Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF

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

Directives de la Swiss Government PKI relatives aux certificats standards de classe C

Explications concernant l'établissement, l'obtention et l'utilisation des certificats standards de classe C de la Swiss Government PKI V1.0, 18.01.2016

1 But des certificats standards de classe C

But

Les certificats standards de classe C ont pour but l'authentification fiable sur des systèmes ou des applications, de même que la signature et le cryptage fiables de documents et de connexions. Ces certificats sont établis pour des personnes, des organisations ou des systèmes. De plus, ils permettent la signature et le cryptage fiable des messages émis à partir de boîtes aux lettres de groupe.

Les certificats standards de classe C pour les systèmes peuvent être utilisés pour des serveurs, des clients, des routeurs, etc. Les certificats d'organisation sont émis au nom d'une personne morale ou d'une organisation, tandis que les certificats de personne de cette classe ne sont émis que pour des personnes physiques.

Les certificats standards de classe C sont disponibles dans les formes suivantes:

Forme	Authentification Client	Authentification serveur	Signature	Cryptage	Nom commun (CN) Sujet
Certificat Personne auth	Oui	explicitement non	Non	Non	Personne (nom)
Certificat Personne auth/sign	Oui	explicitement non	Oui	Non	Personne (nom)
Certificat Personne auth/sign/crypt	Oui	explicitement non	Oui	Oui	Personne (nom)
Certificat Personne sign/crypt	Non	explicitement non	Oui	Oui	Personne (nom)
Certificat Personne sign	Non	explicitement non	Oui	Non	Personne (nom)
Certificat Personne crypt	Non	explicitement non	Non	Oui	Personne (nom)
Certificat Organisation auth	Oui	explicitement non	Non	Non	Organisation (nom)
Certificat Organisation auth/sign	Oui	explicitement non	Oui	Non	Organisation (nom)
Certificat Organisation auth/sign/crypt	Oui	explicitement non	Oui	Oui	Organisation (nom)
Certificat Organisation sign/crypt	Non	explicitement non	Oui	Oui	Organisation (nom)
Certificat Organisation sign	Non	explicitement non	Oui	Non	Organisation (nom)
Certificat Organisation crypt	Non	explicitement non	Non	Oui	Organisation (nom)
Certificat Système auth	Oui	explicitement non	Non	Non	Système (nom)
Certificat Système auth/sign	Oui	explicitement non	Oui	Non	Système (nom)
Certificat Système auth/sign/crypt	Oui	explicitement non	Oui	Oui	Système (nom)
Certificat Système sign/crypt	Non	explicitement non	Oui	Oui	Système (nom)
Certificat Système sign	Non	explicitement non	Oui	Non	Système (nom)
Certificat Système crypt	Non	explicitement non	Non	Oui	Système (nom)
Certificat Boîte aux lettres de groupe sign/crypt	Non	explicitement non	Oui	Oui	Boîte aux lettres de groupe (nom)

Les certificats standards de classe C poursuivent uniquement le but mentionné ci-dessus et ne fournissent aucune autre information, assurance ou garantie. Plus particulièrement, ils ne garantissent pas que:

- le détenteur mentionné dans le certificat est activement impliqué dans l'activité commerciale;
- le détenteur mentionné dans le certificat respecte les dispositions légales en vigueur;
- le détenteur mentionné dans le certificat est digne de confiance et agit de manière sérieuse dans le cadre des affaires;
- les systèmes fonctionnent sans erreur avec ce certificat;

But exclu

Il est explicitement précisé que les certificats de cette classe ne peuvent pas servir à l'authentification serveur. Cette fonction est réservée aux certificats SSL/TLS de la Swiss Government PKI (SG-PKI). Les certificats SSL serveur avec l'extension d'utilisation de clé «authentification du serveur» sont soumis à des conditions particulières et ne sont établis que par l'autorité de certification (Certification Authority, CA) Swiss Government SSL CA 01. A cet effet, des directives et des conditions contractuelles et d'utilisation distinctes sont applicables. De la même manière, bien que les certificats de signature de code de la SG-PKI font partie des certificats standards de classe C, ils sont soumis à d'autres directives et conditions contractuelles et d'utilisation (de plus amples informations sur les certificats de signature de code figurent sous : https://www.bit.admin.ch/adminpki/00240/00241/06072/index.html?lang=fr).

2 Tâches et obligations des émetteurs de certificats

Avant l'émission d'un certificat standard de classe C, il est obligatoire de vérifier et de confirmer l'exactitude des données, l'existence, l'authenticité et l'autorisation du détenteur mentionné dans le certificat. La personne habilitée à émettre le certificat est tenue de suivre la procédure suivante :

- **Existence:** l'émetteur de certificats standards de classe C pour des organisations, des systèmes et des personnes vérifie, au nom de la SG-PKI, le Common Name (CN) du sujet mentionné dans le certificat de même que l'adresse électronique mentionnée dans le certificat.
- **Exactitude des données et authenticité:** l'émetteur entreprend au nom de la SG-PKI toutes les mesures raisonnablement exigibles et nécessaires pour garantir que les données et les informations contenues dans le certificat sont correctes. L'émetteur doit en outre s'assurer que l'exactitude des attributs mentionnés dans le certificat a été confirmée par le biais de l'adresse électronique figurant dans le certificat.
- **Autorisation:** l'émetteur entreprend au nom de la SG-PKI toutes les mesures raisonnablement exigibles et nécessaires pour vérifier que le détenteur mentionné dans le certificat standard de classe C (l'émetteur de la commande) est autorisé à obtenir le certificat.

Veuillez observer les points suivants:

- **Conditions contractuelles et d'utilisation:** l'émetteur habilité de certificats standards de classe C doit lire, accepter et signer les conditions contractuelles et d'utilisation pour les certificats standards de classe C de la SG-PKI.

- **Statut:** la SG-PKI publie le statut des autorisations d'émission octroyées, des certificats, de même que les informations relatives à leur validité ou à leur révocation, de sorte qu'ils puissent être consultés en ligne 24 heures sur 24, 7 jours sur 7. Elle respecte ainsi les dispositions légales et les normes du CA/Browser Forum.
- **Révocation:** la SG-PKI respecte les dispositions des normes du CA/Browser Forum et des CP et CPS de la SG-PKI et peut, si nécessaire, révoquer avec effet immédiat l'autorisation d'émettre octroyée et les certificats standards de classe C pour les motifs mentionnés dans les conditions contractuelles et d'utilisation.

3 Politiques

Toutes les dispositions légales, les politiques (y c. celles des CP et CPS) et les directives en vigueur relatives aux certificats standards de classe C sont publiées sur le site web de la SG-PKI sous: https://www.bit.admin.ch/adminpki/00240/00241/06111/index.html?lang=fr.

4 Contenu et validité des certificats standards de classe C

Contenu

Le certificat standard de classe C de la SG-PKI contient des informations concernant:

- Editeur et CA qui établit le certificat
- Informations concernant la CA Racine de la CA qui établit le certificat
- Informations concernant la politique en vigueur
- Date d'émission et d'échéance du certificat
- Numéro de série du certificat
- Informations concernant la CRL et l'OCSP
- Informations concernant les auditeurs de la CA
- Informations concernant le certificat (*DN=Distinguished Name, voir paragraphe suivant)*:
  - Nom commun
  - Organisation
  - Unité d'organisation
  - Lieu

Distinguished Name

Les certificats standards de classe C se différencient par les DN utilisés de la manière suivante:

Distinguished Name pour les certificats de personne	
CN =	*CN= Common Name: nom(s), prénom(s), par exemple:* ***Mustermeier Hanspeter***
OU =	*OU= Unité organisationnelle: à choisir librement, par exemple, office, division, domaine, etc.* *Exemple:* ***Office fédéral de la recherche prospective (OFREP) - Bureautique***
O =	*O= Organisation: au choix, par exemple unité administrative ou «Swiss Government PKI»* *par exemple:* ***OFREP – Bureautique*** *ou* ***Swiss Government PKI***
L =	*L= Lieu: siège de l'organisation, par exemple:* ***Berne (BE)***
C =	*C= Country: entrée fixe:* ***CH***
Distinguished Name pour les certificats de système	
CN =	*CN= Common Name: nom du système, par exemple:* ***TUSER-SYSP-SCPP123***
OU =	*OU= Nom de la plateforme du système, par exemple:* ***Plateforme système eDocuments***
O =	*O= Organisation: entrée fixe:* ***Admin***
C =	*C= Country: entrée fixe:* ***CH***
Distinguished Name pour les certificats d'organisation	
CN =	*CN= Common Name: description selon le registre IDE ou traduction officielle.* *par exemple:* ***Office fédéral de la recherche prospective (OFREP)***
OU =	*OU= Unité organisationnelle: à choisir librement, par exemple IDE selon registre, division, domaine, etc.* *par exemple:* ***CHE-123.456.789*** *ou* ***Bureautique***
O =	*O= Organisation: à choisir librement, par exemple:* ***Confédération suisse*** *ou* ***OFREP – Bureautique***
L =	*L= Lieu: siège de l'organisation, le cas échéant, le registre IDE, par exemple:* ***Berne (BE)***
C =	*C= Country: entrée fixe:* ***CH***
Distinguished Name pour les certificats de boîte aux lettres de groupe	
CN =	*CN= Common Name: nom de la boîte aux lettres de groupe, par exemple:* ***_BIT-PKI-Info***
OU =	*OU= Unité organisationnelle: entrée fixe:* ***Group Mailboxes***
OU =	*OU= Unité organisationnelle: entrée fixe:* ***eGov-Services***
O =	*O= Organisation: à choisir librement, par exemple:* ***Confédération suisse*** *ou* ***OFREP – Bureautique***
L =	*L= Lieu: siège de l'organisation, par exemple:* ***Berne (BE)***
C =	*C= Country: entrée fixe:* ***CH***

Validité

Les certificats standards de classe C de la SG-PKI sont valables au maximum 3 ans. L'autorisation d'émission du certificat fait l'objet d'une vérification chaque année et devra être confirmée pour l'année suivante.

5 Obtention de l'habilitation à émettre des certificats standards de classe C

Obtention

Les certificats standards de classe C sont délivrés par le Certificate Request Wizard (CRW). Exception : les certificats de boîte aux lettres de groupe doivent toujours être délivrés directement par la SG-PKI et peuvent être commandés au moyen d'un formulaire en ligne à l'adresse: https://www.bit.admin.ch/adminpki/00240/00241/02370/02374/03685/index.html?lang=fr. Pour obtenir des autorisations d'accès à cette application, les documents suivants sont nécessaires:

- Certificat valable de classe B, établi au nom de l'auteur de la demande
- *Formulaire de demande de certificats standards de classe C de la SG-PKI* dûment rempli et muni d'une signature électronique
- *Conditions contractuelles et d'utilisation pour les certificats standards de classe C de la SG-PKI des autorités fédérales de la Confédération suisse*, signées électroniquement (à chaque commande d'autorisations d'accès au CRW)
- Attestation de réussite de la *formation aux certificats standards de classe C*

Les certificats spécifiques pour des organisations peuvent également être commandés directement auprès de la SG-PKI au moyen du formulaire suivant : https://www.bit.admin.ch/adminpki/00240/00241/02370/02374/03685/index.html?lang=fr. La commande de certificats spécifiques pour des organisations et des boîtes aux lettres de groupe requiert la confirmation des présentes *directives* et l'acceptation *des conditions contractuelles et d'utilisation des certificats standards de classe C de la SG-PKI*.

Identification et vérification

L'identification personnelle de l'auteur de la demande est garantie par les processus des certificats de la SG-PKI de classe B. Pour être autorisé à accéder au CRW, l'auteur de la demande doit disposer d'un certificat valable et les documents doivent être signés avec le certificat de classe B personnel. La signature sur le document est validée au moment de l'émission. L'habilitation à émettre des certificats standards de classe C est enregistrée sur le certificat de classe B personnel; elle ne peut donc être ni transmise, ni déléguée. Toute modification ou renouvellement du certificat personnel de classe B requiert un nouvel enregistrement dans le CRW.

Formation

L'auteur de la demande doit suivre une formation d'une demi-journée avant la validation des autorisations. Les formations portant sur les certificats standards de classe C sont publiées sur la page https://www.bit.admin.ch/adminpki/00240/00241/06111/06141/index.html?lang=fr. L'attestation de réussite de la formation est obligatoire pour l'octroi de l'autorisation.

Caractère contraignant

Le présent formulaire et les *conditions contractuelles et d'utilisation pour l'obtention de l'habilitation à émettre des certificats standards de classe C de la SG-PKI* doivent être signés et envoyés électroniquement par l'auteur de la demande avec un certificat de classe B à la SG-PKI.

6 Protection de l'accès au CRW

Transmissibilité

L'accès aux modèles de politique et les autorisations correspondantes dans le CRW sont personnels et protégés par le certificat de classe B. Il est interdit de transmettre à un tiers les données d'accès de même que le certificat de classe B habilité.

Obligation de déclarer

L'émetteur est tenu, le cas échéant, de signaler à la SG-PKI la résiliation de ses fonctions et de demander le blocage de ses droits d'accès au CRW au moyen du formulaire prévu.

7 Protection de la clé privée et du certificat

Transmissibilité

Les certificats standards de classe C pour les personnes ou les systèmes sont établis pour un individu ou un objet précis et ne sont pas transmissibles. Les certificats standards de classe C pour les organisations ou les boîtes aux lettres de groupe sont établis pour une organisation ou une adresse électronique précise et ne peuvent être utilisés qu'au nom de ce sujet, même si le certificat lui-même peut figurer sur plusieurs clients ou comptes d'utilisateur.

Protection de la clé privée

Si le détenteur (ou l'auteur de la demande) délègue l'émission des paires de clés à l'émetteur, le transfert du lot P12 (certificat et paire de clés) au détenteur doit obligatoirement avoir lieu sous forme codée et sécurisée. Le mot de passe de la clé privée doit être communiqué à part, et également sous forme codée (courriel distinct, SMS, lettre, communication personnelle, etc.). Il est strictement interdit à l'émetteur d'archiver la clé privée ou le fichier P12 d'un autre détenteur ou de le conserver d'une quelconque autre manière. Dès que le lot P12 a été transmis au détenteur, l'émetteur doit supprimer la clé privée sur son client ou sur tout autre support de stockage.

Mot de passe et installation de la clé privée

Que le certificat soit inscrit sur un support ou utilisé sous forme de «soft token», les clés privées sont soumises aux règles suivantes:

- Le mot de passe pour l'installation de la clé privée doit être conservé en sécurité par le détenteur du certificat.
- Le mot de passe de la clé privée doit être composé d'au moins 8 caractères et comporter au moins une majuscule, une minuscule et un chiffre. Le mot de passe ne doit en aucun cas être communiqué à des tiers.
- Le mot de passe utilisé pour l'installation de la clé privée doit être unique. En outre, il ne doit pas être utilisé pour d'autres clés privées.
- Lors de l'installation du certificat, la clé privée ne doit pas être marquée comme exportable.

Publication

La clé publique d'une boîte aux lettres de groupe d'entités internes à la Confédération est publiée dans l'annuaire électronique de l'administration fédérale (Admin-Directory) par la SG-PKI directement après l'émission. Sur demande, les clés publiques des certificats d'organisation peuvent également être publiées dans l'Admin-Directory. Il est en outre possible de publier les clés publiques des certificats d'organisation et de boîte aux lettres de groupe sur une page web de la SG-PKI. Cette publication peut être demandée par courriel à l'adresse pki-info@bit.admin.ch. L'actualisation du certificat publié relève de la responsabilité de son détenteur.

Obligation de déclarer

Toute perte du certificat doit être immédiatement signalée à la SG-PKI par l'intermédiaire du Service Desk de l'OFIT (servicedesk@bit.admin.ch). La SG-PKI bloquera les certificats et publiera le blocage sur une liste électronique publique. Si le certificat est retrouvé, les certificats bloqués ne seront pas réactivés. Après blocage dans le CRW, un nouveau certificat standard de classe C peut être commandé. Le processus d'établissement d'un nouveau certificat standard de classe C est le même que pour le premier certificat.

Les changements de fonction au sein de l'organisation, le changement de nom (d'une personne, après mariage, par ex., ou d'un système) ou la modification de l'adresse électronique et de la désignation d'une organisation nécessitent l'émission d'un nouveau certificat.

8 Révocation

Toute révocation doit être signalée à la SG-PKI. Pour cela, un formulaire est à votre disposition : https://www.bit.admin.ch/admin-pki/00240/00241/06072/06095/index.html?lang=fr. Le formulaire doit être signé avec un certificat de classe B de la SG-PKI et remis par voie électronique au Service Desk de l'OFIT (servicedesk@bit.admin.ch). Les instances et les personnes suivantes peuvent demander une révocation:

- le détenteur;
- la hiérarchie;
- le responsable de la sécurité de l'organisation;
- l'émetteur;
- le responsable du serveur;
- le responsable de la boîte aux lettres de groupe;
- le responsable de la sécurité (Security Officer) de la SG-PKI;
- le responsable de la SG-PKI.

9 Prix

Autorisations liées au CRW

L'autorisation pour l'émission d'un certificat dans le CRW est facturée 250 francs par année et par personne. Ces frais couvrent l'exploitation de la plateforme et l'assistance aux personnes autorisées.

Prix des certificats

Les certificats commandés par le biais du CRW au moyen du processus à exécuter soi-même sont facturés 30 francs par année et par certificat. Les certificats établis par la SG-PKI sont facturés 175 francs par année et par certificat.

Les coûts pour les certificats établis sont dus pour la durée totale de validité du certificat (max. 3 ans), même en cas de révocation anticipée.

10 Confirmation et acceptation

En cochant le champ de saisie «Confirmation» sur la page du formulaire, vous confirmez avoir lu, compris et accepté les présentes directives. Le champ de signature dans lequel le formulaire doit être signé numériquement avec un certificat de classe B de la SG-PKI sera alors activé. En cas de question, vous pouvez prendre contact avec la SG-PKI à l'adresse électronique pki-info@bit.admin.ch[1].

[1] Veuillez prendre connaissance des *conditions contractuelles et d'utilisation pour l'obtention de l'habilitation à émettre des certificats standards de classe C de la SG-PKI*. Lors de votre demande d'autorisation pour l'utilisation du CRW, une copie signée de ce document sera demandée. https://www.bit.admin.ch/admin-pki/00240/00241/06111/index.html?lang=fr