Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF

Office fédéral de l'informatique et de la télécommunication OFIT
Betrieb
Betrieb Frontend Services
PKI

Autorisation pour l'acquisition de certificats (EV) SSL de la Swiss Government PKI V2.0

La personne doit être en possession d'un certificat de classe B pour l'activation !

L'autorisation pour l'acquisition de certificats SSL (certificats machines / serveurs) de la *Swiss Government PKI* est demandée par la personne suivante, pour les domaines mentionnés ci-après :

Mandant	
Titre	
Nom, prénom, suffixe	
Canton / office/ entreprise	
Adresse complète	
No de téléphone	
Adresse e-mail	

Niveau de vérification [1]:

Examen : **OV** ◯ **EV** ◯ (Ne pas encore disponible)

Confirmation :
En cliquant sur le champ à droite vous confirmez d'avoir lu et acceptés les lignes directrices (pages suivantes), et les conditions contractuelles de la Swiss Government PKI : ☐

Domaine *admin.ch* :

La signature du propriétaire du domaine (René Staudenmann OFIT) est exigée pour le domaine ***admin.ch.***

La personne a le droit de recevoir des certificats SSL pour les domaines admin.ch :	
Signature propriétaire du domaine ***admin.ch***	

[1] **OV :** *Organization Validated* : L'examen d'autorisation est effectué au niveau d'Organisation.
EV : *Extended Validation* : Pour la validation de l'autorisation un examen approfondi du domaine, de l'organisation et de la personne est effectué. Une lettre d'autorisation de l'organisation est nécessaire. Certificats émis avec une autorisation étendue se reconnaissent à la ligne verte dans l'URL. Informations détaillées se trouvent dans les directives.

Office fédéral de l'informatique et de la télécommunication OFIT
SwissGov-PKI Order Manager
Monbijoustrasse 74
CH-3003 Berne

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF

Office fédéral de l'informatique et de la télécommunication OFIT
Betrieb
Betrieb Frontend Services
PKI

Domaines au dehors de l'admin.ch :

Pour les domaines suivants, le propriétaire du domaine confirme, par sa signature, que :

1. le mandant est autorisé à demander des certificats SSL pour les domaines mentionnés ci-dessous auprès de la Swiss Government PKI.
2. le propriétaire du domaine a pris note du CP/CPS (Certificate Policy and Certification Practice Statement) du „Swiss Government Root CA III".
   http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf
3. la Swiss Government PKI est autorisée à établir des certificats SSL pour les serveurs dans les domaines mentionnés ci-dessous.

Domaine	Lieu, date	Signature du propriétaire du domaine conformément à la saisie dans *WhoIs*

Mandant Nom, prénom : / Fonction :	**Date :**	**Signature : (électronique)**
/		

Merci de renvoyer le formulaire dûment complété et signé à l'adresse postale ci-dessous. Les formulaires signés électroniquement peuvent être renvoyés à l'adresse pki-info@bit.admin.ch

Directives relatives aux certificats d'authentification (EV) SSL/TLS

Explications concernant l'obtention et l'utilisation des certificats (EV) SSL/TLS de la Swiss Government PKI (SG-PKI)

V. 1.0, 24.06.2016

1 But des certificats (EV) SSL/TLS

But

Le but des certificats (EV) SSL/TLS est d'authentifier de manière fiable les serveurs. Les certificats sont établis dans les formes suivantes : *Server Authentication*, *Client Authentication* et *Server/Client Authentication*. Enfin, les certificats (EV) SSL/TLS sont uniquement établis pour les systèmes qui justifient d'un nom de domaine entièrement qualifié (*Fully Qualified Domain Name,* FQDN).

But exclu

Les certificats (EV) SSL/TLS poursuivent uniquement le but mentionné ci-dessus et ne fournissent aucune autre information, assurance ou garantie.
Plus particulièrement, ils ne garantissent pas que :

- les systèmes fonctionnent sans erreur avec ce certificat ;
- l'exploitant et le contenu du serveur mentionnés dans le certificat respectent les dispositions légales en vigueur ;
- l'exploitant et le contenu du serveur mentionnés dans le certificat sont fiables et que l'exploitant agisse de manière sérieuse dans le cadre des affaires.

2 Attestations

Au moment de l'émission d'un certificat (EV) SSL/TLS, la SG-PKI atteste les faits suivants :

- **Existence juridiquement valable** : le mandant du certificat (EV) SSL/TLS, le propriétaire du domaine et l'organisation existent en tant que sujets juridiques et sont enregistrés au niveau de l'office.
- **Identité** : le domaine et l'organisation du serveur et de l'identificateur d'objet (OID) mentionnés dans le certificat (EV) SSL/TLS correspondent aux données des registres publics et sont représentés par une ou plusieurs personnes physiques et identifiables.
- **Autorisation** : La SG-PKI a entrepris toutes les mesures raisonnablement exigibles et nécessaires pour vérifier que le mandant mentionné dans le certificat (EV) SSL/TLS est autorisé à obtenir le certificat pour le domaine et l'organisation.
- **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 contractuelles et d'utilisation :** le mandant du certificat (EV) SSL/TLS a lu, accepté et signé les *conditions contractuelles et d'utilisation des certificats (EV) SSL* de la SG-PKI.
- **Statut :** la SG-PKI publie sur Internet le statut du certificat et les informations concernant sa validité ou sa révocation, de sorte qu'ils peuvent être consultés 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/CPS de la SG-PKI et peut, si nécessaire, révoquer avec effet immédiat le certificat (EV) SSL/TLS pour les motifs mentionnés dans les conditions contractuelles et d'utilisation.

3 Policies

Toutes les dispositions légales, les politiques (y c. celles des CP et CPS) et les directives en vigueur concernant les certificats (EV) SSL/TLS sont publiées sur le site web de la SG-PKI sous : https://www.bit.admin.ch/adminpki/00240/00241/05913/index.html?lang=fr.

4 Contenu et validité des certificats (EV) SSL/TLS

Contenu

Le certificat (EV) SSL/TLS de la SG-PKI contient des informations concernant :

- Editeur (CSP) et CA qui établit le certificat
- CA Racine de la CA qui établit le certificat
- Politique en vigueur
- Date d'émission et d'échéance du certificat
- Numéro de série du certificat
- CRL et OCSP
- Auditeurs de la CA
- OID de l'organisation
- Nom de domaine entièrement qualifié (*Fully Qualified Domain Name,* FQDN)
- Code du pays
- Etat, canton ou localité où est située l'organisation

Validité

Le certificat (EV) SSL/TLS de la SG-PKI est valable au maximum trois ans.

5 Obtention des certificats (EV) SSL/TLS

Obtention

L'obtention du certificat (EV) SSL/TLS de la SG-PKI est soumise aux conditions suivantes :

- Certificat valable de classe B, établi au nom du mandant
- *Formulaire d'autorisation pour les certificats (EV) SSL/TLS de la SG-PKI* dûment rempli et muni d'une signature électronique
- *Conditions contractuelles et d'utilisation des certificats EV SSL/TLS* munies d'une signature électronique
- *Authorization Letter by Organization (EV) SSL* munie d'une signature valable

Refus

Aucun certificat (EV) SSL ne sera en principe émis pour les serveurs ne possédant pas de nom de domaine entièrement qualifié (par ex. adresse IP) ou de joker (par ex. *.bit.admin.ch).

Identification

L'identification personnelle du mandant est garantie par les processus des certificats de la SG-PKI de classe B. S'il veut obtenir un certificat (EV) SSL/TLS, le mandant doit posséder un certificat de classe B valable, qui servira par ailleurs à signer le document d'autorisation. Afin d'obtenir le certificat d'un domaine, le mandant doit recevoir l'autorisation écrite du propriétaire du domaine en question. L'autorisation d'obtenir le certificat pour un domaine particulier est contrôlée par les processus de la SG-PKI ou par le propriétaire du domaine. L'identification de l'organisation et des personnes, et par conséquent l'établissement et la transmission du certificat, dépendent de la validation des signatures, de l'autorisation, du FQDN, de l'identificateur d'objets (ou de l'organisation) et du CSR (Certificate Signing Request).

Vérification

Afin d'attester l'existence du domaine et l'autorisation relative à l'obtention du certificat (EV) SSL/TLS de la SG-PKI, il convient de consulter les registres publiques (www.whois.com, www.firestorm.ch, etc.), les registres internes et externes à la Confédération (Admin-Directory, www.uid.admin.ch, SHAB) et les banques de données internes à la SG-PKI pour les mandants de certificats (EV) SSL/TLS autorisés. Les personnes de contact mentionnées dans le formulaire, en particulier les propriétaires de domaines, seront interrogées par téléphone, par courrier ou personnellement quant à l'authenticité de la signature qu'ils ont apposée sur le formulaire de demande.[1]

Caractère contraignant

Le document d'autorisation et les conditions contractuelles et d'utilisation requièrent une signature numérique avec un certificat de classe B de la SG-PKI et doivent être remis par voie électronique.

6 Protection de la clé privée et du certificat

Transmissibilité

Le certificat (EV) SSL/TLS est émis pour un serveur ou un client en particulier et n'est pas transmissible.

Clés privées

Le mandant doit prendre toutes les mesures appropriées pour garantir constamment l'intégrité de la clé privée et de l'accès sécurisé du certificat. La clé privée et le certificat ne doivent pas être transmis à des tiers. Fait exception le cas dans lequel le mandant n'est pas lui-même le détenteur du certificat, mais a commandé celui-ci de façon légitime pour le transmettre à une personne travaillant dans le même office ou département, conformément aux tâches et aux compétences qui lui ont été attribuées. Dans ce cas, le mandant est tenu de faire accepter par écrit au détenteur du certificat de respecter les obligations découlant des conditions contractuelles et d'utilisation (EV) SSL/TLS ainsi que des présentes directives.

Obligation d'annonce

En cas de perte du certificat, la SG-PKI doit être prévenue par l'intermédiaire du Service Desk de l'OFIT (servicedesk@bit.admin.ch). La SG-PKI bloquera alors les certificats et publiera le blocage sur une liste électronique publique. Le processus d'établissement du nouveau certificat (EV) SSL/TLS est le même que pour le premier certificat.

7 Révocation

Les révocations doivent être adressées au SG-PKI par le Service Desk de l'OFIT en mentionnant les motifs de révocation.

8 Confirmation et acceptation

En cochant la case «Je confirme» dans le document d'autorisation, le mandant confirme avoir lu, compris et accepté les 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] **Certificats OV (règlement de la SG-PKI OID 2.16.756.1.17.3.62.1/2.16.756.1.17.3.62.2)**

Dans le cas des certificats *Organisation Validated (OV)*, l'organisation qui requiert le certificat est vérifiée et le nom de l'organisation est cité dans le certificat.

Certificats EV (règlement de la SG-PKI OID 2.16.756.1.17.3.62.4/2.16.756.1.17.3.62.5)
Les certificats *Extended Validation (EV)* assurent le niveau fiabilité le plus élevé pour l'utilisateur et requièrent beaucoup d'efforts de la CA pour être validés. Des documents supplémentaires doivent être mis à disposition afin de pouvoir émettre un certificat EV.

NON CLASSIFIÉ

Conditions contractuelles et d'utilisation (EV) SSL/TLS

pour l'obtention de certificats d'authentification (EV) SSL/TLS de la Swiss Government PKI des autorités fédérales de la Confédération suisse

V1.0, 02.06.2016

Dans son rôle de fournisseur de services de certification (*Certification Service Provider*, CSP) et sur mandat de l'Unité de pilotage informatique de la Confédération (UPIC), la Swiss Government PKI (SG-PKI) exploite l'infrastructure à clé publique (*Public Key Infrastructure*, PKI) des autorités fédérales de la Confédération suisse. Parmi les prestations standards de l'UPIC figurent l'émission des *certificats d'authentification de classe C SSL/TLS* et *de classe C EV SSL/TLS* (ci-après «certificats (EV) SSL»), de même que l'octroi des *autorisations à commander* de tels certificats. L'émission, l'obtention et l'utilisation des certificats (EV) SSL de la SG-PKI sont soumises aux conditions contractuelles et d'utilisation mentionnées ci-dessous. Celles-ci sont adaptées chaque année par la SG-PKI aux dispositions légales et aux normes du CA/Browser Forum[1]. Ces dernières font partie intégrante des présentes conditions contractuelles et d'utilisation. Les versions en vigueur, aussi bien des présentes conditions contractuelles et d'utilisation que des normes du CA/Browser Forum, sont publiées sur https://www.bit.admin.ch/adminpki/00240/00241/05913/05914/index.html?lang=fr.

Les directives de la SG-PKI relatives aux certificats d'authentification (EV) SSL/TLS de classe C doivent également être respectées. Elles doivent être acceptées séparément lors de la demande d'autorisation à commander les certificats et lors de chaque modification des autorisations.

Exhaustivité et exactitude des informations

La personne habilitée à commander des certificats (EV) SSL (ci-après «mandant»[2]) s'engage à fournir au CSP les informations correctes et complètes lors de la commande de certificats et à communiquer toute modification. Le mandant doit notamment s'assurer que toutes les informations et les données, en particulier le nom de domaine entièrement qualifié (*Fully Qualified Domain Name*, FQDN) et la saisie de l'organisation (O=*organization*), de l'unité d'organisation (OU=*organization unit*) et du lieu (L=*location*), soient enregistrées correctement et dans leur intégralité dans le *Certificate Signing Request* (CSR). Il est en outre tenu d'informer le CSP si son rôle ou son domaine de responsabilité subit une modification importante.

Protection des certificats et de l'accès à la plate-forme

Les certificats (EV) SSL peuvent être émis sur des serveurs (ou serveurs Web) ou des clients. Les données concernant le mandant sont gérées par la SG-PKI. Le mandant s'engage à prendre toutes les mesures appropriées pour garantir en tout temps le contrôle d'accès, la confidentialité et la protection contre l'emploi abusif de la plate-forme. Cette plate-forme ne doit en aucun cas être rendue accessible à des tiers non autorisés ; en outre, elle ne peut et ne doit être utilisée qu'aux fins prévues dans le cadre de la commande de certificats.
La clé privée ne doit pas être transmise à des tiers. Fait exception le cas dans lequel le mandant n'est pas lui-même le détenteur du certificat, mais a commandé celui-ci de façon légitime pour le transmettre à une personne travaillant conformément aux tâches et aux compétences qui lui ont été attribuées.
Le mandant répond de tous les dommages causés par la transmission à des tiers non autorisés des données d'accès à la plate-forme de commande ou par la transmission des certificats et des clés qui lui sont confiés et des éventuels médias qui y sont liés.

[1] *CA/Browser Forum – Guidelines (http://cabforum.org/documents.html)*

[2] Pour plus de lisibilité, la forme masculine («mandant» ou «détenteur») a été retenue pour faire référence aux deux sexes.

Le CSP se réserve le droit de révoquer sans information préalable les autorisations d'accès à la plate-forme de commande en cas de suspicion concrète d'emploi abusif, d'accès non autorisé ou de transmission à des tiers non autorisés des données d'accès et de certificats décrits ci-dessus.

Utilisation de la plate-forme et des certificats

Le mandant s'engage à utiliser la plate-forme de commande et les certificats uniquement à des fins autorisées et légales. Il est notamment interdit de commander volontairement des certificats contenant des informations fausses ou inexactes. Par ailleurs, les certificats doivent être émis uniquement pour des domaines pour lesquels le mandant a reçu une autorisation explicite de la part du propriétaire (lettre d'autorisation dûment signée). Le mandant garantit en outre connaître le contenu, le but et l'effet des certificats qu'il commande. La plate-forme de commande, les certificats (EV) SSL et leurs clés privées doivent être utilisés uniquement pour des affaires (de l'entreprise) autorisées et dans le respect de toutes les dispositions légales, des présentes conditions contractuelles et d'utilisation, ainsi que des normes du CA/Browser Forum.

Compte rendu et révocation

Le mandant s'engage à exiger immédiatement la révocation du certificat quand :

- il existe une suspicion concrète d'emploi abusif du certificat ou de mauvaise utilisation de celui-ci ;
- les informations contenues sur le certificat ne sont plus correctes ou sont imprécises, ou le seront prochainement ;
- il existe une suspicion concrète d'emploi abusif ou de divulgation des données d'activation ou de la clé privée en rapport avec la clé publique liée au certificat ;
- il existe une suspicion concrète que le certificat est utilisé dans le but de compromettre le CSP ou que son utilisation pourrait y conduire.

En cas de suspicion de divulgation ou d'emploi abusif, il est nécessaire de donner suite aux instructions du CSP dans les plus brefs délais. Pour des raisons de sécurité et si cela est justifiable du point de vue de la protection des données, le CSP peut transférer à d'autres services compétents, à d'autres CSP, à des entreprises et des groupes industriels, y compris au CA/Browser Forum, des données concernant le mandant, le propriétaire du domaine, le certificat et d'autres informations en rapport direct quand :

- le mandant abuse de la plate-forme de commande, fait preuve de négligence ou ne respecte pas les conditions contractuelles et d'utilisation ;
- le certificat, la personne qui l'utilise ou le serveur/client sur lequel il est installé est identifié comme étant la source d'une utilisation abusive ou d'un maliciel;
- le détenteur qui commande le certificat ou le serveur/client sur lequel le certificat doit être installé ne peut pas être identifié ou vérifié ;
- le certificat a été révoqué pour d'autres motifs que ceux invoqués par le mandant (par ex. : divulgation, etc.).

Toutes les informations concernant la révocation sont archivées par le CSP pour des raisons de traçabilité.

Fin de l'utilisation du certificat

A l'échéance d'un certificat ou après sa révocation (notamment en raison d'une divulgation), le mandant s'engage à cesser immédiatement l'utilisation du certificat en question ou, s'il n'est pas lui-même détenteur de celui-ci, à prendre contact avec le détenteur et à entreprendre toutes les démarches raisonnablement exigibles et nécessaires pour mettre immédiatement un terme à son utilisation.

Fin de l'activité en tant que mandant de certificat

Le mandant s'engage à informer la SG-PKI d'une éventuelle fin de ses activités ou de son rôle en tant que personne habilitée à commander des certificats (par ex. en cas de changement de poste ou de fonction) et à demander la suppression de ses droits d'accès à la plate-forme au moyen du formulaire ad hoc.

Responsabilité

Le mandant est responsable du fait que toute commande et toute utilisation des certificats (EV) SSL et des clés privées qui y sont liées se fassent uniquement dans le respect de toutes les dispositions légales en vigueur ainsi que des présentes conditions contractuelles et d'utilisation, des directives de la SG-PKI relatives aux certificats d'authentification (EV) SSL/TLS et des normes du CA/Browser Forum.

Toute infraction à ces dispositions entraîne la révocation des droits d'accès à la plate-forme de commande, la révocation des certificats commandés par le mandant, ainsi que d'autres mesures administratives et juridiques. Le mandant est responsable de tous les certificats qu'il a commandés ainsi que des éventuels dommages qui en résultent et de leurs conséquences lorsqu'il est établi qu'il a enfreint intentionnellement ou par négligence les dispositions légales, les présentes conditions contractuelles et d'utilisation ou toute autre disposition issue des directives mentionnées.
Si le mandant n'est pas lui-même le détenteur du certificat, mais a commandé celui-ci de façon légitime pour le transmettre à une personne travaillant dans le même office, conformément aux tâches et aux compétences qui lui ont été attribuées, il est tenu de faire accepter par écrit au détenteur du certificat de respecter lui aussi les présentes conditions contractuelles et d'utilisation (EV) SSL/TLS ainsi que les normes du CA/Browser Forum.

Modification des conditions contractuelles et d'utilisation

Les modifications ultérieures et compléments apportés aux présentes conditions contractuelles et d'utilisation sont considérés comme étant acceptés par le mandant s'il ne les conteste pas dans les 30 jours qui suivent leur communication.

Déclaration de reconnaissance et de consentement

Le mandant prend connaissance du fait que le CSP révoque irrémédiablement l'habilitation à commander des certificats sur la base d'une suspicion justifiée d'emploi abusif, de violation des présentes conditions contractuelles et d'utilisation ou d'une autre infraction contre les dispositions légales en vigueur (par ex. fraude, distribution de certificats compromis, etc.).
Le mandant confirme par sa signature qu'il a lu et compris les présentes conditions contractuelles et d'utilisation et qu'il les accepte.

Lieu, date : _____ Signature: