Ordonnance sur les services de certification dans le domaine de la signature électronique et des autres applications des certificats numériques

(Ordonnance sur la signature électronique, OSCSE)

du 23 novembre 2016 (État le 2 octobre 2020)

Le Conseil fédéral suisse,

vu les art. 4, 6, al. 1, 7, al. 4, 9, al. 4, 10, al. 3, 12, al. 4, 14, al. 2, et 21 de la loi fédérale du 18 mars 2016 sur la signature électronique (SCSE)[1],
vu l'art. 59*a*, al. 3, du code des obligations[2],

arrête:

Art. 1 Organismes de reconnaissance

[1] Le Service d'accréditation suisse (SAS) du Secrétariat d'État à l'économie accrédite les organismes de reconnaissance des fournisseurs de services de certification conformément aux dispositions de l'ordonnance du 17 juin 1996 sur l'accréditation et la désignation[3].

[2] S'il n'existe aucun organisme de reconnaissance accrédité, c'est l'Office fédéral de la communication (OFCOM) qui reconnaît les fournisseurs de services de certification (fournisseurs).

Art. 2 Assurance

[1] Le fournisseur qui entend se faire reconnaître doit conclure une assurance responsabilité civile pour un montant d'au moins 2 millions de francs par cas d'assurance et 8 millions de francs par année d'assurance.

[2] En lieu et place d'une assurance, il peut produire une garantie équivalente.

Art. 3 Élaboration, stockage et utilisation de clés cryptographiques

[1] La longueur des clés et l'algorithme utilisé doivent être à même de résister à des attaques cryptographiques durant la période de validité du certificat réglementé.

[2] L'OFCOM règle les modalités dans les prescriptions techniques et administratives et fixe les exigences applicables aux systèmes d'élaboration, de stockage et d'utilisation des clés cryptographiques privées.

RO **2016** 4667
1 RS **943.03**
2 RS **220**
3 RS **946.512**

Art. 4 Certificats réglementés

1 L'OFCOM règle le format des certificats réglementés pour les applications suivantes:

a. la signature électronique d'une personne physique ou le cachet électronique d'une entité IDE au sens de l'art. 3, al. 1, let. c, de la loi fédérale du 18 juin 2010 sur le numéro d'identification des entreprises (LIDE)[4];

b. l'identification électronique d'une telle personne ou entité;

c. le chiffrement de données électroniques.

2 Les certificats réglementés qui contiennent la mention que leur titulaire peut, par sa signature électronique, s'obliger ou obliger l'entité IDE qu'il représente ne peuvent être délivrés qu'à des personnes physiques.

Art. 5 Délivrance des certificats réglementés à des personnes physiques

1 Les fournisseurs reconnus doivent exiger des personnes qui demandent un certificat réglementé qu'elles présentent personnellement un passeport, une carte d'identité suisse ou une carte d'identité reconnue pour entrer en Suisse.

2 Lorsque des qualités spécifiques (art. 7, al. 3, let. a, SCSE), des pouvoirs de représentation ou l'entité IDE représentée (art. 7, al. 3, let. b, SCSE) sont inscrits au registre du commerce, les fournisseurs reconnus doivent exiger la production d'un extrait de celui-ci, actuel et certifié conforme. Les qualités spécifiques et les pouvoirs de représentation mentionnés dans l'extrait ne requièrent ni confirmation de l'organisme compétent ni approbation de l'identité IDE représentée au sens de l'art. 9, al. 2 et 3, SCSE.

3 Les fournisseurs reconnus doivent s'assurer que les inscriptions dans le certificat ne sont pas contraires à celles du registre du commerce. En particulier, pour une personne qui, d'après le registre du commerce, est habilitée à représenter une entité juridique ou qui y exerce une fonction, ils ne peuvent mentionner dans le certificat, par rapport à l'entité juridique concernée, que les mêmes pouvoirs de représentation ou la même fonction.

4 Lorsque l'entité IDE représentée est inscrite au registre du commerce, l'approbation de la mention dans le certificat de pouvoirs de représentation non inscrits au registre du commerce doit être signée par une personne habilitée à représenter l'entité IDE selon le registre du commerce.

5 Les fournisseurs reconnus vérifient en outre les données relatives aux caractères clés de l'entité IDE représentée en consultant le registre IDE (art. 11, al. 1, LIDE[5]). Si l'entité IDE n'a pas donné son accord à la publication de ses données relatives aux caractères clés (art. 11, al. 3, LIDE), ils doivent exiger la présentation d'un extrait du registre IDE actuel et certifié conforme.

6 Les al. 1 à 5 s'appliquent également à la délivrance d'un certificat réglementé à une personne physique utilisant un pseudonyme.

4 RS **431.03**
5 RS **431.03**

Art. 6 Délivrance des certificats réglementés à des entités IDE autres que des personnes physiques

1 L'identité de la personne qui demande la délivrance d'un certificat réglementé pour une entité IDE qui n'est pas une personne physique doit être vérifiée conformément à l'art. 5, al. 1. Les pouvoirs de représentation de cette personne doivent être justifiés par une procuration écrite, à moins qu'ils ne soient inscrits dans le registre du commerce.

2 Les fournisseurs reconnus doivent vérifier les données relatives aux caractères clés de l'entité IDE en consultant le registre IDE (art. 11, al. 1, LIDE[6]). Si l'entité IDE n'a pas donné son accord à la publication de ses données relatives aux caractères clés (art. 11, al. 3, LIDE), ils doivent exiger la présentation d'un extrait du registre IDE actuel et certifié conforme.

3 Lorsque l'entité IDE est inscrite au registre du commerce, la production d'un extrait de celui-ci, actuel et certifié conforme, doit être exigée.

Art. 7 Dispense de l'obligation de se présenter en personne

1 L'identité d'une personne qui demande un certificat réglementé peut être établie à distance à condition qu'un organisme d'évaluation de la conformité ait confirmé que la méthode d'identification utilisée fournit une garantie équivalente à la présence en personne.

2 Les fournisseurs reconnus peuvent délivrer des certificats réglementés dans le cadre d'un processus de vérification d'identité par le biais d'une communication audiovisuelle en temps réel répondant aux exigences de la loi du 10 octobre 1997 sur le blanchiment d'argent[7]. Les certificats ainsi délivrés ne peuvent être utilisés que dans le cadre des relations entre leurs titulaires et les intermédiaires financiers qui ont vérifié leur identité.

3 Les fournisseurs reconnus peuvent accepter une demande munie d'une signature électronique qualifiée pour la délivrance d'un certificat réglementé:

a. à une entité IDE qui n'est pas une personne physique, pour autant que les pouvoirs de représentation du requérant soient inscrits dans un registre public;

b. à une personne physique sans qualités spécifiques ni pouvoirs de représentation, pour autant que cette personne ait déjà été identifiée par le fournisseur conformément à l'art. 5 ou aux al. 1 et 2 du présent article.

6 RS **431.03**
7 RS **955.0**

Art. 7*a*[8]

Art. 8 Copie et conservation de doubles des clés

Les fournisseurs reconnus peuvent établir et conserver des doubles des clés cryptographiques privées de leurs clients, sauf si celles-ci servent à la signature électronique et sont stockées dans des dispositifs de création de signatures en possession des clients.

Art. 9 Annulation des certificats réglementés

1 Les fournisseurs reconnus informent leurs clients sur la manière de demander l'annulation des certificats réglementés. Ils doivent être en mesure de recevoir les demandes d'annulation en tout temps.

2 Ils doivent garantir aux tiers l'accès en ligne aux informations relatives à l'annulation d'un certificat réglementé jusqu'à l'expiration de la validité de ce dernier. Ces informations comprennent le numéro de série du certificat, la mention qu'il est annulé, ainsi que la date et l'heure de l'annulation. Elles doivent être authentifiées par le cachet électronique réglementé du fournisseur reconnu.

3 Les fournisseurs reconnus doivent être en mesure de fournir les informations permettant la vérification des certificats réglementés qui ne sont plus valables pendant onze ans à partir de l'échéance des certificats.

Art. 10 Horodatage électronique qualifié

L'OFCOM détermine les exigences auxquelles doivent satisfaire les fournisseurs reconnus pour procéder à un horodatage électronique qualifié.

Art. 11 Journal des activités

1 Les fournisseurs reconnus conservent les inscriptions relatives à leurs activités ainsi que les pièces justificatives correspondantes pendant onze ans.

2 Pour les activités relatives aux certificats, le délai commence à courir à partir de l'échéance de ces derniers.

3 Pour les certificats qui ont été émis en application de l'art. 7, al. 3, let. b, les inscriptions et les pièces justificatives relatives à l'identification de leurs titulaires selon les art. 5 et 7, al. 1 et 2, doivent être conservées jusqu'au terme du délai de onze ans qui s'applique au dernier des certificats ainsi établis.

Art. 12 Cessation d'activité

1 Les fournisseurs reconnus annoncent immédiatement, mais au moins 30 jours à l'avance, au SAS et à l'organisme de reconnaissance qu'ils vont cesser leur activité.

8 Introduit par le ch. I de l'O du 1er avril 2020, en vigueur du 2 avril au 1er octobre 2020 (RO **2020** 1149).

2 Lorsqu'il n'existe aucun autre fournisseur reconnu auquel le SAS pourrait transférer les tâches conformément à l'art. 14, al. 2, SCSE, l'OFCOM se charge des tâches suivantes:

a. il continue de traiter les demandes d'annulation des certificats réglementés;

b. il garantit aux tiers l'accès en ligne aux informations relatives à l'annulation des certificats réglementés jusqu'à l'échéance de ces derniers;

c. il tient à jour et conserve le journal des activités et les pièces justificatives correspondantes.

3 Il peut annuler de lui-même les certificats encore valables.

Art. 13 Mesures de sécurité

1 Le titulaire d'un certificat réglementé doit conserver l'accès exclusif à la clé cryptographique utilisée pour créer une signature ou un cachet électronique. Dans la mesure de ce qui peut être exigé, il doit garder le dispositif de création de signature ou de cachet en sa possession ou le mettre en lieu sûr.

2 En cas de perte ou de vol du dispositif de création de signature ou de cachet, le titulaire d'un certificat réglementé doit demander l'annulation de ce dernier dans les meilleurs délais. Il en va de même pour le titulaire qui sait ou qui a des raisons de croire qu'un tiers a pu avoir accès à la clé cryptographique utilisée pour créer une signature ou un cachet électronique.

3 Les données d'activation du dispositif de création de signature ou de cachet ne doivent pas se référer à des données relatives à la personne ou à l'entité IDE titulaire d'un certificat réglementé.

4 Les transcriptions des données d'activation doivent être conservées en lieu sûr et séparément du dispositif de création de signature ou de cachet.

5 Le titulaire d'un certificat réglementé doit modifier les données d'activation du dispositif de création de signature ou de cachet lorsqu'il sait ou qu'il a des raisons de croire qu'un tiers en a eu connaissance. S'il ne peut pas lui-même modifier les données d'activation, il doit demander l'annulation du certificat dans les meilleurs délais.

Art. 14 Registre du commerce

1 Les art. 8, al. 5, 9, al. 4, et 166 de l'ordonnance du 17 octobre 2007 sur le registre du commerce[9] demeurent réservés en ce qui concerne la conservation des pièces justificatives relatives aux certificats réglementés délivrés à des personnes disposant de qualités spécifiques ou de pouvoirs de représentation inscrits au registre du commerce.

2 Seules les inscriptions du registre du commerce font foi des qualités spécifiques et des pouvoirs de représentation des personnes titulaires de certificats réglementés.

9 RS **221.411**

Art. 15 Exécution

L'OFCOM édicte les prescriptions techniques et administratives nécessaires. Il tient compte du droit international pertinent et peut déclarer applicables des normes techniques internationales.

Art. 16 Abrogation et modification d'autres actes

L'abrogation et la modification d'autres actes sont réglées en annexe.

Art. 17 Dispositions transitoires

[1] Les certificats qualifiés délivrés avant le 1er janvier 2017 restent valables jusqu'à leur échéance, mais au plus tard jusqu'au 31 décembre 2019.

[2] Les fournisseurs reconnus selon l'ancien droit peuvent délivrer des certificats réglementés au sens du nouveau droit jusqu'à ce qu'ils aient été reconnus selon le nouveau droit ou que la reconnaissance leur ait été retirée, mais au plus tard jusqu'au 31 décembre 2018. Jusqu'à l'obtention de la nouvelle reconnaissance, la durée de validité des certificats réglementés qu'ils délivrent ne peut excéder le 31 décembre 2019.

Art. 18 Entrée en vigueur

La présente ordonnance entre en vigueur le 1er janvier 2017.

Annexe
(art. 16)

Abrogation et modification d'autres actes

I

L'ordonnance du 3 décembre 2004 sur la signature électronique[10] est abrogée.

II

Les ordonnances mentionnées ci-après sont modifiées comme suit:

…[11]

10 [RO **2004** 5101, **2011** 3457]
11 Les mod. peuvent être consultées au RO **2016** 4667.