Ordonnance sur les services de certification électronique (OSCert)

du 12 avril 2000

Le Conseil fédéral suisse,

vu les art. 28, 62 et 64 de la loi du 30 avril 1997 sur les télécommunications (LTC)[1]; vu les art. 10, 14 et 15 de la loi fédérale du 6 octobre 1995 sur les entraves techniques au commerce (LETC)[2],

arrête:

Chapitre 1 Dispositions générales

Art. 1 Objet et but

[1] La présente ordonnance définit, sous la forme d'une réglementation à caractère expérimental, les conditions auxquelles les fournisseurs de services de certification peuvent être reconnus sur une base volontaire et règle leurs activités dans le domaine des certificats électroniques.

[2] Elle vise à promouvoir la fourniture de services de certification électronique sûrs à un large public, à encourager l'utilisation et la reconnaissance juridique des signatures numériques et à permettre la reconnaissance internationale des fournisseurs de services de certification et de leurs prestations.

[3] Sont réservées les dispositions de droit privé relatives à la conclusion des contrats et à la représentation des personnes morales.

Art. 2 Définitions

Au sens de la présente ordonnance, on entend par:

a. *fournisseur de services de certification*: une personne physique ou morale ou une entité de l'administration fédérale, cantonale ou communale qui certifie des informations dans un environnement électronique et qui délivre à cette fin des certificats électroniques;

b. *certificat électronique*: un ensemble de données électroniques établissant le lien entre une clé publique et une personne physique ou morale ou une entité administrative, authentifiées par la signature numérique d'un fournisseur de services de certification;

c. *clé privée*: une clé cryptographique tenue secrète;

RS **784.103**

1 RS **784.10**

2 RS **946.51**

d. *clé publique*: une clé cryptographique correspondant à une clé privée et tenue à la disposition du public;

e. *clé cryptographique*: un paramètre utilisé avec un algorithme mathématique pour transformer, valider, authentifier, chiffrer ou déchiffrer des données;

f. *signature numérique*: un code électronique joint ou lié logiquement à des données électroniques et chiffré au moyen d'une clé privée, qui permet de vérifier, après déchiffrement au moyen de la clé publique correspondante, que les données émanent bien du titulaire de la clé privée et qu'elles n'ont pas été modifiées depuis qu'elles ont été signées;

g. *organisme de reconnaissance*: un organisme de certification accrédité au sens de l'ordonnance du 17 juin 1996 sur l'accréditation et la désignation[3] qui procède à l'évaluation et à la reconnaissance des fournisseurs de services de certification.

Chapitre 2
Reconnaissance des fournisseurs de services de certification

Art. 3 Reconnaissance

1 Peuvent être reconnus les fournisseurs de services de certification qui sont en mesure de délivrer et de gérer les certificats électroniques conformément aux exigences de la présente ordonnance.

2 Les organismes de reconnaissance accrédités dans le domaine couvert par la présente ordonnance sont compétents pour reconnaître les fournisseurs de services de certification.

3 S'il n'existe aucun organisme de reconnaissance, le Service d'accréditation suisse (SAS) de l'Office fédéral de métrologie reconnaît les fournisseurs de services de certification.

Art. 4 Conditions de la reconnaissance

1 Pour être reconnus, les fournisseurs de services de certification doivent remplir les conditions suivantes:

a. être inscrits au registre du commerce ou faire partie d'une unité administrative de la Confédération, d'un canton ou d'une commune;

b. employer du personnel possédant les connaissances, l'expérience et les qualifications nécessaires;

c. utiliser des systèmes et des produits informatiques fiables;

d. posséder des ressources et des garanties financières suffisantes;

e. contracter les assurances nécessaires afin de couvrir leur responsabilité et les frais découlant des mesures prévues à l'art. 15, al. 2 et 3;

3 RS **946.512**

f. s'engager dans leurs conditions générales à répondre, également envers des tiers, des dommages qui découlent d'un certificat électronique erroné ou de la violation d'obligations de publier, à moins qu'ils ne puissent prouver qu'aucune faute ne leur est imputable;

g. assurer le respect du droit applicable en la matière, notamment de la présente ordonnance et de ses dispositions d'exécution.

2 Les conditions sont précisées dans les prescriptions d'exécution.

Art. 5 Liste des fournisseurs de services de certification reconnus

1 Les organismes de reconnaissance annoncent au SAS les fournisseurs de services de certification qu'ils reconnaissent.

2 Le SAS tient à la disposition du public la liste des fournisseurs de services de certification reconnus.

3 Chaque fournisseur de services de certification reconnu publie la liste de tous les autres fournisseurs de services de certification reconnus ainsi que leur clé publique. Il authentifie la liste en y apposant sa signature numérique. Les autres modalités de la publication sont réglées dans les prescriptions d'exécution.

Chapitre 3 Exigences essentielles

Section 1 Génération et utilisation des clés cryptographiques

Art. 6

Les questions liées à la génération des clés cryptographiques pouvant faire l'objet de certificats électroniques au sens de la présente ordonnance ainsi qu'à la création et à la vérification de la signature numérique sont réglées dans les prescriptions d'exécution. Celles-ci visent à assurer un degré élevé de sécurité en fonction de l'évolution technique.

Section 2 Certificats électroniques

Art. 7

1 Tout certificat électronique délivré au sens de la présente ordonnance doit comporter au moins les informations suivantes:

a. son numéro de série;

b. la mention qu'il est délivré au sens de la présente ordonnance;

c. la mention des éventuelles limites fixées à son utilisation;

d. le nom du titulaire de la clé publique qui est certifiée ainsi que la mention qu'il s'agit d'une personne physique, d'une personne morale, d'une entité administrative ou, le cas échéant, d'un pseudonyme;

e. la clé publique certifiée;

f. sa durée de validité;

g. le nom et la signature numérique du fournisseur de services de certification qui le délivre.

2 Le format des certificats est réglé dans les prescriptions d'exécution.

Section 3 Fournisseurs de services de certification

Art. 8 Délivrance des certificats électroniques

1 Les fournisseurs de services de certification reconnus doivent exiger des personnes qui demandent un certificat électronique qu'elles établissent leur identité et leurs pouvoirs en se présentant personnellement, munies des documents suivants:

a. une carte d'identité ou un passeport pour les personnes physiques;

b. une procuration et une carte d'identité ou un passeport pour les personnes agissant pour des entités administratives;

c. un extrait du registre du commerce et la carte d'identité ou le passeport des personnes habilitées à agir au nom des personnes morales.

2 Lorsqu'une personne ou une entité administrative identifiée selon l'al. 1 depuis moins de dix ans demande un nouveau certificat électronique, les fournisseurs de services de certification reconnus peuvent accepter une demande munie de la signature numérique apposée au moyen de la clé privée correspondant à la clé publique faisant l'objet du certificat à renouveler.

3 Sur demande, ils font figurer dans le certificat électronique un pseudonyme en lieu et place du nom du titulaire de la clé publique certifiée. L'identité de ce dernier doit être établie conformément aux al. 1 et 2.

Art. 9 Obligation d'informer

1 Les fournisseurs de services de certification reconnus doivent tenir à la disposition du public leurs conditions contractuelles générales ainsi que des informations sur leur politique de certification.

2 Ils doivent informer leurs clients des conséquences de la divulgation ou de la perte de leur clé privée, au plus tard lors de la délivrance des certificats électroniques. Ils doivent leur indiquer les mesures appropriées pour maintenir leur clé secrète.

Art. 10 Conservation des clés privées

Les fournisseurs de services de certification reconnus ne peuvent pas conserver de copies des clés privées de leurs clients.

Art. 11 Annulation des certificats électroniques

[1] Les fournisseurs de services de certification reconnus annulent immédiatement les certificats électroniques à la demande de leurs titulaires.

[2] Ils doivent s'assurer que la personne qui demande l'annulation est légitimée à le faire. Cette exigence est réputée satisfaite lorsque la demande est munie de la signature numérique apposée au moyen de la clé privée correspondant à la clé publique faisant l'objet du certificat à annuler.

[3] Les fournisseurs de services de certification reconnus sont tenus d'annuler immédiatement les certificats électroniques qu'ils ont délivrés s'il s'avère que ceux-ci ont été obtenus de manière frauduleuse ou qu'ils ne permettent plus de garantir le lien entre une personne ou une entité administrative et une clé publique.

[4] Ils peuvent suspendre provisoirement les certificats électroniques pour une durée maximale de trois jours. A l'échéance de ce délai, ils annulent définitivement les certificats ou rétablissent leur validité. Dans le premier cas, l'annulation prend effet au moment où le certificat a été suspendu; dans le second cas, la suspension n'a pas d'effet sur la validité du certificat.

[5] Les fournisseurs de services de certification reconnus informent sans délai les titulaires des certificats électroniques de l'annulation ou de la suspension de ces derniers.

Art. 12 Annuaire des certificats électroniques et liste des certificats annulés ou suspendus

[1] Les fournisseurs de services de certification reconnus tiennent un annuaire des certificats électroniques qu'ils délivrent, dans lequel leurs clients peuvent faire inscrire leurs certificats électroniques.

[2] Ils doivent tenir à jour une liste de tous les certificats annulés ou suspendus, même s'ils n'ont pas été inscrits dans l'annuaire. Cette liste mentionne uniquement le numéro de série du certificat électronique, la mention qu'il est annulé ou suspendu, ainsi que la date et l'heure de l'annulation ou de la suspension. Elle est authentifiée par la signature numérique du fournisseur de services de certification reconnu.

[3] Les fournisseurs de services de certification reconnus doivent en tout temps garantir aux tiers l'accès en ligne à l'annuaire des certificats électroniques et à la liste des certificats annulés ou suspendus, sans autres frais que ceux découlant de l'utilisation de moyens de télécommunication publics.

[4] Les modalités relatives à la tenue des annuaires de certificats électroniques et des listes de certificats annulés ou suspendus ainsi qu'à l'accès aux annuaires et aux listes sont réglées dans les prescriptions d'exécution.

Art. 13 Conservation des certificats électroniques

[1] Les fournisseurs de services de certification reconnus doivent conserver les certificats électroniques échus ou annulés ainsi que les listes de certificats annulés et permettre leur consultation pendant onze ans à partir de l'échéance ou de l'annulation des certificats.

2 Durant les six premières années, la consultation doit être en tout temps garantie en ligne et sans autres frais que ceux découlant de l'utilisation de moyens de télécommunication publics.

Art. 14 Journal des activités

1 Les fournisseurs de services de certification reconnus consignent dans un journal les activités relatives à la délivrance, à l'annulation et à la suspension des certificats électroniques.

2 Ils conservent les inscriptions dans le journal ainsi que les pièces justificatives correspondantes aussi longtemps qu'ils doivent conserver le dernier certificat renouvelé selon l'art. 8, al. 2.

Art. 15 Cessation d'activité

1 Les fournisseurs de services de certification reconnus annoncent au SAS 30 jours à l'avance qu'ils vont cesser leur activité. Ils lui annoncent sans délai une comination de faillite qui leur a été notifiée.

2 En cas de cessation volontaire d'activité, les fournisseurs de services de certification reconnus doivent annuler les certificats électroniques non échus qu'ils ont délivrés. Le SAS charge un autre fournisseur de services de certification reconnu de tenir la liste des certificats annulés et de conserver les certificats échus ou annulés, le journal des activités et les pièces justificatives correspondantes.

3 En cas de faillite d'un fournisseur de services de certification reconnu, le SAS charge un autre fournisseur de services de certification reconnu d'annuler les certificats électroniques non échus qu'il a délivrés, de tenir la liste des certificats annulés et de conserver les certificats échus ou annulés, le journal des activités et les pièces justificatives correspondantes.

Art. 16 Protection des données

1 Les fournisseurs de services de certification reconnus ne peuvent collecter et traiter que les données personnelles qui sont nécessaires à l'accomplissement de leurs tâches.

2 Par ailleurs, la législation sur la protection des données est applicable.

Chapitre 4
Surveillance des fournisseurs de services de certification reconnus

Art. 17

1 La surveillance des fournisseurs de services de certification reconnus est assurée par les organismes de reconnaissance selon les règles du droit de l'accréditation.

2 Lorsqu'un organisme de reconnaissance retire la reconnaissance d'un fournisseur de services de certification, il l'annonce immédiatement au SAS. L'art. 15, al. 3, est applicable.

Chapitre 5
Reconnaissance des fournisseurs de services de certification étrangers

Art. 18

Le SAS tient à la disposition du public la liste des fournisseurs de services de certification étrangers reconnus dans le cadre des accords internationaux conclus par le Conseil fédéral en vertu de l'art. 14 LETC.

Chapitre 6
Attestation de la conformité d'une signature numérique avec la présente ordonnance

Art. 19

1 Sur demande et contre paiement d'un émolument, le SAS atteste par écrit que la signature numérique figurant sur un document électronique a bien été apposée au moyen de la clé privée correspondant à une clé publique qui a fait l'objet d'un certificat électronique délivré par un fournisseur de services de certification reconnu et que ce certificat était valable à un moment donné.

2 Le Département fédéral de justice et police fixe le montant de l'émolument.

3 Les attestations au sens de l'al. 1 peuvent également être fournies par d'autres organismes pour autant qu'ils disposent des qualifications nécessaires.

Chapitre 7 Dispositions finales

Art. 20 Exécution

L'Office fédéral de la communication édicte les prescriptions d'exécution prévues par la présente ordonnance, en collaboration avec l'Unité de stratégie informatique de la Confédération et le SAS. Il tient compte des normes et dispositions internationales dans ce domaine.

Art. 21 Entrée en vigueur et durée de validité

1 La présente ordonnance entre en vigueur le 1er mai 2000.

2 Elle a effet jusqu'à l'entrée en vigueur d'une loi en la matière, mais au plus tard jusqu'au 31 décembre 2009.

12 avril 2000 Au nom du Conseil fédéral suisse:

Le président de la Confédération, Adolf Ogi
La chancelière de la Confédération, Annemarie Huber-Hotz