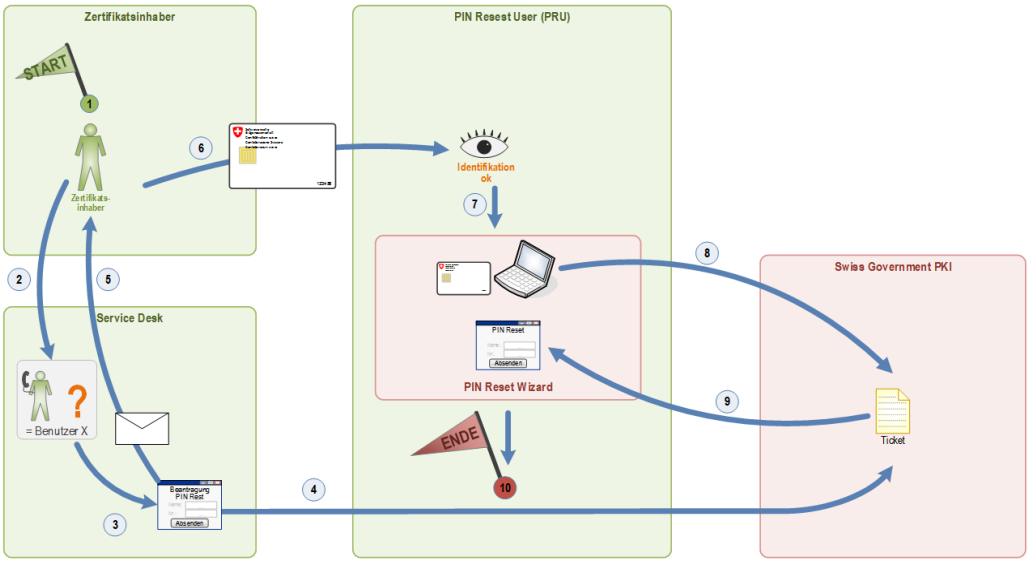
Formulaire de demande de réinitialisation du NIP pour les superutilisateurs et le Service Desk

Autorisation d'établir un ticket en ligne

V1.1, 25.10.2019

Ce formulaire permet de valider l'autorisation d'établir un ticket en ligne en vue de réinitialiser le NIP d'un utilisateur de carte à puce. Il est à compléter uniquement pour les collaborateurs du Service Desk ou les superutilisateurs. L'autorisation d'établir un ticket n'est que la première étape pour réinitialiser le NIP des cartes à puce préparées. L'utilisateur concerné doit dans un deuxième temps activer sa carte à puce sur l'ordinateur d'un collaborateur en entrant son nouveau NIP. (Voir la notice pour les PIN Reset User):
https://www.bit.admin.ch/bit/fr/home/subsites/generalites-concernant-la-swiss-government-pki.html

Processus de réinitialisation du NIP:



Données de l'auteur de la demande:

Nom, prénom, suffixe:

Département / canton:

Office:

Fonction:

Adresse électronique:

Numéro de téléphone:

No. série cert. d'authentification

Date:

Signature numérique: _____

Autorisation (avec indication de la date):

Signature numérique du resp. de l'org.:

_____

Signature numérique du directeur de l'office:

_____

Signature numérique du SecOff. SG PKI:

_____

Retrait d'autorisation:

Veuillez retirer à la personne susmentionnée (appelée *auteur de la demande*) l'autorisation d'établir un ticket de demande de réinitialisation du NIP. ☐

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF
Office fédéral de l'informatique et de la télécommunication OFIT
Swiss Government PKI

NON CLASSIFIÉ

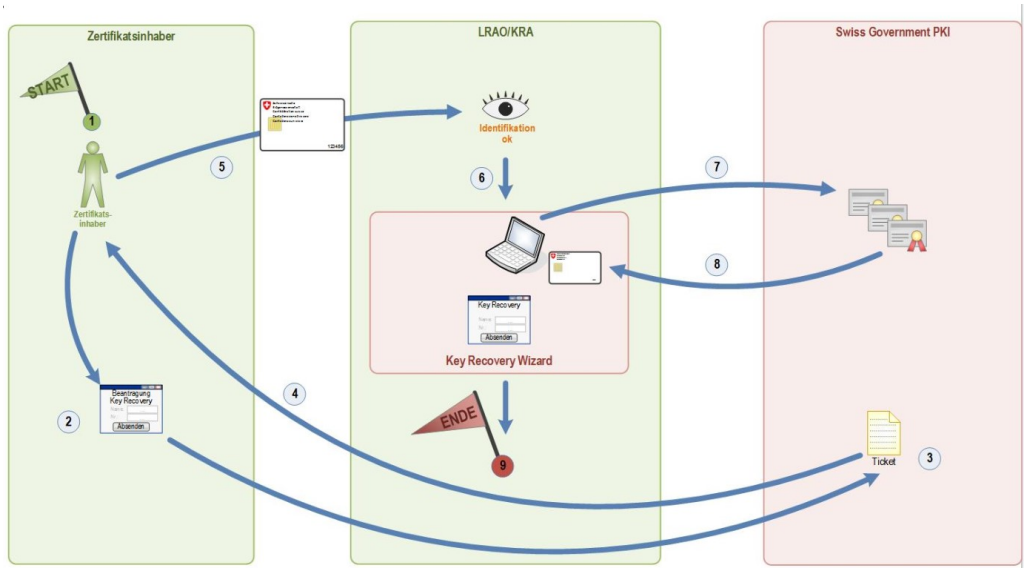
Formulaire de demande concernant un Key Recovery Agent (KRA)

Autorisations pour l'assistant de récupération des clés (Key Recovery Wizard)

V1.1, 25.10.2019

Le présent formulaire permet de nommer un RIO, un collaborateur d'un service d'assistance informatique ou un superutilisateur en tant qu'agent habilité à la récupération des clés (Key Recovery Agent, KRA) et de lui accorder les autorisations correspondantes. Celles-ci sont nécessaires pour la deuxième partie du processus de récupération des clés. L'utilisateur qui a besoin de récupérer ses clés ouvre dans son navigateur la page ad hoc (https://keyrecovery.pki.admin.ch/KeyRecoveryRequest/) et y crée un **e-ticket** dans le système PKI centralisé. Lorsque le titulaire du certificat a remis au KRA son e-ticket, le KRA lance l'assistant de récupération des clés et saisit le numéro de l'e-ticket. L'assistant affiche tous les certificats de cryptage qui ont déjà été délivrés au titulaire du certificat. Celui-ci indique au KRA quelles clés il souhaite récupérer. Après que le titulaire du certificat a saisi son NIP, l'assistant inscrit les clés de cryptage sélectionnées sur la carte à puce.

Processus de récupération des clés:



Données de l'auteur de la demande:

Nom, prénom, suffixe:

Département / canton:

Office:

Fonction:

Adresse électronique:

Numéro de téléphone:

No. série cert. d'authentification

Date:

Signature numérique: _____

Autorisation (avec indication de la date):

Signature numérique du resp. de l'org.:

_____

Signature numérique du directeur de l'office:

_____

Signature numérique du SecOff. SG PKI:

_____

Retrait d'autorisation:

Veuillez retirer à la personne susmentionnée (appelée *auteur de la demande*) les autorisations d'agent habilité à la récupération des clés (Key Recovery Agent, KRA). ☐

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF

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

NON CLASSIFIÉ

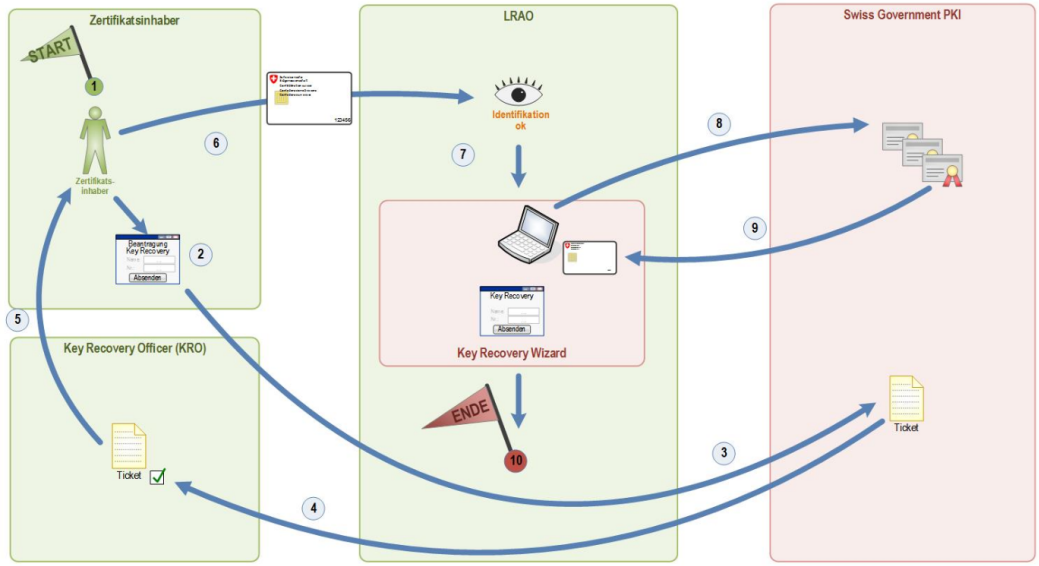
Formulaire de demande concernant un Key Recovery Officer (KRO)

Autorisations pour valider les demandes de récupération des clés

V1.1, 25.10.2019

Le présent formulaire permet de nommer un RIO, un collaborateur d'un service d'assistance informatique ou un superutilisateur en tant que Key Recovery Officer (KRO) et de lui accorder les autorisations correspondantes. Celles-ci sont nécessaires pour la deuxième partie du processus de récupération des clés. L'utilisateur qui a besoin de récupérer ses clés ouvre dans son navigateur la page ad hoc (https://keyrecovery.pki.admin.ch/KeyRecoveryRequest/) et y crée un **e-ticket** dans le système PKI centralisé. Le KRO est ensuite chargé de vérifier la demande et de la valider le cas échéant, avant que le titulaire du certificat ne se rende avec son **e-ticket** auprès de l'officier LRA ou du KRA, qui lancera alors l'assistant de récupération des clés et saisira le numéro de l'**e-ticket**. L'assistant affiche tous les certificats de cryptage qui ont déjà été délivrés au titulaire du certificat. Celui-ci indique à l'officier LRA ou au KRA quelles clés il souhaite récupérer. Après que le titulaire du certificat a saisi son NIP, l'assistant inscrit les clés de cryptage sur la carte à puce.

Processus de récupération des clés (avec Key Recovery Officer):



Données de l'auteur de la demande:

Nom, prénom, suffixe:

Département / canton:

Office:

Fonction:

Adresse électronique:

Numéro de téléphone:

No. série cert. d'authentification

Date:

Signature numérique: _____

Autorisation (avec indication de la date):

Signature numérique du resp. de l'org.:

_____

Signature numérique du directeur de l'office:

_____

Signature numérique du SecOff. SG PKI:

_____

Retrait d'autorisation:

Veuillez retirer à la personne susmentionnée (appelée *auteur de la demande*) les autorisations de Key Recovery Officer (KRO). ☐

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF
Office fédéral de l'informatique et de la télécommunication OFIT
Swiss Government PKI

NON CLASSIFIÉ

Demande de révocation des certificats de classe B de la Swiss Government PKI

V2.4, 20.09.2019

Requérant:			
☐ **Titulaire de certificat**	☐ **Supérieur**	☐ **RH**	☐ **DSIO**
☐ **Responsable PKI**	☐ **Officier LRA**	☐ **Officier de sécurité PKI**	
Nom:		Prénom:	
Unité d'organisation:			

Titulaire du certificat (*à ne remplir que si le titulaire n'est pas le requérant):		
Nom*:	Prénom*:	Suffixe*:
Unité d'organisation*:		
Type de certificat: ☐ Certificat standard ☐ Certificat de fonction d'administrateur ☐ Certificat de fonction pour des tests		
☐ Collaborateur interne ☐ Collaborateur externe ☐ Liste de révocation		

Motifs de la révocation:	
☐ Perte de la carte à puce	☐ Carte à puce défectueuse
☐ Soupçon de divulgation	☐ Départ
☐ Émission erronée	☐ Soupçon d'abus
☐ Autres	

Révoqué le:	
Officier LRA exécutant (nom, prénom):	Signature: _____

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

Classe B: journal de l'officier LRA de la Swiss Government PKI

V2.1, 20.09.2019

Numéro d'ordre #	Date	Client	Activité: CS: certificat standard, CFA: certificat d'administrateur, CFT: certificat de test, E: émission, R: révocation, K: récupération des clés	Numéro de série de la carte à puce	Carte à puce retirée? OUI / NON	Visa de l'officier LRA

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF
Office fédéral de l'informatique et de la télécommunication OFIT
Swiss Government PKI

NON CLASSIFIÉ

Classe B: demande d'autorisation pour officier LRA

V4.5, 20.09.2019

☐ **Nouvel officier LRA** → Sections A et B
☐ **Renouvellement LRAO** → Sections A et B
☐ **Mutation des droits** → Section B
☐ **Révocation du certificat LRAO** → Section C

Section A) Les conditions suivantes doivent être remplies pour que la demande puisse être traitée:

☐ Formation suivie et test réussi: joindre une copie de l'attestation et une confirmation de la réussite du test
☐ Entrée disponible dans les pages jaunes de l'annuaire AdminDir
☐ Informations de l'officier LRA à la *section B* remplies correctement et de façon complète

Section B) Informations sur l'officier LRA et sur les autorisations d'émission:

Émission classe B pour AF: ☐ L'adresse électronique se termine par «admin.ch» (prestaged/Enhanced CA02)
☐ L'adresse électronique ne se termine *pas* par «admin.ch» (prestaged/Enhanced CA01)

Émission classe B pour externes (non AF): ☐ Prestaged (Enhanced CA01)
☐ *Non* prestaged/standard (Enhanced CA01)

Informations sur l'officier LRA (conformes aux données dans l'annuaire AdminDir, *= obligatoire)			
Nom*:		Prénom*:	
Suffixe*:		Département*:	
Office*:		Tél.*:	
Adresse électronique*:			
Adresse (rue, NPA, localité)*:			
Autorisations d'émission pour (département/office)*:			☐ Nouveau ☐ Retirer
N° de série du certificat d'authentification personnel de classe B			
Autorisations pour les certificats de **comptes d'administrateur** (comptes A) au niveau départemental	☐ Nouveau ☐ Retirer pour le département: DFF		

Section C) Les conditions suivantes doivent être remplies pour que la demande soit traitée:

Date d'exécution de la révocation:

L'officier LRA a-t-il un successeur? ☐ Non ☐ Oui, nom:

☐ Les informations sur l'officier LRA sont dûment indiquées dans la ***section B***.

L'officier LRA encore actif s'engage à transmettre les dossiers clients et le journal à son successeur. Il est prié de renvoyer sa carte à puce d'officier LRA.

Conditions d'utilisation générales pour l'officier LRA

Déclaration de confidentialité

Le requérant s'engage, par sa signature, à traiter de manière confidentielle sa carte à puce et son mot de passe; il s'engage également à ne pas transmettre les informations personnelles qui lui ont été communiquées dans le cadre de son travail en tant qu'officier LRA à des tiers, mais uniquement à des collaborateurs internes qui ont impérativement besoin d'accéder à ces informations pour accomplir leurs tâches. Les collaborateurs assumant un rôle d'officier LRA sont tenus de

respecter le secret de fonction, si cela n'est pas déjà imposé par leur contrat de travail. Aucune copie partielle ou complète des données et des informations à traiter ne doit être effectuée.

L'officier LRA est tenu de demander la révocation du certificat lorsqu'il quitte ses fonctions.
La présente déclaration reste valable après le départ de l'officier LRA.

Le certificat d'officier LRA est soumis au document «Convention et conditions d'utilisation pour officiers LRA de la SG PKI», aux «Directives relatives au certificat LRAO de la Swiss Government PKI» (pages suivantes) et aux «Directives d'enregistrement de la classe B de la Swiss Government PKI». Par sa signature, le futur officier LRA confirme qu'il a lu, compris et accepté toutes les règles et procédures contenues dans ces documents conformément aux CP/CPS applicables de la SG Root CA I et s'engage à les respecter pleinement. Le futur officier LRA confirme par sa signature qu'il accepte l'émission d'une nouvelle carte à puce d'officier LRA personnelle à utiliser dans le cadre de ses activités d'officier LRA.

Requérant (prénom, nom)	**Date:** **Signature:**

Contrôle de la fiabilité

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

- Exécution du contrôle de sécurité prévu à l'art. 10 de l'ordonnance sur les contrôles de sécurité relatifs aux personnes (OCSP; RS *120.4*) au service CSP du DDPS

  et/ou

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

Confirmation

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

Signatures

Si les chemins d'accès à l'autorisation sont demandés pour plusieurs offices, les personnes autorisées à signer de chacun des offices concernés doivent fournir leur signature. Pour ce faire, veuillez utiliser les listes que vous trouverez dans les formulaires pour la classe B sous www.pki.admin.ch.

Les personnes autorisées à signer sont:

- au **niveau des offices**: les DSIO, les responsables PKI des cantons ou des corps de police, les préposés à la sécurité des offices cantonaux, ainsi que le conseil de gestion de la SG PKI;
- au **niveau du département**: les DSID, les responsables PKI des cantons ou des polices cantonales, ainsi que les préposés à la sécurité des cantons et de la police cantonale

Personne de l'office autorisée à signer (prénom, nom et fonction)	**Date:** **Signature:**

L'autorisation pour l'émission de certificats pour les comptes d'administrateur (uniquement internes à l'administration fédérale) nécessite la signature du **DSID** (*l'autorisation est toujours valable pour l'ensemble du département!*). Si une autorisation est demandée pour plusieurs départements, le champ ci-dessous doit être signé par les DSID de tous les départements concernés par la demande. Pour ce faire, veuillez utiliser les listes que vous trouverez dans les formulaires pour la classe B sous www.pki.admin.ch.

Personne du département autorisée à signer (prénom, nom) Département ou canton	**Date:** **Signature:**

NON CLASSIFIÉ

Directives relatives au certificat LRAO de la Swiss Government PKI

Explications concernant l'obtention et l'utilisation du certificat LRAO des classes A et B de la Swiss Government PKI

V1.0, 28.08.2018

1 But du certificat LRAO

But

Les certificats des classes A et B sont définis dans le cadre du modèle de marché applicable au service standard Gestion des identités et des accès (SD005). Les officiers de l'autorité d'enregistrement locale (officiers LRA) sont chargés de l'émission des certificats des classes A et B. Le certificat LRAO peut être utilisé aux fins suivantes:

- émission, révocation et gestion des certificats des classes A et B de la SG PKI.

Les mécanismes étendus de vérification et de sécurité qui sont appliqués lors du processus d'émission des certificats des classes A et B permettent de déterminer l'identité du titulaire de certificat avec un niveau de sécurité élevé. Ces certificats sont toujours délivrés en personne et uniquement après une identification du titulaire à l'aide d'une pièce d'identité valable autorisant l'entrée en Suisse.

But exclu

Le certificat LRAO poursuit uniquement les fins mentionnées ci-dessus et ne fournit aucune autre information, assurance ou garantie. Plus particulièrement, il ne garantit pas que le titulaire l'utilise de manière correcte et légale.
Par ailleurs, le certificat LRAO ne garantit pas que le titulaire mentionné sur le certificat:

- participe activement aux activités concernées;
- respecte les dispositions légales en vigueur;
- agit de manière sérieuse dans le cadre des affaires.

2 Qualité du certificat LRAO

La SG PKI respecte les processus définis dans les directives d'enregistrement, qui fixent les mesures nécessaires et raisonnablement exigibles pour confirmer les faits suivants lors de la délivrance initiale d'un certificat LRAO:

- **Existence juridiquement valable:** le titulaire mentionné sur le certificat LRAO existe en tant que personne physique et est inscrit personnellement dans Admin Directory.
- **Identité:** le nom du titulaire mentionné sur le certificat LRAO correspond au nom figurant dans Admin Directory et sur la pièce d'identité en cours de validité.
- **Autorisation:** le titulaire mentionné dans le certificat LRAO a été autorisé à obtenir le certificat par la personne de son office qui est habilitée à signer.
- **Exactitude des données:** toutes les données et informations contenues sur le certificat sont correctes.
- **Convention et conditions d'utilisation:** le titulaire mentionné sur le certificat LRAO a lu et compris les droits et obligations décrits dans le document «Convention et conditions d'utilisation pour officiers LRA de la SG PKI», et les a acceptés par sa signature sur le formulaire de demande de certificat d'officier LRA de la SG PKI. La SG PKI a répondu clairement aux questions du titulaire.

- **Statut:** la SG PKI publie en ligne le statut du certificat et les informations concernant sa validité ou sa révocation.
- **Révocation:** la SG PKI peut révoquer avec effet immédiat le certificat LRAO pour les motifs mentionnés dans le document «Convention et conditions d'utilisation pour officiers LRA de la SG PKI».

3 Politiques

Toutes les dispositions légales, politiques (y c. les CP/CPS de la SG Root CA I) et directives d'enregistrement de certificats de la SG PKI applicables, ainsi que le document «Convention et conditions d'utilisation pour officiers LRA de la SG PKI» et les présentes directives sont accessibles en ligne sur le site Internet de la SG PKI: www.pki.admin.ch.

En signant le formulaire «Classe B: demande d'autorisation pour officier LRA», le futur LRAO s'engage à respecter les directives et la législation en vigueur et à exécuter son travail en conséquence. Il s'agit notamment des documents suivants:

- les CP/CPS de la SG Root CA I: («Certificate Policy and Certification Practice Statement of the Swiss Government Root CA I», en particulier les obligations énoncées aux points 5.3.1 et 5.5.2);
- les «Directives d'enregistrement de la classe B de la Swiss Government PKI»;
- le document «Convention et conditions d'utilisation pour officiers LRA de la SG PKI»;
- les «Directives relatives au certificat LRAO de la Swiss Government PKI» (le présent document).

Contenu

Le certificat LRAO de la SG PKI contient des informations concernant:

- l'éditeur et l'autorité de certification (CA) qui émet le certificat;
- l'autorité de certification racine de la CA qui émet le certificat;
- la politique appliquée;
- la date d'émission et d'expiration du certificat;
- le numéro de série du certificat;
- le but d'utilisation du certificat;
- la liste de révocation des certificats et l'OCSP (*online certificate status protocol*);
- les auditeurs de la CA;
- le titulaire du certificat d'après l'inscription dans Admin Directory au moment de la délivrance initiale:
    1) nom commun du titulaire
    2) adresse électronique
    3) nom d'utilisateur principal

Validité

Le certificat LRAO de la SG PKI est valable au maximum trois ans. Une fois la période de validité expirée, le certificat LRAO doit être demandé à nouveau par l'officier LRA à la SG PKI selon le processus d'émission initial et délivré par la SG PKI.

4 Obtention du certificat LRAO

Obtention

Les documents et inscriptions suivants sont requis pour obtenir un certificat LRAO de la SG PKI:

- une pièce d'identité valable autorisant l'entrée en Suisse (carte d'identité, passeport) établie au nom du requérant; le responsable du cours vérifie l'identité pendant la formation obligatoire LRAO;
- une inscription du requérant dans Admin Directory, comprenant le nom, le prénom (comme indiqués sur la pièce d'identité), une adresse électronique valable et éventuellement un nom d'utilisateur principal;
- une attestation confirmant la participation effective à la formation obligatoire LRAO et la réussite à l'examen;
- un formulaire de demande rempli et signé (électroniquement) pour le certificat d'officier LRA de la Swiss Government PKI, dans lequel
    1) le futur LRAO accepte par sa signature
        - la déclaration de confidentialité,

- le document «Convention et conditions d'utilisation pour officiers LRA de la SG PKI»,
- les présentes directives,

et commande la carte à puce LRAO;

2) la personne autorisée à signer de l'autorité de recrutement confirme par sa signature la fiabilité du futur officier LRA selon les exigences du formulaire de demande sous le chapitre «Contrôle de la fiabilité».

Identification

Afin d'être identifié, le requérant doit fournir une pièce d'identité dont la validité, la conformité et l'authenticité sont contrôlées pendant la formation LRAO. Les formateurs de la SG PKI sont également tenus de valider la photo du document de la personne présente et participant à la formation. En outre, la plausibilité de toute demande d'émission de certificat personnel doit être vérifiée par la SG PKI (le requérant travaille bien au sein de l'unité organisationnelle figurant dans Admin Directory et a besoin du certificat pour son travail; le requérant est autorisé à demander un certificat).

Caractère contraignant

La demande doit être approuvée par les autorités compétentes. Les présentes directives et le document «Convention et conditions d'utilisation pour officiers LRA de la SG PKI» doivent être compris par le candidat ou la candidate et acceptés par la signature (numérique) du formulaire de demande pour LRAO.

5 Protection de la clé privée et du certificat

Transmissibilité

Le certificat LRAO est toujours personnel et ne peut pas être transmis. Les données personnelles relatives à leur titulaire sont enregistrées tant sur les certificats qu'auprès de la SG PKI.

NIP et PUK

Le NIP doit être choisi indépendamment de tout autre mot de passe et ne doit pas être accessible à des tiers. Il ne doit pas être modifié régulièrement sauf s'il y a lieu de croire qu'un tiers en a eu connaissance.

Le certificat (ou son support: carte à puce, clé USB, etc.) doit être sécurisé par un NIP d'au moins huit caractères. Les NIP purement numériques et les NIP mélangés sont autorisés. Ce code ne doit jamais être communiqué à un tiers afin d'éviter tout emploi abusif de l'identité électronique du titulaire du certificat.

La PUK de la carte à puce doit comprendre au moins huit caractères selon les règles mentionnées ci-dessus.

Obligation de déclaration

Toute perte de la carte à puce doit être immédiatement signalée par le LRAO à la SG PKI. Le certificat concerné est ensuite bloqué (révoqué) et cette action est inscrite sur une liste de blocage électronique et publique. Même si la carte à puce est retrouvée par la suite, le certificat reste bloqué et invalide. Un nouveau certificat LRAO peut être demandé à la SG PKI immédiatement après le blocage. Son processus d'émission est identique à celui du certificat initial.

Tout changement d'organisation, de nom (p. ex. en raison d'un mariage) ou d'adresse électronique nécessite l'émission d'un nouveau certificat (processus identique à celui de la délivrance initiale).

6 Révocation

Toute révocation doit faire l'objet d'une demande auprès de la SG PKI. Un formulaire destiné aux personnes dûment autorisées (cf. liste exhaustive ci-dessous) est disponible à cet effet sur le site Internet de la SG PKI www.pki.admin.ch. Si la révocation est demandée par téléphone, la SG PKI identifie l'auteur de la demande grâce à la phrase de révocation ainsi qu'à ses informations personnelles (date et lieu de naissance, etc.). Seul le titulaire du certificat lui-même est autorisé à demander une révocation par téléphone. Les autres personnes habilitées à demander une révocation doivent le faire par écrit.

Les personnes autorisées à demander une révocation sont les suivantes:

- le titulaire du certificat lui-même,
- le responsable de la SG PKI;
- les responsables de la sécurité de la SG PKI;
- les personnes de référence pour le titulaire du certificat:
  - les collaborateurs des RH (service du personnel);
  - les supérieurs hiérarchiques;
  - les officiers LRA;
  - le DSIO;
  - le DSID;
  - le responsable PKI de l'organisation.

7 Contenu du certificat

Certificat d'authentification (clé d'authentification)
Empreinte digitale (SHA-1):
Validité du certificat:
Numéro de série:

8 Confirmation de réception de la carte à puce

En apposant sa signature sur le formulaire de réception de la carte à puce LRAO, le titulaire du certificat confirme:

- l'exactitude des informations enregistrées sur le certificat;
- la réception de la carte à puce LRAO;
- comprendre et accepter les présentes directives ainsi que les droits et obligations résultant des présentes directives; toutes les questions posées à la SG PKI ont reçu des réponses claires;
- avoir rempli correctement les champs nécessaires relatifs à la phrase de révocation et aux autres informations requises pour l'identification téléphonique de la personne et du certificat.

En outre, le futur LRAO s'engage à respecter et appliquer les directives décrites dans le présent document, dans les CP/CPS («Certificate Policy and Certification Practice Statement of the Swiss Government Root CA I») ainsi que les exigences et les tâches indiquées dans les «Directives d'enregistrement de la classe B de la Swiss Government PKI».

Toute question subsidiaire peut être posée à la SG PKI en envoyant un courriel à l'adresse électronique suivante: pki-info@bit.admin.ch.

NON CLASSIFIÉ

Convention et conditions d'utilisation pour officiers LRA de la SG PKI

concernant l'émission de certificats personnels de classe A (qualifiés et réglementés) et de certificats (avancés) de classe B de la Swiss Government PKI, l'autorité fédérale de la Confédération suisse

V1.0, 28.08.2018

Dans son rôle de prestataire de services de confiance (*Trust Service Provider*, TSP) et sur mandat de l'Unité de pilotage informatique de la Confédération (UPIC), la Swiss Government PKI (SG PKI) de l'OFIT exploite l'infrastructure à clé publique (*Public Key Infrastructure*, PKI) des autorités fédérales de la Confédération suisse. Les certificats des classes A et B sont définis dans le cadre du modèle de marché applicable au service standard Gestion des identités et des accès (SD005). Les officiers de l'autorité d'enregistrement locale (officiers LRA) sont chargés de l'émission des certificats des classes A et B. L'obtention et l'utilisation des certificats LRAO des classes A et B sont soumises aux dispositions des conventions et conditions d'utilisation des classes A et B. Celles-ci sont adaptées tous les ans par la SG PKI aux dispositions légales en vigueur et aux exigences normatives concernant les PKI, sur lesquelles elles s'appuient. Ces exigences font partie intégrante du présent document, dont la version en vigueur est publiée sur www.pki.admin.ch. Tous les titulaires de certificats sont informés par courriel de la publication d'une version actualisée.
Les directives de la SG PKI relatives au certificat LRAO doivent également être respectées. Celles-ci doivent être acceptées lors de l'obtention d'un certificat LRAO.

Exhaustivité et exactitude des informations

Le titulaire d'un certificat LRAO de la SG PKI (appelé ci-après «titulaire ou LRAO»[4]) s'engage à fournir à tout moment au TSP les informations exactes et complètes nécessaires au processus d'émission et au contenu du certificat. Avant l'émission de ce dernier, le LRAO doit être identifié en personne à l'aide d'une pièce d'identité valable. Le certificat est ainsi indissociable du LRAO. Le certificat comprend systématiquement le prénom, le nom, le suffixe et l'adresse électronique du LRAO.

Le titulaire s'engage également à vérifier les données de ses clients (= titulaires de certificats des classes A et/ou B) conformément aux directives d'enregistrement pour les certificats de classe A ou B.

Le LRAO est tenu d'informer le TSP si ses données personnelles changent, notamment son prénom, son nom, son suffixe (utilisé dans l'Admin Directory de la Confédération) ou son adresse électronique.

Protection de la clé privée et du certificat

Le LRAO s'engage à prendre toutes les mesures appropriées pour garantir le contrôle exclusif, la confidentialité et la protection contre la perte et l'emploi abusif de la clé privée ainsi que des éventuels supports (p. ex. carte à puce) et données d'activation (p. ex. NIP et PUK) qui y sont liés. La clé privée du certificat peut et doit être utilisée uniquement en rapport avec le certificat et aux fins prévues pour ce dernier (émission/révocation/gestion des certificats des classes A et B). Elle ne doit en aucun cas être rendue accessible à des tiers non autorisés. Le titulaire répond de tous les dommages causés par la transmission à des tiers de la clé privée et des éventuels supports et données d'activation qui y sont liés.

Le TSP se réserve le droit de révoquer le certificat sans information préalable en cas de suspicion concrète d'emploi abusif ou d'accès non autorisé à la clé privée.

[4] Par souci de lisibilité, seule la forme masculine est utilisée dans l'ensemble de ce document pour désigner aussi bien des personnes de sexe féminin que celles de sexe masculin.

Utilisation du certificat

Le LRAO s'assure de connaître le contenu, le but et l'effet de l'utilisation du certificat LRAO. Il s'engage à utiliser le certificat disponible sur la carte à puce LRAO et la clé privée uniquement pour des opérations autorisées et dans le respect de toutes les dispositions légales en vigueur ainsi que du présent document.

Compte rendu et révocation

Le LRAO s'engage à cesser sans délai l'utilisation du certificat et de sa clé privée ainsi qu'à demander la révocation auprès du TSP si:

- l'on soupçonne concrètement que des activités suspectes ont été exécutées avec le certificat (emploi abusif des données d'activation);
- les informations du certificat ne sont plus correctes ou sont imprécises, ou le seront dans un avenir proche.

Si l'on soupçonne une compromission ou un usage abusif du certificat, il faut immédiatement suivre les instructions du TSP.

Pour des raisons de sécurité et si cela est justifiable du point de vue de la protection des données, le TSP peut transférer à d'autres services compétents, à d'autres TSP, à des entreprises et des groupes industriels des données concernant le LRAO, le certificat et d'autres informations en rapport direct quand le certificat ou la personne qui l'utilise sont identifiés comme sources d'utilisation abusive.

Toutes les informations concernant la révocation sont archivées par le TSP pour des raisons de traçabilité.

Fin de l'utilisation du certificat

Le LRAO s'engage à cesser immédiatement toute utilisation du certificat après son échéance ou sa révocation (en particulier en cas de compromission).

Responsabilité

Le LRAO est responsable du fait que le certificat LRAO et la clé privée qui y est liée soient utilisés uniquement dans le respect des dispositions figurant au paragraphe «Utilisation du certificat» du présent document. Toute infraction à ces dispositions entraîne la révocation du certificat ainsi que d'autres mesures administratives et juridiques. Le LRAO est responsable de toutes les activités qu'il a effectuées avec le certificat de la carte à puce LRAO ainsi que des éventuels dommages qui en résultent et de leurs conséquences.

Déclaration de reconnaissance et de consentement

Le LRAO prend acte que le TSP révoquera avec effet immédiat le certificat en cas de soupçon fondé d'une utilisation abusive, d'une violation des dispositions du présent document ou de toute autre violation des prescriptions légales en vigueur.

En signant le formulaire «Classe A/B: demande d'autorisation pour officier LRA», le LRAO confirme avoir lu et compris le présent document «Convention et conditions d'utilisation pour officiers LRA de la SG PKI» et en accepter les dispositions.

NON CLASSIFIÉ

Convention et conditions d'utilisation des certificats de classe B

Pour l'obtention de certificats personnels avancés de la Swiss Government PKI des autorités fédérales de la Confédération suisse

V1.1, 31.03.2017

Dans son rôle de fournisseur de services de certification (*Certification Service Provider*, CSP) et sur mandat de l'Unité de pilotage informatique de la Confédération, la Swiss Government PKI (SG PKI) exploite l'infrastructure à clé publique (*Public Key Infrastructure*, PKI) des autorités fédérales de la Confédération suisse au sein de l'Office fédéral de l'informatique et de la télécommunication. Les certificats de classe B sont définis dans le cadre du modèle de marché applicable au service standard Gestion des identités et des accès (SD005). L'obtention et l'utilisation de ces certificats de classe B de la SG PKI sont soumises aux prescriptions du présent document, qui sont adaptées chaque année par la SG PKI aux dispositions légales en vigueur et aux exigences normatives concernant les infrastructures à clé publique. Ces exigences font partie intégrante du présent document, dont la version en vigueur est publiée sur www.pki.admin.ch. Tous les titulaires de certificats sont informés par courriel de la publication d'une version actualisée.

Les directives de la SG PKI relatives aux certificats de classe B doivent également être respectées. Elles doivent être acceptées séparément lors de l'obtention d'un certificat de classe B.

Exhaustivité et exactitude des informations

Le titulaire d'un certificat de classe B de la SG PKI (ci-après le «titulaire»[5]) s'engage à fournir à tout moment au CSP les informations exactes et complètes nécessaires au processus d'émission et au contenu du certificat. Avant l'émission de ce dernier, il doit être identifié en personne à l'aide d'une pièce d'identité valable. Le certificat est ainsi indissociable de son titulaire.

Le certificat comprend systématiquement le prénom, le nom, le suffixe et l'adresse électronique de son titulaire. La SG PKI saisit d'autres données personnelles sur le titulaire, telles que sa phrase de révocation et une copie numérisée de sa pièce d'identité valable.

Le titulaire est tenu d'informer le CSP si ses données personnelles changent, notamment son prénom, son nom, son suffixe (utilisé dans l'Admin Directory de la Confédération) ou son adresse électronique.

Protection des clés privées et des certificats

Le titulaire s'engage à prendre toutes les mesures appropriées pour garantir le contrôle exclusif, la confidentialité et la protection contre la perte et l'emploi abusif des clés privées, ainsi que des éventuels supports (p. ex. carte à puce) et de leurs données d'activation (p. ex. NIP et PUK). Les clés privées des certificats peuvent et doivent être utilisées uniquement en rapport avec les certificats et aux fins prévues pour ces derniers (signature, authentification, chiffrement). Elles ne doivent en aucun cas être rendues accessibles à des tiers non autorisés. Le titulaire répond de tous les dommages causés par la transmission à des tiers des privées et des éventuels supports et données d'activation qui y sont liés.

Le CSP se réserve le droit de révoquer les certificats sans information préalable en cas de suspicion concrète d'emploi abusif ou d'accès non autorisé aux clés privées.

Utilisation des certificats

[5] Par souci de lisibilité, seule la forme masculine est utilisée dans l'ensemble de ce document pour désigner aussi bien des personnes de sexe féminin que celles de sexe masculin.

Le titulaire s'assure de connaître le contenu, le but et l'effet de l'utilisation des certificats de classe B. Il s'engage à utiliser ces certificats et les clés privées uniquement pour des opérations autorisées et dans le respect de toutes les dispositions légales en vigueur ainsi que du présent document.

Compte rendu et révocation

Le titulaire s'engage à cesser immédiatement l'utilisation des certificats et des clés privées ainsi qu'à exiger la révocation des certificats auprès du CSP si:

- l'on soupçonne concrètement que des activités suspectes ont été exécutées avec un certificat (emploi abusif des données d'activation, du certificat de signature ou du certificat de chiffrement);
- les informations des certificats ne sont plus correctes ou sont imprécises, ou le seront dans un avenir proche.

Si l'on soupçonne une divulgation ou un emploi abusif des certificats, il faut immédiatement suivre les instructions du CSP.

Pour des raisons de sécurité et si cela est justifiable du point de vue de la protection des données, le CSP peut transférer à d'autres services compétents, à d'autres CSP, à des entreprises et à des groupes industriels des données concernant le titulaire, les certificats et d'autres informations en relation directe lorsque les certificats ou la personne qui les utilise sont identifiés comme sources d'activités suspectes.

Toutes les informations concernant la révocation sont archivées par le CSP pour des raisons de traçabilité.

Fin de l'utilisation des certificats

Le titulaire s'engage à cesser immédiatement toute utilisation des certificats après leur échéance ou leur révocation (en particulier en cas de compromission).

Responsabilité

Le titulaire est responsable du fait que les certificats de classe B et les clés privées qui y sont liées soient utilisés uniquement dans le respect de toutes les dispositions figurant au paragraphe «Utilisation des certificats» du présent document. Toute infraction à ces dispositions entraîne la révocation des certificats ainsi que d'autres mesures administratives et, le cas échéant, juridiques. Le titulaire est responsable de toutes les signatures, authentifications et de tous les chiffrements qu'il a effectués ainsi que des éventuels dommages qui en résultent et de leurs conséquences.

Déclaration de reconnaissance et de consentement

Le titulaire prend acte que le CSP révoquera sans délai les certificats en cas de soupçon fondé d'une utilisation abusive, d'une violation des dispositions du présent document ou de toute autre violation des prescriptions légales en vigueur.

Le titulaire confirme par sa signature qu'il a lu et compris le présent document «Convention et conditions d'utilisation des certificats de classe B» et qu'il en accepte les dispositions.

Lieu et date: _____ Signature: _____

NON CLASSIFIÉ

Directives relatives aux certificats de classe B de la Swiss Government PKI

Explications concernant l'obtention et l'utilisation des certificats de classe B de la Swiss Government PKI

V1.0, 09.03.2017

1 But des certificats de classe B

But

Les certificats de classe B sont définis dans le cadre du modèle de marché applicable au service standard Gestion des identités et des accès (SD005). Ils peuvent être utilisés aux fins suivantes:

- la signature fiable de données afin d'en garantir l'authenticité et l'intégrité;
- le cryptage de données afin d'en garantir la confidentialité;
- l'authentification de personnes afin de garantir une identification sécurisée du titulaire par les composants de contrôle d'accès tels que des portails d'entrée.

L'identité du titulaire des certificats est établie à un haut niveau de sécurité grâce à des mécanismes avancés de contrôle et de sécurité utilisés au cours du processus d'émission des certificats de classe B. Ces certificats sont toujours délivrés en personne et uniquement après l'identification du titulaire à l'aide d'une pièce d'identité valable autorisant l'entrée en Suisse.

But exclu

Les certificats de classe B poursuivent uniquement les fins mentionnées ci-dessus et ne fournissent aucune autre information, assurance ou garantie. Plus particulièrement, ils ne garantissent pas que le titulaire les utilise de manière correcte et légale, ni que:

- le titulaire mentionné sur le certificat est activement impliqué dans les activités opérationnelles;
- le titulaire mentionné sur le certificat respecte les dispositions légales en vigueur;
- le titulaire mentionné sur le certificat est digne de confiance et agit de manière sérieuse dans le cadre des affaires;
- le titulaire mentionné sur le certificat possède les compétences professionnelles, techniques, organisationnelles ou autres pour utiliser ce certificat correctement.

2 Qualité des certificats de classe B

L'officier LRA de la SG PKI respecte les processus définis dans les directives d'enregistrement, qui fixent les mesures raisonnablement exigibles et nécessaires pour confirmer les faits suivants lors de la délivrance initiale de certificats de classe B:

- **Existence juridiquement valable:** le titulaire mentionné sur le certificat de classe B existe en tant que personne physique et est inscrit personnellement dans Admin Directory.
- **Identité:** le nom du titulaire mentionné sur le certificat de classe B correspond au nom figurant sur sa pièce d'identité valable.
- **Autorisation:** le titulaire mentionné sur le certificat de classe B est autorisé à obtenir ce dernier.
- **Exactitude des données:** toutes les données et informations contenues sur le certificat sont correctes.

- **Convention et conditions d'utilisation:** le titulaire mentionné sur le certificat de classe B a été informé par l'officier LRA (*Local Registration Authority*) des droits et obligations décrits dans le document « Convention et conditions d'utilisation des certificats de classe B ». L'officier LRA a répondu clairement aux questions du titulaire. Ce dernier a lu, accepté et signé le document susmentionné.
- **Statut:** la SG PKI publie en ligne le statut du certificat et les informations concernant sa validité ou sa révocation.
- **Révocation:** la SG PKI peut révoquer avec effet immédiat le certificat de classe B pour les motifs mentionnés dans le document « Convention et conditions d'utilisation des certificats de classe B ».

3 Politiques

Toutes les dispositions légales, les politiques (y c. les CP et CPS) et les directives en vigueur relatives aux certificats de classe B sont publiées sur le site web de la SG PKI: www.pki.admin.ch.

4 Contenu et validité des certificats de classe B

Contenu

Les certificats de classe B de la SG PKI contiennent des informations concernant:

- l'éditeur et l'autorité de certification (CA) qui émet le certificat;
- l'autorité de certification racine de la CA qui émet le certificat;
- la politique appliquée;
- la date d'émission et d'expiration du certificat;
- le numéro de série du certificat;
- le but d'utilisation du certificat;
- la liste de révocation des certificats et l'OCSP (*online certificate status protocol*);
- les auditeurs de la CA;
- le titulaire du certificat selon les données inscrites dans Admin Directory lors de la délivrance initiale:
    1) nom commun du titulaire
    2) adresse électronique
    3) nom d'utilisateur principal

Validité

Les certificats de classe B de la SG PKI sont valables au maximum trois ans. Avant la date d'expiration, le titulaire peut renouveler lui-même ses certificats au maximum deux fois pour trois années supplémentaires. Pour ce faire, il dispose de l'assistant de renouvellement des certificats (Rekeying Wizard). Après l'expiration de la troisième période de validité, un nouveau certificat doit être émis par l'intermédiaire de l'officier LRA lors d'un processus identique à celui de la délivrance initiale.

5 Obtention de certificats de classe B

Obtention

Les documents et inscription suivants sont requis pour obtenir des certificats de classe B de la SG PKI:

- une pièce d'identité valable autorisant l'entrée en Suisse (carte d'identité, passeport) établie au nom du requérant;
- un formulaire de demande de certificats de classe B de la SG PKI dûment rempli et signé (électroniquement), ou une demande par la voie hiérarchique de l'office ou par le processus RH défini en interne;
- le document «Convention et conditions d'utilisation des certificats de classe B» signé (qui est imprimé par l'officier LRA à chaque fin du processus d'émission de certificats de classe B, en même temps que le présent document);
- une inscription du requérant dans Admin Directory, comprenant le nom, le prénom (comme indiqués sur la pièce d'identité), une adresse électronique valable et éventuellement un nom d'utilisateur principal (UPN).

Identification

L'identification personnelle du requérant est assurée par un officier LRA de classe B de la SG PKI au moment de la délivrance initiale de certificats et au plus tard après expiration de leur troisième période de validité. Lors d'une émission décentralisée (asynchrone) de certificats de classe B, l'identification personnelle est assurée par un RIO (*Registration Identification Officer*), un collaborateur mandaté par l'officier LRA. Le RIO transmet la confirmation de l'identification à l'officier LRA afin que ce dernier valide ensuite la demande.

Afin d'être identifié, le requérant doit fournir une pièce d'identité dont la validité, la conformité et l'authenticité sont contrôlées. L'officier LRA est en outre tenu de s'assurer que la photo correspond à la personne. En outre, la plausibilité de toute demande d'émission de certificat personnel doit être vérifiée (si le requérant travaille bien au sein de l'unité organisationnelle figurant dans Admin Directory et a besoin du certificat pour son travail, il est autorisé à le demander).

Caractère contraignant

La demande ou le processus interne de demande doivent être approuvés par le service compétent. Les présentes directives ainsi que le document « Convention et conditions d'utilisation des certificats de classe B » doivent être acceptés et signés (électroniquement) par le requérant.

6 Protection de la clé privée et du certificat

Transmissibilité

Les certificats de classe B sont personnels et ne peuvent pas être transmis. Les données personnelles relatives à leur titulaire sont enregistrées tant sur les certificats qu'auprès de la SG PKI.

NIP et PUK

Le NIP doit être choisi indépendamment de tout autre mot de passe et ne doit pas être accessible à des tiers. Il ne doit pas être modifié régulièrement sauf s'il y a lieu de croire qu'un tiers en a eu connaissance.

Les certificats (et ainsi leur support: carte à puce, clé USB, etc.) doivent être protégés à l'aide d'un NIP comprenant au moins six caractères et pouvant être purement numérique ou mélangé. Ce code ne doit jamais être communiqué à un tiers afin d'éviter tout emploi abusif de l'identité électronique du titulaire des certificats.

La PUK de la carte à puce doit comprendre au moins huit caractères selon les règles mentionnées ci-dessus.

Obligation de déclaration

Toute éventuelle perte de carte à puce doit être signalée sans délai par son titulaire à l'organisation de services informatiques ou à l'officier LRA compétent. Le certificat concerné est ensuite bloqué (révoqué) et cette action est inscrite sur une liste de blocage électronique et publique. Même si la carte à puce est retrouvée par la suite, le certificat reste bloqué et invalide. Une fois le blocage effectif, de nouveaux certificats de classe B peuvent immédiatement être demandés auprès de l'officier LRA compétent. Leur processus d'émission est identique à celui de la délivrance initiale.

Tout changement d'organisation, de nom (p. ex. en raison d'un mariage) ou d'adresse électronique nécessite l'émission de nouveaux certificats (processus identique à celui de la délivrance initiale).

7 Révocation

Toute révocation doit faire l'objet d'une demande auprès d'un officier LRA. Un formulaire destiné aux personnes dûment autorisées (cf. liste exhaustive ci-dessous) est disponible à cet effet sur le site Internet de la SG PKI www.pki.admin.ch. Si la révocation est demandée par téléphone, l'officier LRA identifie le titulaire grâce à la phrase de révocation et à ses informations personnelles (date et lieu de naissance, etc.). Seul le titulaire du certificat lui-même est autorisé à demander une révocation par téléphone. Les autres personnes habilitées à demander une révocation doivent le faire par écrit.

Les personnes autorisées à demander une révocation sont les suivantes:

- le titulaire du certificat lui-même;
- le responsable de la SG PKI;
- les responsables de la sécurité de la SG PKI;
- les personnes de référence pour le titulaire du certificat:
  - les collaborateurs des RH (service du personnel);
  - les supérieurs hiérarchiques;
  - les officiers LRA;
  - le DSIO;
  - le DSID;
  - le responsable PKI de l'organisation.

8 Contenu du certificat

Certificat d'authentification (clé d'authentification)
Empreinte digitale (SHA-1):
Validité du certificat:
Numéro de série:

Certificat de cryptage (clé de cryptage)
Empreinte digitale (SHA-1):
Validité du certificat:
Numéro de série:

Certificat de signature (clé de signature)
Empreinte digitale (SHA-1):
Validité du certificat:
Numéro de série:

9 Confirmation de réception de la carte à puce

En apposant sa signature, le titulaire des certificats confirme:

- l'exactitude des informations enregistrées sur le certificat;
- la réception de la carte à puce;
- avoir lu les présentes directives et en avoir discuté avec l'officier LRA, qui a répondu clairement aux éventuelles questions;
- comprendre et accepter les droits et devoirs résultant des présentes directives;
- appliquer les directives définies dans le présent document.

Toute question subsidiaire peut être posée à la SG PKI en envoyant un courriel à l'adresse électronique suivante: pki-info@bit.admin.ch[6].

Nom commun:

Date d'émission: **Signature:** _____

[6] Veuillez également lire le document « Convention et conditions d'utilisation des certificats de classe B de la Swiss Government PKI ». Une copie signée de ce document est exigée lors de la commande de votre certificat de classe B. www.pki.admin.ch

Annexe C: 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 soutenue 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 de bureautique 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 point 3.10 – a été supprimé
V5.2	Remplacement de la station LRA par des clients de bureautique 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 point 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» und «adminSurNameLong») dans AdminDir 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
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 point 6.1.1
V5.2	Listes de contrôle – plusieurs corrections	Annexe A
V5.2	Formulaires – plusieurs mises à jour/corrections et 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 et état/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 point 3.12 «Réparation»	Ancien point 3.12
V6.0	Version après validation	N° de version

État à la version 6.0: 01.11.2019

Entrée en vigueur de la version allemande: 01.01.2020