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

Convention et conditions d'utilisation des certificats de classe A – certificats réglementés et qualifiés au sens de la SCSE (pour les personnes physiques et morales)

V2.4, 11.11.2025

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 l'infrastructure à clé publique (*public key infrastructure*, PKI) des autorités fédérales de la Confédération suisse. Les certificats de classe A pour la signature réglementée ou qualifiée (ci-après les «certificats») au sens de la SCSE 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 sur www.pki.admin.ch. 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.

Table des matières

1 Exactitude des informations

La personne physique ou morale[1] titulaire d'un certificat de classe A de la SG PKI (ci-après le «titulaire»[2]) 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 émet la demande (ci-après le «requérant»[3]) avec un niveau de sécurité élevé. Avant l'émission du certificat, le requérant doit notamment être identifié en personne avec certitude à l'aide d'une pièce d'identité valable. Le certificat est ainsi indissociable de son titulaire.

- Certificats pour les personnes physiques:

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

[1] En vertu de la SCSE, les certificats réglementés peuvent être délivrés au nom d'une personne physique ou d'une entité IDE. La SG PKI délivre des certificats réglementés uniquement à des personnes morales figurant dans le registre IDE. Pour les personnes physiques, elle établit des certificats qualifiés.

[2] Le terme «titulaire» désigne la personne physique ou morale au nom de laquelle le certificat a été établi. La personne morale peut être une autorité, par exemple.

[3] Le terme «requérant» désigne la personne physique qui sollicite le certificat pour elle-même ou pour une personne morale pour laquelle elle dispose du pouvoir de représentation.

- Certificats pour les personnes morales:

  Le requérant doit être autorisé à représenter le titulaire. Les procurations écrites, ainsi que la version numérisée de la pièce d'identité valable du requérant, sont collectées et stockées auprès de la SG PKI.

  Le titulaire est désigné sous forme de nom distinctif (*distinguished name*) dans le certificat, conformément à la norme X.509. Le certificat comprend l'IDE et le nom officiel de la personne morale (par ex. l'autorité) au niveau des attributs respectifs «Organization» et «OrganizationIdentifier».

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

La clé privée du certificat de classe A est stockée sur une mémoire centrale de haute sécurité (HSM, service de signature) de la SG PKI.

- Service de signature de l'OFIT:

  Pour activer la clé en vue de créer une signature/cachet électronique réglementé, l'utilisateur utilise dans l'application correspondante le certificat d'authentification stocké sur sa carte à puce personnelle de classe B avec le NIP correspondant ou le MobileID personnelle. Si le service de signature d'une application spécialisée est utilisé et que l'on a recours à une clé commune enregistrée dans l'application pour activer la clé en vue de créer une signature électronique, la clé et les données d'accès doivent être conservées en un lieu manifestement sûr.
  En cas d'utilisation de la MobileID, les conditions d'utilisation séparées de la MobileID font partie intégrante du présent document (https://www.mobileid.ch/fr/documents).

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 de la clé privée et données d'accès. La clé privée du certificat peut et doit être utilisée uniquement en rapport avec le certificat et aux fins prévues pour ce dernier (signature).

Les clés privées de certificats pour les personnes physiques ne sont pas transmissibles et ne doivent en aucun cas être rendues accessibles à des tiers.

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

Les HSM utilisés répondent aux exigences de la SCSE.

Le TSP 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.

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 du certificat

- Certificats qualifiés pour les personnes physiques :

  Les certificats qualifiés de classe A pour les personnes physiques ne peuvent être utilisés que pour apposer une signature électronique fiable, juridiquement valable et assimilée à une signature manuscrite. Ils confirment l'authenticité et l'intégrité des documents ainsi que l'accord du signataire avec leur contenu. Le titulaire s'assure de connaître le contenu, le but et l'effet de l'utilisation du certificat. Il s'engage à utiliser le certificat et sa clé privée dans le respect de toutes les dispositions légales en vigueur ainsi que conformément au présent document et aux instructions de son unité administrative / employeur.

Les certificats qualifiés de classe A poursuivent uniquement le but susmentionné et ne fournissent aucune autre information, assurance ou garantie. En particulier, ils ne garantissent pas que le titulaire d'un certificat agisse de manière licite et correcte en employant ce dernier, 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 de ce dernier.

Au moment de l'émission d'un certificat qualifié de classe A, la SG PKI confirme les points suivants:

- Existence juridiquement valable: le titulaire mentionné dans le certificat existe en tant que personne physique ou morale.
- Identité: le nom du titulaire mentionné dans le certificat (sans le suffixe) correspond à celui qui figure sur sa pièce d'identité 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 entrepris 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.
- Conditions d'utilisation: le requérant a été informé par l'officier de l'autorité d'enregistrement locale (officier LRA) des droits et obligations figurant dans le présent document. L'officier LRA de la SG PKI a répondu clairement à ses questions en la matière. Le requérant a lu, accepté et signé le document en question.
- Révocation: le cas échéant, la SG PKI peut révoquer sans délai le certificat pour les motifs mentionnés dans le présent document.

- Certificats réglementés pour les personnes morales:

  Les certificats réglementés de classe A pour les personnes morales, également appelés certificats d'autorité, sont soumis aux dispositions de la SCSE, de l'OSCSE ainsi qu'à d'autres prescriptions légales. Ils ne peuvent être utilisés que pour signer des documents électroniques.

  La signature par un certificat réglementé de classe A pour les personnes morales crée des cachets électroniques. Les services administratifs et les autorités peuvent signer numériquement des documents officiels à l'aide d'un certificat émis pour l'unité concernée et d'un horodatage qualifié (art. 2, let. j, SCSE). Les citoyens et les entreprises doivent pouvoir vérifier que les documents officiels signés (cachetés) électroniquement proviennent réellement de l'autorité indiquée. L'horodatage opéré atteste du moment précis où le document a été signé.

  Les certificats réglementés de classe A remplissent uniquement le but susmentionné et ne fournissent aucune autre information, assurance ou garantie. En particulier, ils ne garantissent pas que la personne physique qui utilise le certificat agisse de manière licite et correcte en employant ce dernier, ni que la personne qui utilise 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 de ce dernier.

  Au moment de l'émission d'un certificat réglementé de classe A , la SG PKI confirme les points suivants:

- Existence juridiquement valable: la personne morale mentionnée dans le certificat réglementé existe et est inscrite dans le registre IDE public (www.uid.admin.ch).
- Identité: le nom qui figure dans le certificat réglementé à l'attribut «O=» du certificat correspond à celui de la personne morale inscrite dans le registre IDE.
- Autorisation: la SG PKI a exécuté toutes les étapes nécessaires et exigées par la SCSE pour vérifier que le requérant est autorisé à obtenir le certificat.
- Exactitude des données: la SG PKI a entrepris toutes les mesures raisonnablement exigibles et nécessaires pour garantir que les données et les informations contenues dans le certificat sont correctes.
- Conditions d'utilisation: le requérant a été informé par l'officier LRA des droits et des obligations figurant dans le présent document. L'officier LRA de la SG PKI a répondu clairement à ses questions en la matière. Le requérant a lu, accepté et signé le document en question.
- 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 de la SCSE et de l'OSCSE ainsi que les autres prescriptions légales.
- Révocation: le cas échéant, la SG PKI peut révoquer le certificat sans délai pour les motifs mentionnés dans le présent document.

Plusieurs certificats peuvent être délivrés pour une même personne morale. Les demandes correspondantes peuvent être présentées par le même ayant droit.

La clé privée est stockée sur un HSM pour être utilisée avec le service de signature, soit plusieurs utilisateurs peuvent être autorisés avec leur certificat personnel de classe B ou le MobileID personnelle, soit, dans le cas des applications spécialisées, un certificat TLS commun peut être enregistré dans l'application. Ce certificat TLS enregistré, qui valide l'utilisation du certificat de signature proprement dit pour une personne morale, et les données d'accès correspondantes peuvent être remis à des collaborateurs sur ordre du requérant, celui-ci portant la responsabilité au nom de la personne morale. La transmission des données d'accès doit être consignée par écrit de manière transparente et exhaustive. Les applications spécialisées avec authentification par le biais d'un certificat TLS ne peuvent être reliées au service de signature qu'après un audit réalisé par un auditeur externe.

En cas d'utilisation de la MobileID, les conditions d'utilisation séparées de la MobileID font partie intégrante du présent document (https://www.mobileid.ch/fr/documents).

Le requérant répond de tout dommage causé par la transmission à des tiers des données d'accès à la clé privée et de leurs éventuels supports.

Le requérant garantit que le contenu, le but et l'effet de l'utilisation du certificat réglementé de classe A sont connus de lui, et le cas échéant des autres utilisateurs autorisés. Il s'engage à utiliser le certificat de classe A et sa clé privée dans le respect de toutes les dispositions légales en vigueur et conformément au présent document. Il informe en détail et de manière vérifiable ses co-utilisateurs au sujet des dispositions en vigueur et du présent document.

La signature se fait à l'aide du certificat et d'un logiciel de signature. Au moment de la validation du présent document, les applications recommandées à cet effet par la SG PKI sont DesktopSigner et le service de signature de l'OFIT. La signature est vérifiée chez le destinataire par le biais du validateur (www.validator.admin.ch). Une signature électronique n'est valable qu'avec un horodatage qualifié. Pour garantir une validation à long terme (LTV), il est recommandé d'apposer la signature conformément au standard LTV, c'est-à-dire d'ajouter systématiquement un horodatage. Ce cachet peut être obtenu auprès de la SG PKI (autorité d'horodatage, TSA).

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. 058 465 88 88). Pour une procédure de réclamation ou pour toute question concernant le présent document, il est possible de contacter la SG PKI à l'adresse électronique pki-secoff@bit.admin.ch.

5 Compte rendu et révocation

Le titulaire s'engage à cesser immédiatement l'utilisation du certificat et de la clé privée correspondante ou à les retirer et à demander aussitôt au TSP (p. ex. officier LRA de la SG PKI dans l'organisation du titulaire) la révocation (déclaration d'annulation) du certificat lorsque:

- l'on soupçonne concrètement que des activités suspectes ont été exécutées avec le certificat (compromission/usage abusif du certificat de signature);
- les informations contenues sur le certificat ne sont plus correctes ou sont imprécises, ou le seront dans un avenir proche;

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

Le requérant initial du certificat peut en demander la révocation soit personnellement, soit par courriel signé, soit par téléphone. Le TSP ou la personne mandatée par lui (p. ex. officier LRA) identifiera le titulaire avec certitude.

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 (pour les personnes morales: un fondé de pouvoir du titulaire);
- le requérant initial;
- les supérieurs hiérarchiques du titulaire et du requérant;
- la personne responsable à la SG PKI;
- un officier de sécurité de la SG PKI;
- l'officier LRA compétent de la SG PKI;
- le délégué à la sécurité informatique de l'unité organisationnelle (DSIO);
- pour les certificats destinés aux personnes physiques: les collaborateurs des RH compétents pour le titulaire (service du personnel).

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, le certificat et d'autres informations en rapport direct quand le certificat ou la personne qui l'utilise sont identifiés comme sources d'activités suspectes.

Aux fins de traçabilité, le TSP archive toutes les informations concernant la révocation conformément aux prescriptions légales.

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

6 Fin de l'utilisation du certificat

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

7 Responsabilité

Le titulaire est responsable du fait que son certificat qualifié de classe A et la clé privée qui y est liée soient utilisés uniquement dans le respect de toutes les prescriptions légales en vigueur ainsi que des dispositions figurant au paragraphe «Utilisation du certificat» du présent document. Toute infraction entraîne la révocation du certificat ainsi que, le cas échéant, d'autres mesures administratives et juridiques. Le titulaire est responsable de toutes les signatures qu'il a apposées ainsi que des éventuels dommages résultant d'une utilisation illicite et de leurs conséquences.

Lorsque la SG PKI contrevient à des obligations découlant de la loi sur la signature électronique (SCSE) ou de ses dispositions d'exécution, elle répond, conformément à l'art. 17 SCSE, du dommage causé au titulaire du certificat et aux tiers qui se sont fiés à un certificat valable.

La responsabilité de la SG PKI est limitée selon le droit applicable:

- en cas de violation du contrat, la SG PKI répond des dommages attestés, à moins qu'elle ne prouve qu'aucune faute ne lui est imputable;
- en cas de négligence grave, à 100 000 francs par sinistre et par an;
- en cas de négligence légère, à un montant équivalant aux prestations fournies durant l'année du contrat en cours, mais au maximum à 50 000 francs par sinistre et par an.

La SG PKI décline toute autre responsabilité. Elle n'assume en particulier aucune responsabilité pour les dommages dus au fait que le titulaire utilise les certificats à d'autres fins que celles qui sont définies dans les prescriptions légales et dans les dispositions du paragraphe «Utilisation du certificat» du présent document.

La responsabilité pour les dommages consécutifs, le manque à gagner et la perte de données est expressément exclue.

En outre, la SG PKI ne répond pas des dommages et du retard résultant de cas de force majeure, catastrophes naturelles (p. ex. foudre, événements naturels), pannes de courant, conflits armés, grèves, restrictions administratives imprévisibles, contournement de dispositifs de blocage, PC-Dialer, cyberattaques, infection d'équipements informatiques par un virus (p. ex. chevaux de Troie), etc. Si la SG PKI ne remplit pas ses obligations contractuelles à la suite d'un tel événement, l'exécution du contrat ou le délai d'exécution du contrat est reporté en fonction de l'événement survenu. La SG PKI n'est pas responsable des éventuels dommages causés au client par le report de l'exécution du contrat.

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) loi sur la signature électronique (SCSE, RS *943.03*);
2) ordonnance sur la signature électronique (OSCSE, RS *943.032*);
3) 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) loi fédérale sur le numéro d'identification des entreprises (LIDE; RS *431.03*);
5) CP/CPS Root CA IV de la SG PKI (http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_5_0.pdf);
6) «Convention et conditions d'utilisation des certificats de classe A – certificats réglementés et qualifiés au sens de la SCSE (pour les personnes physiques et morales)» (le présent document).
   En cas d'utilisation de la MobileID : les conditions d'utilisation de la MobileID (https://www.mobileid.ch/fr/dokumente)

Les dispositions légales, les politiques et les directives en vigueur applicables aux certificats réglementés et qualifiés de classe A sont publiées ou mises en lien sur le site web de la SG PKI (www.pki.admin.ch).

9 Contenu et validité des certificats réglementés et qualifiés de classe A

Les certificats de la SG PKI contiennent des informations concernant:

- l'autorité de certification racine et l'autorité émettrice;
- la politique en vigueur;
- la date d'émission et d'expiration du certificat;
- le numéro de série du certificat;
- la CRL et l'OCSP;
- le titulaire du certificat:
  - ses nom(s) et prénom(s) selon son passeport ou sa carte d'identité; l'IDE et le nom officiel du titulaire dans le cas de personnes morales,
  - le nom commun du titulaire, à savoir nom(s), prénom(s), suffixe,
  - l'adresse électronique;

- la clé publique.

Le certificat est valable au maximum trois ans. À l'expiration de ces trois ans, le TSP doit émettre un nouveau certificat en procédant à une nouvelle identification personnelle. Le titulaire ne peut pas renouveler son certificat lui-même. La procédure pour le renouvellement est la même que pour l'émission initiale. Il faut se présenter personnellement en vue d'une nouvelle identification, avec les documents nécessaires.

10 Demande et obtention de certificats de classe A

Les documents ou inscriptions suivants sont requis pour obtenir des certificats de classe A de la SG PKI:

- Certificats qualifiés pour les personnes physiques:

  Les documents ou inscriptions suivants sont requis pour obtenir des certificats qualifiés de classe A de la SG PKI:

  - une pièce d'identité valable autorisant l'entrée en Suisse (carte d'identité, passeport), établie au nom du futur titulaire;
  - un formulaire de demande de certificats qualifiés de classe A de la SG PKI dûment rempli et signé (par voie électronique, au moins avec un certificat de classe B);
  - une inscription personnelle dans l'Admin Directory de la Confédération comportant les nom(s) et prénom(s) (conformément à la pièce d'identité) et l'adresse électronique;
  - le document «Convention et conditions d'utilisation des certificats de classe A – certificats réglementés et qualifiés au sens de la SCSE (pour les personnes physiques et morales)» signé (le présent document).

  Afin d'identifier avec certitude le futur titulaire, la validité, la conformité et l'authenticité de la pièce d'identité sont contrôlées. La correspondance de la photo avec la personne présente est également vérifiée. De même, la plausibilité de la requête doit être vérifiée avant d'émettre un certificat qualifié personnel (la personne travaille bel et bien dans l'unité d'organisation indiquée dans Admin Directory et a besoin du certificat dans son quotidien professionnel; le futur titulaire est autorisé à demander un certificat).

- Certificats réglementés pour les personnes morales:

  Les documents ou inscriptions suivants sont requis pour obtenir un certificat réglementé de classe A de la SG PKI:

  - le futur titulaire est une entité IDE au sens de l'art. 3, al. 1, let. c, de la loi fédérale du 18 juin 2010 sur le numéro d'identification des entreprises (LIDE);
  - le requérant doit être autorisé à représenter l'entité IDE en question. Cette autorisation peut être attestée grâce à un extrait du registre du commerce certifié conforme ou un pouvoir de représentation muni d'une signature juridiquement valable;
  - le formulaire de demande pour les certificats réglementés de classe A de la SG PKI rempli et signé par le requérant. Le requérant peut signer la demande sous forme électronique à l'aide de son certificat de signature qualifié personnel de classe A;
  - le document «Convention et conditions d'utilisation des certificats de classe A – certificats réglementés et qualifiés au sens de la SCSE (pour les personnes physiques et morales)» signé par le requérant (le présent document);
  - une pièce d'identité valable autorisant l'entrée en Suisse (carte d'identité, passeport), établie au nom du requérant.

  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 de classe A de la SG PKI lors de l'émission du certificat. L'officier LRA est en outre tenu de s'assurer que la photo correspond à la personne. De même, la plausibilité de la requête doit être vérifiée avant d'émettre un certificat réglementé (la personne travaille bel et bien dans l'unité d'organisation indiquée, elle est autorisée à obtenir et utiliser un certificat réglementé de classe A pour les personnes morales et elle a besoin du certificat dans son quotidien professionnel).

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 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.

Par sa signature sur la demande , le requérant atteste avoir lu et compris le présent document «Convention et conditions d'utilisation des certificats de classe A – certificats réglementés et qualifiés au sens de la SCSE (pour les personnes physiques et morales)» et accepter les dispositions qui y figurent.