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

25.06.2025

Convention et conditions d'utilisation des certificats avancés de classe B (pour les personnes physiques) de Swiss Government PKI

Entrée en vigueur : 01.08.2025 V2.0

Dans son rôle de prestataire de services de confiance Trust Service Provider (TSP) et sur mandat du secteur Transformation numérique et gouvernance de l'informatique (TNI), la Swiss Government PKI (SG PKI) de l'Office fédéral de l'informatique et de la télécommunication (OFIT) exploite la *public key infrastructure* (PKI) des autorités fédérales de la Confédération suisse. Les certificats de classe B pour la signature avancée au sens de la loi sur la signature électronique (SCSE), pour l'authentification et pour le chiffrement 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 tels certificats sont soumises aux prescriptions du présent document, qui sont contrôlées chaque année par la SG PKI et adaptées en cas de besoin aux dispositions légales en vigueur et aux exigences normatives concernant les infrastructures à clé publique.

La version en vigueur est publiée à l'adresse Swiss Government PKI. Tous les titulaires de certificats sont informés par courriel de la publication d'une version actualisée. La nouvelle version est réputée tacitement acceptée si aucune demande de révocation immédiate du certificat n'est transmise dans les 30 jours suivant l'envoi de cette information, des définitions, acronymes, abréviations et références

Remarque : Vous trouverez le glossaire sur la page d'accueil de la PKI.

Contenu

Convention et conditions d'utilisation des certificats avancés de classe B (pour les personnes physiques) de Swiss Government PKI 1
1. Exhaustivité et exactitude des informations 2
2. Protection des clés privées et des certificats 2
3. Réception du certificat 3
4. Utilisation des certificats 3
5. Compte rendu et révocation 4
6. Fin de l'utilisation des certificats 5
7. Responsabilité 5
8. Bases légales, validité des documents et éléments constitutifs du contrat 5
9. Contenu et validité des certificats avancés de classe B 5
10. Demande et obtention de certificats de classe B 6
11. Déclaration de reconnaissance et de consentement 7

1. Exhaustivité et exactitude des informations

La personne physique titulaire de certificats de classe B de la SG PKI (ci-après le « titulaire »[1]) s'engage à fournir à tout moment au TSP les informations exactes et complètes nécessaires au processus d'émission et au contenu du certificat. Les mécanismes étendus de vérification et de sécurité qui sont appliqués pendant le processus d'émission des certificats permettent de déterminer l'identité de la personne qui formule la demande (ci-après le « requérant »[2]) avec un niveau de sécurité élevé. Avant l'émission du certificat, le requérant doit notamment être identifié en personne à l'aide d'une pièce d'identité valable pour l'entrée en Suisse. Le certificat est ainsi indissociable de son titulaire.

Les nom(s) et prénom(s) du titulaire, son suffixe et son adresse électronique sont toujours indiqués dans le certificat (inscription dans l'Admin Directory de la Confédération). La SG PKI saisit et enregistre d'autres données personnelles, comme la date de naissance, les phrases de révocation et une copie numérisée du document d'identification valable.

Le titulaire est tenu d'informer le TSP sans délai de tout changement de ses données enregistrées dans le certificat.

2. Protection des clés privées et des certificats

Les clés privées des certificats de classe B sont enregistrées sur une carte à puce personnelle. Pour activer les clés privées en vue de créer une signature électronique, pour l'authentification et pour le déchiffrement, le titulaire doit utiliser le code PIN de la carte à puce de classe B. Le code NIP de la carte à puce peut être modifié par le titulaire lui-même dans SafeNet Authentication (SAC) Client. Un code NIP peut être utilisé pour une seule carte à puce, et un nouveau code doit être choisi si une carte est remplacée. Ce code ne doit pas être utilisé à d'autres fins (p. ex. Postcard). Il est intransmissible et doit être modifié dès qu'on soupçonne qu'un tiers en a pris connaissance. Les certificats (et ainsi leur support : carte à puce, clé USB, etc.) doivent être protégés à l'aide d'un code NIP comprenant entre six et quatorze caractères et pouvant être purement numérique ou mélangé. Les caractères spéciaux ne sont explicitement pas autorisés dans les codes NIP des certificats de classe B. Le titulaire s'engage à prendre toutes les mesures appropriées à cet égard pour garantir le contrôle exclusif, la confidentialité et la protection contre la perte et l'emploi abusif des clés privées, ainsi que des éventuelles données d'activation (NIP) et de la carte à puce. 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).

Si le titulaire oublie son code NIP ou le saisit plusieurs fois de manière incorrecte, il peut en définir un nouveau en contactant un superutilisateur autorisé par la SG PKI à réinitialiser le code et en se faisant identifier par celui-ci. Cette identification peut se faire au moyen d'une phrase définie lors de l'émission du certificat et de la réponse correspondante. Le superutilisateur chargé de la réinitialisation du code NIP génère un ticket électronique et le titulaire peut choisir un nouveau code après s'être à nouveau identifié auprès d'un utilisateur désigné par l'organisation pour la réinitialisation des codes NIP.

[1] Le terme « titulaire » désigne la personne physique au nom de laquelle le certificat a été établi.

[2] Le terme « requérant » décrit la personne physique faisant la demande de certificat pour elle-même.

Les clés privées des certificats de classe B ne sont pas transmissibles et ne doivent en aucun cas être rendues accessibles à des tiers non autorisés[3]. Elles sont désignées comme non exportables sur le support des certificats (p. ex. la carte à puce).

Le titulaire répond de tout dommage provoqué par la transmission à des tiers des clés privées, des données d'accès aux clés ou des éventuelles données d'activation qui y sont liées ou de la carte à puce.

Les cartes à puce utilisées répondent aux exigences de la SCSE. Tous les composants doivent en outre avoir été approuvés par l'OFIT. Une liste des composants autorisés est publiée sur le site Swiss Government PKI Classe B - Standards, directives et bases légales.

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

3. Réception du certificat

Le titulaire vérifie le contenu du certificat lors de sa réception et s'assure que celui-ci est correct pendant toute la durée de validité.

4. Utilisation des certificats

Les certificats avancés de classe B pour les personnes physiques peuvent être utilisés aux fins suivantes :

- signature fiable de données : l'authenticité et l'intégrité des données sont ainsi garanties ;
- chiffrement de données : la confidentialité des données est assurée ;
- authentification de personnes : le certificat fournit une identification sécurisée du titulaire aux composants de contrôle d'accès (p. ex. portails d'entrée).

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 n'utiliser les certificats de classe B et leur clé privée que pour des opérations autorisées et dans le respect des dispositions légales en vigueur (voir chap. 8 Bases légales, validité des documents et éléments constitutifs du contrat) ainsi que des prescriptions du présent document.

Les certificats avancés de classe B poursuivent uniquement le but mentionné 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 dans le certificat :

- participe activement aux activités concernées ;
- respecte les dispositions légales en vigueur ;
- soit digne de confiance et agisse avec sérieux dans son environnement professionnel ;
- possède les compétences spécialisées, techniques, organisationnelles ou autres nécessaires à l'emploi correct du certificat.

[3] Dans le présent document, on entend par « tiers non autorisés » toutes les personnes qui n'ont pas été autorisées à récupérer des informations au sujet d'un certificat en raison d'un décès ou d'une procédure judiciaire.

Au moment de la première émission d'un certificat avancé de classe B, la SG PKI confirme les points suivants :

- *Existence juridiquement valable :* le titulaire mentionné dans le certificat existe en tant que personne physique et est inscrit personnellement dans l'Admin Directory de la Confédération.
- *Identité :* le nom du titulaire mentionné dans le certificat correspond à celui qui figure sur son document d'identification valable.
- *Autorisation :* la SG PKI a exécuté toutes les étapes raisonnablement exigibles et nécessaires pour vérifier que le titulaire mentionné dans le certificat est autorisé à obtenir ce dernier.
- *Exactitude des données :* la SG PKI a pris toutes les mesures raisonnablement exigibles et nécessaires pour garantir que les données et les informations contenues dans le certificat sont correctes.
- *Statut :* la SG PKI publie le statut du certificat et des informations sur sa validité ou sa révocation, qui sont consultables en ligne 24 heures sur 24, 7 jours sur 7. Elle respecte ainsi les dispositions légales.

En cas de questions ou de problèmes dans l'utilisation des certificats, vous pouvez contacter votre Service Desk local ou celui de l'OFIT (tél. +41 (0)58 465 88 88). Pour une procédure de recours ou pour toute question concernant ce document, vous pouvez contacter la SG PKI à l'adresse pki-info@bit.admin.ch.

5. Compte rendu et révocation

Le titulaire s'engage à cesser sans délai d'utiliser les certificats et les clés privées correspondantes ainsi qu'à demander immédiatement au TSP (p. ex. officier LRA de la SG PKI au sein de l'organisation du titulaire) la révocation (déclaration d'annulation) des certificats lorsque :

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

Il convient de suivre immédiatement les instructions du TSP, en particulier en cas de soupçon de compromission ou d'usage abusif des certificats.

Le titulaire peut demander la révocation en personne ou par téléphone. Le TSP ou la personne mandatée par lui (p. ex. officier LRA) identifiera le titulaire.

Les autres personnes qui ont le droit de solliciter une révocation doivent déposer leur demande par écrit à l'aide du formulaire (électronique) de révocation. Les personnes autorisées à demander une révocation sont les suivantes :

- le titulaire lui-même ;
- le supérieur hiérarchique du titulaire ;
- la personne responsable à la SG PKI ;
- la personne responsable de la sécurité à la SG PKI ;
- l'officier LRA compétent de la SG PKI ;
- le délégué à la sécurité informatique de l'unité organisationnelle ou du département ;
- les collaborateurs des ressources humaines (service du personnel) responsables du titulaire.

L'établissement de nouveaux certificats peut être demandé au TSP aussitôt après un blocage. Le processus d'émission est identique à celui du certificat initial.

Les informations relatives à l'identification, à l'émission des certificats et à la révocation sont saisies par le TSP à des fins de traçabilité ainsi que traitées et conservées conformément aux dispositions légales. Le délai de conservation obligatoire de onze ans commence au moment de l'échéance ou de la déclaration d'annulation des certificats.

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 titulaire, les certificats et d'autres informations en rapport direct quand les certificats ou le titulaire qui les utilise sont identifiés comme sources d'utilisation abusive.

6. 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).

7. Responsabilité

Le titulaire doit garantir une utilisation de ses certificats de classe B et des clés privées associées conformément aux dispositions du paragraphe intitulé Utilisation des certificats (chap. 4) » du présent document. Toute infraction à ces dispositions entraîne la révocation des certificats ainsi que, le cas échéant, d'autres mesures administratives et juridiques. Le titulaire est responsable de toutes les signatures, authentifications et chiffrements dont il est l'auteur ainsi que des éventuels dommages résultant d'une utilisation illicite et de leurs conséquences.

8. Bases légales, validité des documents et éléments constitutifs du contrat

Les bases légales suivantes et les autres règles ci-après font partie intégrante de la présente convention. Elles s'appliquent dans l'ordre suivant :

1. La loi fédérale sur les services de certification dans le domaine de la signature électronique et des autres applications des certificats numériques (SCSE ; RS *943.03*) ;
2. L'ordonnance sur les services de certification dans le domaine de la signature électronique et des autres applications des certificats numériques (OSCSE ; RS *943.032*) ;
3. L'ordonnance de l'OFCOM sur les services de certification dans le domaine de la signature électronique et des autres applications des certificats numériques (RS *943.032.1*) ;
4. Le document CP/CPS Root CA I de la SG PKI ;
5. Le présent document « Convention et conditions d'utilisation des certificats avancés de classe B (pour les personnes physiques) de Swiss Government PKI » ;
6. Les exigences normatives relatives aux infrastructures à clé publique.

Les dispositions légales, les politiques et les directives en vigueur applicables aux certificats réglementés et avancés de classe B sont publiées ou mises en lien sur le site Internet de la Swiss Government PKI Classe B - Standards, directives et bases légales.

9. Contenu et validité des certificats avancés de classe B

Les certificats de la SG PKI contiennent des informations concernant :

- l'émetteur (TSP) et l'autorité de certification (*certificate authority*, CA) qui établit le certificat ;
- la CA racine de la CA qui établit le certificat ;
- la politique en vigueur ;
- la date d'émission et d'expiration du certificat ;
- le numéro de série du certificat ;
- la liste de révocation des certificats (*certificate revocation list*) et le protocole de vérification des certificats en ligne (*online certificate status protocol*) ;
- le titulaire du certificat au moment de la première émission de celui-ci :

- prénom(s), nom(s) et suffixe figurant dans l'Admin Directory (*common name* du titulaire) ;
- l'adresse électronique du titulaire ;
- le nom d'utilisateur principal (*user principal name*, UPN) ;
- la clé publique.

Les certificats sont valables trois ans maximum. 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 (Renewal Wizard). Après l'expiration de la troisième période de validité, un nouveau certificat doit être émis par l'intermédiaire de l'officier LRA selon un processus identique à celui de la première émission. Dans ce cas également, la procédure est la même que pour la première émission. Il faut se présenter personnellement en vue d'une nouvelle identification, avec les documents nécessaires.

10. Demande et obtention de certificats de classe B

Les documents et inscriptions suivants sont requis pour obtenir des certificats avancés 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 futur titulaire. La date d'expiration ne doit pas être dépassée ;
- un formulaire de demande de certificats de classe B de la SG PKI dûment rempli et signé (électroniquement, classe B au moins), ou une demande écrite par la voie hiérarchique de l'organisation ou par le processus RH défini en interne ;
- une inscription du requérant dans l'Admin Directory de la Confédération, avec nom(s), prénom(s) (comme indiqués sur la pièce d'identité), une adresse électronique valable et éventuellement un UPN ;
- «Convention et conditions d'utilisation des certificats avancés de classe B (pour les personnes physiques) de Swiss Government PKI» (présent document) dûment signé.

L'identification personnelle du requérant est assurée par un officier LRA de classe B de la SG PKI lors de la première émission des 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 agent d'enregistrement et d'identification (*registration identification officer*, RIO), 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. Le requérant doit se présenter personnellement pour l'émission du certificat. Afin d'identifier le requérant, la validité, la conformité et l'authenticité de la pièce d'identité sont vérifiées par l'officier LRA ou le RIO lors de l'émission du certificat. L'officier LRA et le RIO sont en outre tenus de s'assurer que la photo correspond à la personne. En outre, la plausibilité de toute demande d'émission de certificat avancé doit être vérifiée (si l'auteur de la demande travaille bien au sein de l'unité administrative indiquée, a besoin du certificat pour son travail, est autorisé à demander un certificat).

Si des informations complémentaires sont requises, le requérant a dix jours pour les fournir à la SG PKI. Passé ce délai, la demande devient automatiquement caduque.

11. Déclaration de reconnaissance et de consentement

Le requérant prend acte que le TSP révoquera 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.

Par sa signature, le requérant atteste avoir lu et compris le présent document «Convention et conditions d'utilisation des certificats avancés de classe B (pour les personnes physiques) de Swiss Government PKI» et accepte les dispositions qui y figurent.

Nom, prénom (requérant) :	(électronique cl. B) signature requérant :
Lieu et date :	