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[1].

Nom commun:

Date d'émission: **Signature:** _____

[1] 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