Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF

Bundesamt für Informatik und Telekommunikation BIT Swiss Government PKI

NON CLASSIFIÉ

Conditions contractuelles et d'utilisation pour l'obtention de l'habilitation à émettre des certificats standards de classe C de la Swiss Government PKI des autorités fédérales de la Confédération suisse

V1.0, 04.04.2016

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 figurent l'établissement des certificats standards de classe C, de même que l'octroi des habilitations pour l'émission de tels certificats. L'émission, l'obtention et l'utilisation des certificats standards de classe C de la SG-PKI sont soumises aux conditions contractuelles et d'utilisation mentionnées ci-dessous. Elles 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/00240/00241/06111/index.html?lang=fr.
Les directives de la SG-PKI relatives aux certificats standards de classe C doivent également être respectées. Elles doivent être acceptées séparément lors de la demande d'habilitation à émettre des certificats et lors de chaque modification des autorisations.

Exhaustivité et exactitude des informations

La personne habilitée par le CSP à émettre des certificats standards de classe C (ci-après l'émetteur[2]) s'engage à fournir au CSP en tout temps les informations correctes et complètes, aussi bien pour l'obtention de l'habilitation à émettre des certificats que lors de l'émission des certificats proprement dits, et à communiquer les modifications. L'émetteur doit notamment s'assurer que toutes les informations et les données, ainsi que les adresses électroniques des détenteurs de certificats qui s'adressent à lui sont enregistrées correctement dans l'application prévue à cet effet (actuellement le Certificate Request Wizard, CRW). Il est en outre tenu d'informer le CSP si son rôle ou son domaine de responsabilité se modifie de manière importante.

Protection de l'accès au CRW, des certificats et des clés privées

Les certificats standards de classe C sont établis pour des personnes, des organisations, des systèmes ou des boîtes aux lettres. Les données concernant l'émetteur et les détenteurs des certificats qu'il a établis sont gérées par la SG-PKI. L'émetteur 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 l'application d'émission (CRW). Il doit également garantir le contrôle d'accès, la confidentialité et la protection contre la perte et l'emploi abusif des clés privées et des éventuelles données d'activation qui y sont liées. Le CRW ne peut et ne doit être utilisé qu'aux fins prévues dans le cadre de la demande de certificats et le traitement des certificats établis par l'émetteur et des clés privées correspondantes. Le CRW, les clés privées et les certificats ne doivent en aucun cas être rendus accessibles à des tiers non autorisés. L'émetteur répond de tous les dommages causés par la transmission à des tiers non autorisés des données d'accès au CRW ou de la transmission des clés privées et des éventuels médias et des données d'activation qui y sont liés.
Le CSP se réserve le droit de révoquer sans information préalable l'habilitation pour l'émission de certificats standards de classe C 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 clés privées décrites ci-dessus.

Utilisation du CRW et des certificats

L'émetteur s'engage à utiliser le CRW, les certificats et les clés privées qui s'y rapportent uniquement à des fins autorisées et légales. Il est notamment interdit d'émettre volontairement des certificats contenant des informations fausses ou inexactes. L'émetteur garantit en outre connaître le contenu, le but et l'effet des certificats qu'il établit. Le CRW, les certificats standards de classe C 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.

---

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

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

Compte rendu et révocation

L'émetteur 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 l'émetteur, le détenteur du certificat, le certificat et d'autres informations en rapport direct quand :

- l'émetteur abuse de l'application CRW, fait preuve de négligence ou ne respecte pas les conditions contractuelles et d'utilisation ;
- le certificat ou la personne qui utilise le certificat est identifié comme étant la source d'une utilisation abusive ;
- le détendeur qui demande le certificat ne peut pas être identifié ou vérifié ;
- le certificat a été révoqué pour d'autres motifs que ceux invoqués par l'émetteur ou le détenteur (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), l'émetteur s'engage à prendre contact avec le détenteur du certificat et à entreprendre toutes les démarches raisonnablement exigibles et nécessaires pour mettre immédiatement un terme à l'utilisation du certificat en question.

Fin de l'activité en tant qu'émetteur de certificat

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

Responsabilité

L'émetteur est responsable d'émettre les certificats standards de classe C et les clés privées qui y sont liées 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 standards de classe C et des normes du CA/Browser Forum. Toute infraction à ces dispositions entraîne la révocation des droits d'accès au CRW, la révocation des certificats établis par l'émetteur, ainsi que d'autres mesures administratives et juridiques. L'émetteur est responsable de tous les certificats qu'il a délivrés 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 toutes autres dispositions issues des directives mentionnées.

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 l'émetteur s'il ne les conteste pas dans les 30 jours qui suivent leur communication.

Déclaration de reconnaissance et de consentement

L'émetteur prend connaissance du fait que le CSP révoque irrémédiablement l'habilitation à émettre des certificats à partir 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.).
L'émetteur 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: _____