Projet d'ordonnance sur les services de certification dans le domaine de la signature électronique (OSCSE)

Explications

Généralités

La loi fédérale du 19 décembre 2003 sur les services de certification dans le domaine de la signature électronique (SCSE; FF 2003 7493) reprend l'essentiel des dispositions de l'ordonnance du 12 avril 2000 sur les services de certification électronique (OSCert; RS 784.103). Le projet de nouvelle ordonnance sur les services de certification dans le domaine de la signature électronique (OSCSE) maintient en règle générale les dispositions non reprises au niveau de la loi, donne suite aux divers mandats du législateur et précise au besoin la portée des dispositions légales. Pour l'essentiel, la structure de l'ordonnance suit celle de la loi.

Reconnaissance des fournisseurs de services de certification

Art. 1 Reconnaissance

En exécution de l'art. 4 SCSE, cette disposition reprend le système actuel. Le SAS accrédite les organismes qui ont qualité pour reconnaître les fournisseurs de services de certification (FSC) selon le système général de l'accréditation. A l'image de ce que prévoit aujourd'hui l'OSCert (art. 3, al. 3), il incombe au SAS de reconnaître les FSC s'il n'existe aucun organisme de reconnaissance accrédité. Cette solution est toutefois susceptible d'engendrer des conflits de compétence au sein du SAS par le cumul des fonctions d'organe d'accréditation et d'organe de reconnaissance. C'est pourquoi il est envisagé de modifier l'art. 1, al. 2, et de confier la tâche de reconnaissance à une autre autorité telle que l'OFCOM.

Art. 2 Conditions de la reconnaissance

Les FSC répondent du dommage causé lorsqu'ils contreviennent aux obligations légales (art. 16 SCSE). Ils ne peuvent certes pas exclure leur responsabilité, mais ils ne répondent que jusqu'à concurrence de la valeur des transactions indiquée sur le certificat (art. 16, al. 3, en relation avec l'art. 7, al. 2, let. c, SCSE). Le même certificat peut créer une multitude de dommages qui, cumulés, peuvent représenter un montant important. D'où la nécessité de garanties financières suffisantes permettant de couvrir la responsabilité du FSC.

En complément aux dispositions de la SCSE, l'ordonnance fixe le montant minimum qui doit être pris en charge par l'assurance du FSC, aussi bien par cas que par année d'assurance. Cela devrait contribuer à l'émergence d'un marché de l'assurance des risques liés à la certification électronique tout en garantissant une protection suffisante des titulaires et des utilisateurs de certificats électroniques. Par cas d'assurance, il faut entendre l'ensemble des dommages qui résultent de la violation d'une ou plusieurs de ses obligations par le FSC. Un cas d'assurance peut comprendre plusieurs dommages. Le dommage déterminant est celui subi dans le cadre d'une transaction au sens de l'art. 7, al. 2, let. c, SCSE.

Par ailleurs, l'ordonnance permet au FSC qui entend se faire reconnaître de produire une garantie financière équivalente au lieu de conclure une assurance. Cette garantie doit au moins couvrir la responsabilité du FSC jusqu'à concurrence des mêmes montants que ceux

prévus pour l'assurance. Cela peut être une garantie bancaire ou toute autre garantie financière équivalente.

Elaboration et utilisation des clés de signature et de vérification de signature

Art. 3

Selon l'art. 6, al. 1, SCSE, le Conseil fédéral règle l'élaboration des clés de signature et de vérification de signature pouvant faire l'objet de certificats qualifiés. La présente disposition fixe les critères déterminants, à savoir la longueur des clés et l'algorithme utilisé pour leur élaboration. Compte tenu de l'évolution de la technique, l'OFCOM est chargé de régler les détails. En application de l'art. 20, al. 2, SCSE, il reçoit également le mandat de mettre en œuvre l'art. 6, al. 2, SCSE (exigences relatives aux dispositifs de création de signature). Il pourra également, au besoin, préciser les exigences relatives au processus de vérification de la signature mentionnées à l'art. 6, al. 3, SCSE.

Certificats qualifiés

Art. 4

Selon l'art. 7, al. 3, SCSE, le Conseil fédéral règle le format des certificats. S'agissant d'une question éminemment technique, il confie cette tâche à l'OFCOM sur la base de l'art. 20, al. 2, SCSE (sous-délégation).

Devoirs des fournisseurs reconnus

Art. 5 Délivrance des certificats qualifiés

Selon l'art. 8, al. 2, SCSE, le Conseil fédéral détermine les documents de nature à prouver l'identité et, le cas échéant, les qualités des personnes qui demandent un certificat et peut, à certaines conditions, prévoir l'exemption de l'obligation de se présenter en personne. Le projet d'ordonnance reprend pour l'essentiel la réglementation actuelle. Comme des personnes morales ne peuvent plus être titulaires de certificats qualifiés, il convient de préciser quel genre de documents doivent produire les titulaires de clés de signature disposant de qualités spécifiques, telle que la qualité de représenter une personne morale déterminée (cf. al. 1, let. b).

L'al. 2 correspond à l'art. 8, al. 2, OSCert à la différence près que le délai d'exemption de l'obligation de se présenter en personne a été réduit de dix à six ans. Quant à l'al. 3, il précise, comme aujourd'hui, que l'identité d'une personne qui fait figurer dans le certificat un pseudonyme en lieu et place de son nom doit être établie selon les al. 1 et 2.

Art. 6 Conservation des clés de signature

Cette disposition correspond à la réglementation actuelle (cf. art. 10 OSCert). Elle répond à un souci de sécurité reconnu.

Art. 7 Annulation des certificats qualifiés

L'al. 1 reprend l'art. 11, al. 2, OSCert. La vérification de la validité des certificats qualifiés doit en outre pouvoir se faire par un accès en ligne aux informations relatives aux certificats annulés que les FSC doivent enregistrer et mettre à la disposition du public (al. 2 et 3).

Art. 8 Service d'annuaire pour les certificats qualifiés

L'offre d'un service d'annuaire des certificats qualifiés n'est désormais plus obligatoire (cf. art. 11, al. 2, SCSE). Lorsqu'une telle prestation est fournie volontairement, elle doit toutefois répondre aux exigences fixées par l'OFCOM (al. 1).

Selon l'art. 11, al. 4, SCSE, le Conseil fédéral détermine la durée minimale pendant laquelle doit demeurer possible la vérification des certificats qualifiés qui ne sont plus valables. La réglementation proposée (al. 2) reprend le délai de onze ans figurant à l'art. 13 OSCert, qui correspond au délai de prescription général de l'art. 127 du Code des obligations (CO) et au délai de conservation des livres de l'art. 962 CO.

Art. 9 Journal des activités

Selon l'art. 9, al. 3, SCSE, il incombe au Conseil fédéral de régler la durée pendant laquelle le journal et les documents qui s'y rapportent doivent être conservés. Le délai de onze ans de l'art. 8, al. 2, s'impose ici également.

Art. 10 Cessation d'activité

L'al. 1 précise par rapport à la loi que l'annonce d'une cessation d'activité doit se faire 30 jours à l'avance. Quant à l'al. 2, il règle, en application de l'art. 13, al. 2, SCSE, le cas où il n'existe aucun autre FSC reconnu pour reprendre les tâches du fournisseur qui cesse son activité. Celles-ci incomberont à l'organisme qui a reconnu ce dernier fournisseur.

Responsabilité en matière de clé de signature : mesures de sécurité

L'art. 59*a*, al. 3, CO charge le Conseil fédéral d'arrêter les mesures de sécurité que doit prendre le titulaire d'une clé de signature pour éviter d'être responsable d'une utilisation abusive de cette dernière. Il s'agit de tenir compte du fait que ce risque de responsabilité ne se concrétise que dans le contexte de la signature électronique (avancée) décrite dans la SCSE. Cela signifie que le dispositif de création de signature doit être conçu de manière à ce que le titulaire puisse protéger la clé de signature de manière fiable contre toute utilisation abusive (art. 6, al. 2, let. c, SCSE). A l'heure actuelle, cela implique que le titulaire dépose la clé de signature sur du matériel informatique (Smartcard, Token) qu'il peut plus ou moins aisément conserver sous clé.

Il convient également de signaler le sens de l'art. 59*a*, al. 3, CO. Le législateur a choisi cette solution afin que les mesures de sécurité exigées du titulaire d'une clé de signature demeurent raisonnables. Ce but ne pourrait que difficilement être atteint s'il revenait aux fournisseurs de services de certification de définir ces mesures. Lors de la rédaction de l'ordonnance, le souci du législateur doit donc être pris en considération.

Art. 11 Clé de signature

Prenons deux situations extrêmes. Dans l'un des cas, le titulaire d'une clé de signature confie cette dernière à un tiers. Qu'il assume ensuite toute responsabilité subséquente est incontesté. Dans l'autre cas, le titulaire se fait prendre la clé de signature par la force. Qu'il n'assume aucune responsabilité en ce cas est également incontesté. Mais où se situe la limite ?

Il est exigé du titulaire d'une clé de signature qu'il la porte sur lui ou la mette sous clé, pour autant qu'il puisse raisonnablement le faire. On tient ainsi compte du fait qu'une clé de signature, notamment dans un environnement familier, n'est pas toujours hors de la portée de tiers, sans que cela puisse pour autant être reproché au titulaire.

Art. 12 Mot de passe

Il faut savoir que, précisément dans le contexte professionnel, le matériel informatique comportant la clé de signature est assez facilement accessible, mais qu'une protection par un mot de passe permet d'empêcher un usage abusif de cette clé.

L'al. 2 interdit à une personne qui s'appellerait Felix Muster d'utiliser felixmuster ou musterfelix comme mot de passe. Si elle est née le 30 mars 1960, cette personne ne peut pas non plus employer la combinaison de chiffres 30031960, 30196003 ou 19603003, 19600330, 0330160 ou encore 03196003.

Aucune obligation n'a été établie pour que le mot de passe ou la combinaison de chiffres soient régulièrement modifiés. D'une part, il ne serait pas possible de contrôler le respect d'une telle obligation. D'autre part, le changement d'un mot de passe n'augmente la sécurité que sous certaines conditions; en effet, même un mot de passe modifié le jour précédent peut être épié puis utilisé de manière abusive.

Il n'est pas non plus interdit de noter les mots de passe ou les combinaisons de chiffres, mais il faut toujours veiller à ce que ces relevés soient aussi mis sous clé (al. 3).

Au cours de la discussion sur la fiabilité des signatures électroniques, il est régulièrement exigé que l'accès à la signature électronique soit garanti de manière biométrique. Il convient de tenir compte de cet élément dans la mesure où l'accès au matériel informatique, et donc à la clé de signature, peut être protégé par un procédé biométrique. Dans un tel cas, la biométrie revêt la même fonction qu'un mot de passe. L'ordonnance se contente du principe de base, sans débattre de la question de savoir à quel moment un procédé biométrique atteint un degré de fiabilité suffisant (al. 4).

Conserver séparément la clé de signature et le mot de passe ou la combinaison de chiffres constitue la mesure la plus efficace pour éviter une utilisation abusive de la signature électronique (al. 5). Si le titulaire de la clé de signature observe cette mesure, un abus est pratiquement exclu; certes, on peut aussi ici se demander ce qu'on entend par "conserver séparément". Ce ne sera manifestement pas le cas lorsque la clé de signature et le mot de passe ou la combinaison de chiffres sont rangés dans le même porte-monnaie ou le même tiroir.

Art. 13 Annonce en cas de perte

L'annonce de la perte d'une clé de signature et donc la nécessité d'annuler le certificat sont en principe incontestées. Toutefois, il est évident qu'une telle annonce ne peut être demandée que si elle est possible et raisonnablement exigible. Ce n'est ainsi pas le cas

lorsque la victime se trouve à l'hôpital suite à un accident et qu'elle a d'autres soucis que de procéder à l'annulation de son certificat. Il conviendrait cependant de se demander s'il faut se contenter du simple principe de l'"annonce immédiate" ou s'il s'agit de fixer un délai minimum. Ce dernier s'impose en définitive dans le sens d'une plus grande sécurité juridique. Il est fixé à 24 heures à compter du moment où le titulaire s'est rendu compte de la perte de sa clé de signature.

Dispositions finales

Art. 14 Exécution

En application de l'art. 20, al. 2, SCSE, l'OFCOM est chargé d'édicter les prescriptions techniques et administratives nécessaires. Les actuelles prescriptions (RS 784.103.1) doivent être révisées pour tenir compte des développements intervenus ces dernières années dans le domaine de la normalisation.

Art. 15 Abrogation du droit en vigueur

L'ordonnance actuelle, qui n'a qu'une durée de validité limitée (cf. art. 21, al. 2, OSCert), est formellement abrogée.

Art. 16 Entrée en vigueur

La loi, l'ordonnance et les prescriptions techniques et administratives entreront en vigueur simultanément le 1er janvier 2005.

OFCOM/01.06.2004