Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF

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

Liste de contrôle : Émission de certificats de classe B

Directives d'enregistrement de la Swiss Government PKI pour la LRA (DdE)
→Chapitre No. 5.2 Processus d'émission d'un certificat

V2.3 / 13.11.2025 **PUBLIC**

No.	Description	Référence
Étape 1 - Préparation pour la délivrance du certificat		
1.1	Vérifier s'il reste **suffisamment de cartes à puce** ➢ *Si nécessaire, commander des cartes à puce* ➢ *Remarque concernant la conservation et l'élimination des cartes à puce*	• DdE Chapitre 5.2.3.7 • Commande de carte à puce - classe B • DdE Chapitre 3.9 et 3.11
1.2	**Commande** (e-mail signé par les RH/la hiérarchie), ticket ou formulaire de demande (signé par l'utilisateur) reçu?	
1.3	• L'utilisateur est-il autorisé à obtenir un certificat de classe B ? • Êtes-vous responsable de la délivrance en tant que LRAO (branche de l'AdminDirectory) ? Disposez-vous, en tant que LRAO, de l'autorisation nécessaire pour la délivrance ? ➢ *Si l'utilisateur n'est pas autorisé à obtenir le certificat et/ou si vous n'êtes pas responsable de sa demande, rejetez la demande.*	• DdE Chapitre 5.2.1 • AdminDir
1.4	Les **informations fournies dans la demande** sont-elles complètes et plausibles, et le nom, y compris les suffixes, et l'adresse e-mail indiqués dans la demande correspondent-ils à ceux figurant dans le répertoire administrateur ? ➢ *Si les informations fournies ne sont pas correctes, veuillez-vous adresser à votre service des ressources humaines et demander une correction.*	DdE Chapitre 5.2.3.1 et 5.2.3.2
1.5	**Convenir d'une date** pour la délivrance du certificat à l'adresse e-mail indiquée par l'utilisateur. • Informer l'utilisateur dans l'invitation au rendez-vous qu'il doit apporter son document de voyage valide (carte d'identité/passeport). • Les liens vers les documents suivants doivent être joints à l'invitation au rendez-vous. De plus, l'utilisateur doit être invité à lire les conditions d'utilisation et à noter ses éventuelles questions : ○ Convention et conditions d'utilisation des certificats avancés de classe B (pour les personnes physiques) de Swiss Government PKI ○ Guide rapide: Règles pour le code PIN des cartes à puce ○ Guide rapide :Qestions possibles pour les phrases de révocation	• DdE Chapitre 5.2.3.3 • Vérification de l'identité des personnes • Commande de carte à puce - classe B
1.6	Créer un **dossier client** (classeur numérique et/ou papier)	DdE Chapitre 3.6

No.	Description	Référence
Étape 2 – Délivrance de certificats		
2.1	Les **informations fournies** dans la **demande** correspondent-elles à celles figurant dans le **document de voyage** (carte d'identité/passeport) et dans l'**AdminDirectory**, en particulier le nom et le prénom de l'utilisateur (voir le document « Vérification de l'identité des personnes demandant des certificats de classe B ») ? • *Si les informations ne correspondent pas, AUCUN certificat ne doit être délivré. Veuillez-vous adresser à votre service des ressources humaines et demander une correction.*	• DdE Chapitre 5.2.3.1 et 5.2.3.6 • Vérification de l'identité des personnes
2.2	• **Vérifier l'authenticité des documents de voyage (pièce d'identité/passeport)** o d'une carte d'identité/d'un passeport ? → OK o d'un « permis F », vous ne pouvez, en tant que LRAO, délivrer le certificat à cet utilisateur que si vous disposez du « Formulaire complémentaire pour les demandeurs titulaires d'un permis F classe B » rempli par le responsable de la sécurité de votre office/organisation (au niveau fédéral, il s'agit de l'DSID/DSIO). • **Le document de voyage est-il valide** (date d'expiration) ? o Si le document de voyage a expiré (même d'un seul jour), l'utilisateur doit commander un nouveau document de voyage. Une carte à puce ne sera délivrée qu'avec le nouveau document de voyage valide. o Remarque : vous pouvez demander une dérogation au responsable de la sécurité PKI par e-mail (pki-secoff@bit.admin.ch). Le certificat ne peut toutefois être créé qu'après l'octroi d'une dérogation (e-mail crypté du responsable de la sécurité PKI). **Le document de voyage est-il authentique ?** o Le numéro d'identification est-il identique au recto et au verso / le numéro de passeport est-il identique sur chaque page ? o Caractéristiques des documents de voyage (voir les documents sous Vérification de l'identité des personnes). o « Son » émis par la pièce d'identité lorsqu'on la laisse tomber sur la table (le son est différent de celui d'une carte de crédit, par exemple) o Pour les documents de voyage provenant de l'UE, vous pouvez consulter les caractéristiques de sécurité sur PRADO.	• DdE Chapitre 5.2.3.5 • Vérification de l'identité des personnes
2.3	**Identification de l'utilisateur** Les informations figurant dans le document de voyage correspondent-elles à celles de l'utilisateur ? L'utilisateur peut-il être cette personne ? • Voir le document Vérification de l'identité des personnes • Comparer le visage du demandeur avec la photo figurant dans le document de voyage (symétrie du visage) • Taille	• DdE Chapitre 5.2.3.5 • Vérification de l'identité des personnes

No.	Description	Référence
2.4	**Numérisez** (scannez) et enregistrez le **document de voyage** (carte d'identité/passeport) et, le cas échéant, les autres documents nécessaires.	DdE Chapitre 5.2.3.8
2.5	Informer les utilisateurs du choix du code PIN et de la phrase secrète de révocation (conformément à l'invitation au rendez-vous et aux guides rapides correspondants).	DdE Chapitre 5.2.3.9
2.6	• Émettre un certificat sur une carte à puce à l'aide du Walk-In-Wizard. • L'utilisateur doit définir lui-même le code PIN et la phrase secrète de révocation.	DdE Chapitre 5.2.3.10
2.7	Informer l'utilisateur de ses droits et obligations conformément à l' «Convention et conditions d'utilisation des certificats avancés de classe B (pour les personnes physiques) de Swiss Government PKI (V2.0) », répondre à ses questions et faire signer le document par l'utilisateur. • Voir « Points importants (pages 4-5) »	• DdE Chapitre 5.2.3.11 • Commande de carte à puce - classe B
2.8	La signature de l'utilisateur sur le « Contrat d'utilisation et conditions d'utilisation classe B » correspond-elle à celle figurant dans le document de voyage ? • *Si ce n'est pas le cas, clarifier pourquoi.*	
2.9	Remettre à l'utilisateur la carte à puce, le document de voyage (pièce d'identité/passeport) et, le cas échéant, une copie du document « Contrat d'utilisation et conditions d'utilisation classe B ».	DdE Chapitre 5.2.3.12
Étape 3 - Documentation (entrée dans le journal et classement dans le dossier client)		
3.1	Effectuer une entrée dans le journal (sous forme numérique et/ou papier).	DdE Chapitre 5.2.3.13
3.2	Supprimer les documents de voyage éventuellement enregistrés, y compris les e-mails utilisés pour leur envoi, des systèmes locaux.	DdE Chapitre 5.2.3.14
3.3	Conserver toutes les preuves dans le dossier client préparé. Il s'agit des documents suivants : • « Contrat d'utilisation et conditions d'utilisation de classe B » signé (dernière page) • Demande de certificat personnel de classe B ou commande HR	DdE Chapitre 5.2.3.15 et 3.6
Remarque : Délais de conservation		
	Vous devez vous assurer que les demandes peuvent être clairement attribuées aux expositions et que la documentation relative aux demandes ainsi que les preuves utilisées sont encore disponibles 11 ans après l'expiration du certificat. **Nous recommandons une durée de conservation de 15 ans.**	DdE Chapitre 3.6 et 6.1

Points importants :
Convention et conditions d'utilisation des certificats avancés de classe B (pour les personnes physiques) de Swiss Government PKI (V2.0)

Chapitre 1 : Exhaustivité et exactitude des informations

- La personne titulaire (user) d'un certificat de classe B (user) doit s'assurer que les informations requises pour le processus de délivrance et le contenu du certificat sont correctes et complètes.
- L'identité du demandeur est vérifiée au moyen d'une identification personnelle et d'un contrôle du document de voyage.

Chapitre 2 : Protection des clés privées et des certificats

- Les clés privées des certificats de classe B doivent être protégées par un code PIN qui ne peut être utilisé que pour une seule carte à puce.
- Le titulaire doit prendre toutes les précautions nécessaires pour garantir le contrôle exclusif, la confidentialité et la protection contre la perte et l'utilisation abusive des clés privées et de la carte à puce.

Chapitre 3 : Acceptation du certificat

La personne titulaire (user) doit vérifier le contenu du certificat à sa réception et s'assurer qu'il est correct pendant toute sa durée de validité.

Chapitre 4 : Utilisation des certificats

Les certificats de classe B peuvent être utilisés pour

- la signature fiable de données
- le cryptage de données et
- l'authentification de personnes.

La personne titulaire (user) doit s'assurer que les certificats et les clés privées ne sont utilisés que pour des transactions autorisées et dans le respect des dispositions légales en vigueur.

Chapitre 5 : Rapports et révocation

La personne titulaire (user)

- doit informer immédiatement le fournisseur de services de confiance (TSP), c'est-à-dire la Swiss Government PKI BIT, s'il soupçonne une utilisation abusive ou un accès non autorisé à la clé privée.
- peut demander la révocation en personne ou par téléphone.

Le fournisseur de services de confiance (TSP), c'est-à-dire la Swiss Government PKI BIT, est autorisé à transmettre des données et des informations à d'autres autorités compétentes, TSP, entreprises ou groupes industriels en cas de dommage.

Chapitre 6 : Fin de l'utilisation des certificats
La personne titulaire (user) doit immédiatement cesser d'utiliser les certificats après leur expiration ou leur révocation.

Chapitre 7 : Responsabilité
La personne titulaire (user)

- est responsable de veiller à ce que les certificats de classe B et les clés privées associées ne soient utilisés que dans le respect des dispositions de la section Utilisation des certificats.
- est responsable de toutes les signatures, authentifications et cryptages qu'il effectue, ainsi que des dommages et conséquences éventuels résultant d'une utilisation contraire à ses obligations.

Chapitre 8 : Bases juridiques, validité des documents et éléments constitutifs du contrat
Le document « Convention d'utilisation et conditions d'utilisation des certificats avancés de classe B » fait partie intégrante des bases juridiques.

Chapitre 9 : Contenu et validité des certificats avancés de classe B
Les certificats de la Swiss Government PKI contiennent des informations concernant l'émetteur, l'autorité de certification émettrice, la politique applicable, la date d'émission et d'expiration du certificat, le numéro de série du certificat et des informations concernant la personne titulaire (user) du certificat.

Chapitre 10 : Demande et obtention de certificats de classe B
Pour obtenir des certificats avancés de classe B, il faut présenter un document de voyage valable pour entrer en Suisse, une demande signée (p. ex. formulaire de demande, courriel signé du HR, etc.), une inscription personnelle dans le répertoire administratif de la Confédération et un accord d'utilisation et des conditions d'utilisation signés.

Chapitre 11 : Déclaration de reconnaissance et d'accord
La personne qui fait une demande

- prend acte du fait que le fournisseur de services de confiance (TSP), c'est-à-dire la Swiss Government PKI BIT, révoque immédiatement les certificats en cas de suspicion fondée d'abus, de violation des dispositions du présent document ou de toute autre infraction aux dispositions légales en vigueur.
- atteste par sa signature qu'il a lu et compris le présent document et qu'il accepte les dispositions qui y sont énoncées.