Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP
Office fédéral de la justice OFJ

Révision totale de la loi du 19 décembre 2003 sur la signature électronique (SCSE)

Rapport explicatif relatif à l'avant-projet de loi destiné à la consultation

1 Partie générale

1.1 Contexte

Dès son adoption, la loi du 19 décembre 2003 sur la signature électronique (SCSE ; RS 943.03) avait déjà fait l'objet de critiques, certains estimant que la solution proposée en ce qui concerne la signature électronique reconnue n'était pas adaptée aux opérations de masse.

Suite à la motion Baumann du 3 octobre 2008 (08.3741 ; Certification obligatoire contraire au droit dans l'ordonnance relative à la loi sur la TVA), le Département fédéral de justice et police (DFJP) a chargé l'Office fédéral de la justice (OFJ) de procéder à un examen approfondi visant à évaluer la nécessité de réviser la SCSE, le but étant de s'assurer que cette loi contribue à une mise en œuvre réussie de la stratégie du Conseil fédéral pour une société de l'information en Suisse.

Une analyse a ensuite été réalisée afin de déterminer si des mesures devaient être prises. Le bilan de cette analyse est présenté dans le « rapport du groupe de travail interdépartemental sur les résultats du mandat d'examen relatif à la mise en œuvre de la stratégie du Conseil fédéral pour une société de l'information en Suisse : consolidation des bases légales » (voir chap. 3.3.3), qui a été rédigé par le groupe de travail interdépartemental constitué à cette occasion. Le Conseil fédéral a pris acte de ce rapport le 11 juin 2010 et chargé le DFJP d'examiner les mesures législatives devant être prises afin de pouvoir mettre en œuvre cette stratégie.

Il ressort de cet examen qu'une réglementation relative à l'utilisation de la signature par les personnes morales et les autorités ainsi qu'à l'authentification s'avère indispensable dans les secteurs économiques et administratifs et qu'il règne une grande insécurité juridique concernant la manière de procéder avec les documents signés au moyen d'une signature électronique.

Par décision du 27 juin 2011, le Conseil fédéral a confié au DFJP le mandat de lui soumettre début 2012 un avant-projet de loi sur la signature électronique et un rapport explicatif prêts à être envoyés en consultation.

Enfin, le Conseil fédéral a chargé le DFJP le 28 mars 2012 d'examiner l'ensemble des éléments devant figurer dans une législation exhaustive sur la signature électronique et de lui soumettre d'ici la fin de l'année 2012 une proposition sur la suite à donner à ce dossier. Le DFJP devra notamment élaborer une réglementation sur les « écrits électroniques simples » et voir comment inscrire dans la loi le droit de communiquer des écrits par la voie électronique. Il devra par ailleurs étudier les différentes possibilités d'abaisser les exigences auxquelles doit satisfaire la signature électronique qualifiée pour être reconnue comme équivalente à la signature manuscrite. La complexité de la procédure a en effet été décriée à plusieurs reprises. Ce rapport traitera également de cet aspect.

1.2 Objectifs de la révision

Voici les trois principaux objectifs de la révision qui nous occupe ici :

- Premièrement, introduire dans la loi une nouvelle forme de signature électronique qui vienne compléter la signature électronique qualifiée et qui puisse donc être utilisée non plus seulement par les personnes physiques mais aussi par les personnes morales et les autorités, et qui soit soumise à des prescriptions techniques pouvant éventuellement faire l'objet d'adaptations ponctuelles aux exigences du monde professionnel. Lorsqu'il devra définir les prescriptions de forme devant être appliquées dans une procédure déterminée, le législateur pourra ainsi choisir entre la signature électronique qualifiée qui existe déjà (pour des exigences spécifiques) et la nouvelle signature réglementée (pour des exigences normales).
- Deuxièmement, créer la base légale qui régira non seulement la signature électronique mais aussi l'authentification sûre via des produits de certification. Dans la pratique, la confiance entre des partenaires impliqués dans un échange électronique s'instaure en effet la plupart du temps non pas par le biais d'une communication signée, mais d'une authentification par un service en ligne.
- Enfin, dans la mesure du possible, simplifier les termes employés dans les dispositions sur la signature électronique contenues dans les diverses lois et ordonnances en vigueur.

Dans le cadre des travaux de révision, on s'est par ailleurs demandé s'il fallait à l'avenir exiger que la signature électronique qualifiée soit systématiquement munie d'un horodatage.

Les délégations de compétences prévues par la SCSE en vigueur ne sont pas suffisantes pour que le Conseil fédéral puisse s'attaquer aux deux premiers objectifs. Aussi la révision vise-t-elle à lui donner la possibilité de régler par voie d'ordonnance une nouvelle forme de signature et d'autres utilisations de certificats, en particulier l'authentification, et d'élaborer des prescriptions techniques en la matière.

Le but ici n'est pas de modifier les concepts et les principes (p. ex. reconnaissance facultative des fournisseurs de services de certification, réglementation non exhaustive des produits de certification) existants ni de remettre en cause la conformité de la législation suisse à la directive européenne sur les signatures (directive 1999/93/CE sur un cadre communautaire pour les signatures électroniques ; ci-après directive de l'UE), nécessaire dans l'optique d'une reconnaissance internationale. Aussi, lorsqu'aucune modification ne s'imposait pour des motifs matériels, s'est-on efforcé de conserver la structure de la loi, qui est plutôt inhabituelle pour la Suisse avec ses définitions détaillées, et la terminologie européenne.

Voici ce que pourront proposer les fournisseurs de services de certification une fois la nouvelle loi entrée en vigueur :

- Tout fournisseur pourra proposer n'importe quel type de certificat ou produit de certification pour toute sorte d'utilisations, à l'exception du certificat réglementé, du certificat qualifié et de l'horodatage qualifié.
- Un fournisseur reconnu au sens de la SCSE pourra proposer tous les produits susmentionnés et les trois produits régis par la SCSE, à savoir :
    - o le certificat réglementé (nouveau) :
      - aux personnes physiques, aux personnes morales et aux autorités
      - pour toute sorte d'utilisations (sauf pour la signature électronique qualifiée)
    - o le certificat qualifié (inchangé) :
      - uniquement aux personnes physiques
      - uniquement pour la signature électronique qualifiée
    - o l'horodatage qualifié (nouveau)

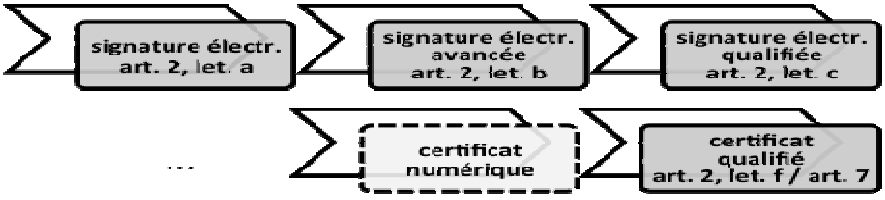
1.3 Grandes lignes du projet

1.3.1 Signature électronique réglementée fondée sur un certificat réglementé délivré au nom d'une personne physique, d'une personne morale ou d'une autorité

La loi actuelle subordonne – en conformité avec la directive de l'UE – la création de la signature électronique qualifiée à l'utilisation d'un certificat qualifié et confère, dans son art. 6, au Conseil fédéral la compétence de régler l'élaboration des clefs faisant l'objet d'un tel certificat et les dispositifs de création de signature. Son art. 7 énumère, quant à lui, les principaux éléments que doit contenir un certificat qualifié et charge le Conseil fédéral de régler la question du format.

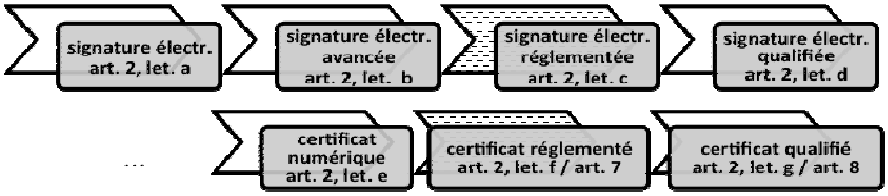
La révision n'entraînera ici aucun changement. L'avant-projet prévoit cependant une nouvelle forme de signature appelée « signature réglementée » entre la signature électronique avancée et la signature électronique qualifiée ainsi qu'un nouveau « certificat réglementé » sur lequel celle-ci se fondera. Le Conseil fédéral se voit confier la tâche de régler également l'élaboration et l'utilisation des clefs pouvant faire l'objet de ce type de certificat et la question du format.

Autrement dit : la loi en vigueur définit trois niveaux de signature, qui sont la signature électronique (art. 2, let. a), la signature électronique avancée (art. 2, let. b) et la signature électronique qualifiée (art. 2, let. c). La signature électronique qualifiée doit satisfaire plus d'exigences que la signature électronique avancée, laquelle doit remplir des conditions plus strictes que la signature électronique.
Notons que le certificat numérique constitue déjà la base du certificat qualifié dans la loi en vigueur, mais qu'il n'y fait l'objet d'aucune définition.

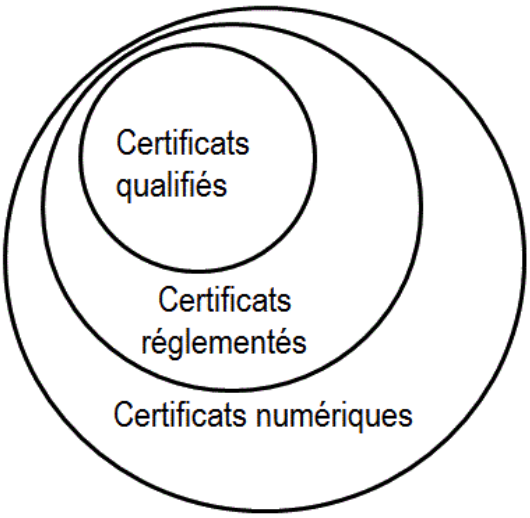


L'avant-projet prévoit le nouveau schéma suivant : les deux premiers niveaux de signature, à savoir la signature électronique (art. 2, let. a ; inchangée) et la signature électronique avancée (art. 2, let. b ; inchangée), sont conservés, mais on trouve, au troisième niveau, la signature électronique réglementée (art. 2, let. c) avant la signature électronique qualifiée, qui fait office de quatrième niveau (art. 2, let. d). Cette dernière devra satisfaire à plus d'exigences

que la signature électronique réglementée, laquelle devra remplir des conditions plus strictes que la signature électronique avancée.



Le certificat réglementé est une forme particulière de certificat numérique et le certificat qualifié une forme particulière de certificat réglementé. On peut en déduire qu'un certificat qualifié est aussi un certificat réglementé et qu'il est donc soumis aux mêmes exigences que ce dernier (en particulier celles de l'art. 7).



La principale différence entre le certificat qualifié et le certificat réglementé réside dans le fait que le premier ne pourra – comme c'est le cas aujourd'hui – être accessible qu'aux personnes physiques alors que le deuxième pourra aussi être délivré à des personnes morales et à des autorités. Il y a lieu de noter que le certificat réglementé ne peut, lui non plus, pas être un pur certificat machine, c'est-à-dire qu'il ne peut être établi simplement pour une machine telle qu'un serveur.

Eu égard à l'objectif de simplification terminologique visé par la révision, on précise d'ores et déjà dans la définition du certificat réglementé que celui-ci doit être délivré par un fournisseur reconnu de services de certification, ce qui permet de simplifier la manière dont on peut désigner la signature électronique normalement reconnue en Suisse. Aujourd'hui, il faut utiliser une formulation telle que : « Est considérée comme reconnue la signature électronique qualifiée au sens de la SCSE, fondée sur un certificat qualifié délivré par un fournisseur reconnu de services de certification. » La loi actuelle précise certes que la signature électronique qualifiée doit être fondée sur un certificat qualifié, mais pas que celui-ci doit être délivré par un fournisseur reconnu. Théoriquement, un tel certificat peut donc être délivré par un fournisseur de services de certification qui n'est pas reconnu. Comme ce type de produit n'existe pas sur le marché et qu'aucune utilisation judicieuse ne saurait lui être trouvée, on l'a exclu par la nouvelle définition. Grâce à la précision apportée dans la SCSE, on devrait simplement pouvoir dire : « Est considérée comme reconnue la signature électronique qualifiée au sens de la SCSE ».

Même si l'avant-projet confère au Conseil fédéral la compétence de régler deux types de certificats et non plus un seul, comme c'est le cas actuellement, il faut garder à l'esprit que tout fournisseur, qu'il soit reconnu ou non, sera libre de proposer d'autres types de certificats.

Afin d'éviter d'avoir à mentionner la compétence qui est conférée au Conseil fédéral de régler l'élaboration, l'enregistrement et l'utilisation des clefs cryptographiques à chaque fois qu'il est question d'une nouvelle forme d'utilisation d'un certificat – signature électronique réglementée, signature électronique qualifiée, authentification (voir chap. 1.3.3), etc. –, l'actuel art. 6 a été reformulé de manière à s'appliquer à n'importe quelle utilisation de certificats et non plus seulement à la signature électronique qualifiée. La compétence en ce qui concerne cette dernière demeure inchangée, ce qui permet de rester conforme à la directive de l'UE. Ce qui est nouveau en revanche, c'est que le Conseil fédéral reçoit cette compé-

tence également pour un deuxième type de certificat, propre à la Suisse, et pour d'autres utilisations.

1.3.2 Excursus relatif à la problématique des certificats délivrés aux entreprises

Pendant toute la genèse de la SCSE, les avis étaient partagés quant à savoir si les certificats qualifiés devaient être strictement réservés aux personnes physiques ou s'ils pouvaient également être délivrés à des personnes morales. Le projet sur lequel portait le message de 2001 prévoyait encore que ces dernières pouvaient y avoir accès ; un alinéa de l'art. 7, qui a par la suite été supprimé, précisait toutefois que si un certificat qualifié était délivré au nom d'une personne morale, il n'entraînait pas de pouvoir de représentation de cette dernière. Cette réserve montre les réticences que le certificat destiné aux entreprises pouvait susciter. Sans elle, on aurait pu supposer que le simple fait d'avoir accès à un tel certificat donnait à l'utilisateur le droit de représenter la personne morale qui y figurait. Afin d'éviter que les principes fondamentaux du droit de représentation soient bafoués, le législateur a finalement restreint l'utilisation du certificat qualifié aux personnes physiques.

Depuis l'entrée en vigueur de la SCSE, la pratique a toutefois montré qu'un certificat propre aux entreprises se révélait nécessaire dans le cadre du commerce électronique et des échanges électroniques avec les autorités. C'est en effet étrange que de devoir, lorsqu'on effectue des opérations de masse, signer les communications en se servant de certificats personnels et parfois saisir à nouveau le code PIN après seulement quelques opérations. De surcroît, c'est un procédé qui n'est pas très pratique.
En pareils cas, on utilise généralement la signature avancée de l'entreprise ou uniquement du serveur et on exclut par contrat – au besoin – les exceptions de forme. L'inconvénient ici est que la qualité du certificat utilisé ne répond pas à des critères fixés par l'Etat mais doit être définie dans chaque cas d'espèce.
Pour preuve du réel besoin existant dans ce domaine, mentionnons l'initiative du Département fédéral des finances, qui a défini par voie d'ordonnance et imposé un certificat propre aux entreprises pour le seul cas où il existe un important volume d'échanges avec les autorités, à savoir la transmission des factures des entreprises aux services de la TVA à des fins de déduction de l'impôt préalable. Cette initiative a été à l'origine de la motion Baumann évoquée précédemment et en partie aussi de cette révision.

Le problème rencontré par les entreprises privées se pose aussi pour les autorités, par exemple lors de la production automatique de documents, tels que les extraits du casier judiciaire, du registre du commerce ou du registre foncier. Dans ce cas, on utilise soit le certificat qualifié d'une personne déterminée, comme le préposé au registre – certificat qui, en cas de changement de personnel, est mis au nom du nouveau collaborateur –, soit un certificat avancé ne répondant à aucun critère de qualité défini.
On retrouve des expériences similaires dans d'autres pays européens. L'Autriche a ainsi édicté une norme instituant une « signature officielle » fondée sur un certificat délivré au nom d'une autorité déterminée.

En Suisse aussi, il existe aujourd'hui sur le marché différents types de certificats qui se réfèrent d'une manière ou d'une autre à une personne morale. Outre le certificat spécial TVA déjà évoqué, on peut mentionner le certificat pour serveur (https) SSL, qui est par exemple utilisé lors des transactions bancaires en ligne. Il est en outre possible de mentionner sur un certificat qualifié que le titulaire est un collaborateur d'une entreprise ou un représentant d'une personne morale. Toutes ces possibilités n'ont jusqu'à présent jamais donné lieu à aucune méprise quant aux pouvoirs de représentation.

La présente révision vise à régler les problèmes liés à l'inexistence de certificats propres aux entreprises. L'option choisie ici n'a cependant pas été d'étendre le cercle des titulaires potentiels du certificat qualifié, comme c'était prévu à l'origine, mais de créer un certificat qui présente les caractéristiques du certificat avancé et non pas celles du certificat qualifié dans la

mesure où il devra remplir des exigences moins strictes et pourra être délivré au nom de personnes morales et d'autorités.
Ce nouveau certificat destiné aux entreprises et aux autorités n'aura pas la même valeur que le certificat qualifié. D'une manière générale, la SCSE ne règle que les exigences de qualité auxquelles certains produits de certification doivent satisfaire et les obligations qui incombent aux fournisseurs de ces produits. La valeur de certains produits ou procédures dans les relations juridiques est définie dans d'autres actes législatifs. C'est par exemple le code des obligations (CO ; RS 220), dans son art. 14, al. 2^{bis}, qui règle la question de l'assimilation de la signature électronique qualifiée à la signature manuscrite. Pour ce qui est du nouveau certificat réglementé et de la signature électronique réglementée, le législateur compétent sera libre de les accepter ou non dans certains buts, tout comme les services de la TVA acceptent un certificat qu'ils ont eux-mêmes défini pour la transmission de factures aux fins de faire valoir la déduction de l'impôt préalable. De la même manière, des partenaires commerciaux pourront convenir qu'un certificat réglementé suffit pour les transactions qui ne sont soumises à aucune exigence légale de forme, comme ils le font aujourd'hui avec les accords EDI lors des échanges électroniques de masse. Contrairement à aujourd'hui, ils disposeront à l'avenir pour ce faire d'un certificat soumis à des exigences réglées de manière uniforme et d'une procédure de signature.

Si l'on s'en tient à cette vision des choses, il n'existe aucun risque que l'on conclue à tort qu'un certificat délivré au nom d'une entreprise entraîne un pouvoir de représentation. Afin de prévenir toute méprise, un alinéa formulant cette restriction a été ajouté dans l'art. 1, al. 2.

Du moment que ni le bien-fondé du certificat qualifié et de la signature électronique qualifiée ni leur conformité à la directive de l'UE ne sont remis en cause et qu'on ne restreint pas le marché libre en diminuant le nombre de produits et de fournisseurs, rien n'empêche de rendre service à l'économie en définissant au niveau national un certain nombre d'autres produits de certification. La réglementation proposée offre en quelque sorte sur le plan technique et organisationnel un gage de confiance validé par l'Etat dans des domaines d'utilisation tout entiers et favorise le secteur, voire l'émergence de marchés. Ce sont toutefois les différentes parties impliquées, les autres actes législatifs et la doctrine qui détermineront les effets juridiques des utilisations qui seront réservées à ces produits standardisés.

1.3.3 Authentification

Afin que le commerce électronique entre particuliers et avec les autorités se développe en Suisse, il importe que les partenaires impliqués soient certains de l'identité de l'interlocuteur avec lequel ils communiquent, qu'ils soient sûrs que cet interlocuteur est bien celui qu'il prétend être. Lorsque la SCSE en vigueur a été conçue, il y a de cela une bonne dizaine d'années, on partait du principe que le commerce électronique serait principalement basé sur l'échange de communications de type courriers électroniques ou données structurées et que c'est grâce à la signature électronique figurant sur ces communications qu'on pourrait attester de l'identité de l'expéditeur. Ce modèle de communication ne s'est toutefois imposé que dans certains domaines et est plutôt utilisé pour la communication entre professionnels. En revanche, un autre modèle de communication en ligne se développe de plus en plus, celui où un partenaire – la plupart du temps, le client ou le citoyen – s'inscrit sur un système d'application ou le portail d'un autre partenaire – généralement, une entreprise ou une autorité – pour y effectuer son opération. L'inscription peut aussi intervenir à un niveau inférieur : dans ce cas, une application du client se connecte à un service Web du fournisseur et les deux programmes s'authentifient mutuellement. Dans les deux cas, un processus d'authentification s'enclenche (aussi bien du côté de la personne qui s'inscrit que de celui du service Web) dès que les deux systèmes se connectent l'un à l'autre, permettant d'établir avec certitude l'identité des différents partenaires. Des communications signées sont échangées, mais dans le cas de la procédure qui intervient à un niveau inférieur, il ne s'agit pas de communications signées consciemment. En principe, on utilise donc le même type de certificat que pour la signature électronique, mais pas le même certificat pour les deux utilisations

afin d'éviter les attaques par des tiers et donc les abus. C'est pour cette raison que les milieux économiques concernés réclament depuis longtemps, pour certains cas d'authentification, un certificat qui, par son caractère officiel et les exigences légales de qualité auxquelles il serait soumis, offrirait un gage de confiance validé par l'Etat et apporterait une sécurité accrue aux échanges.

Aujourd'hui, le certificat qualifié sert à créer des signatures électroniques, en particulier des signatures électroniques qualifiées, qui déploient des effets particuliers. Pour des raisons techniques, et plus précisément pour éviter certains risques d'attaques informatiques contre la signature sûre, l'avant-projet prévoit aussi de limiter son usage à la signature électronique.

Cette spécificité ne vaudra cependant pas pour le nouveau certificat réglementé, qui sera soumis à des exigences légèrement moins sévères. Il pourra, sur le plan juridique, être utilisé aussi bien pour les signatures électroniques en tous genres que pour l'authentification ou d'autres applications de sécurité telles que celles qui requièrent un certificat SSL.

Sur le plan de la technique législative, toutes les dispositions qui portaient sur l'utilisation de certificats à des fins de signature ont été reformulées de façon à ce qu'elles puissent s'appliquer à toutes les utilisations. On ne parle ainsi plus de « clés de signature » ni de « clés de vérification de signature » mais de « clefs cryptographiques publiques et privées ».
Il convient de noter que cette formulation plus ouverte ne change rien, sur le plan matériel, pour le certificat qualifié, dont le seul usage possible est la signature.

1.3.4 Signature électronique qualifiée avec horodatage obligatoire

Au cours des dernières années, des voix se sont élevées à plusieurs reprises au sein des secteurs concernés pour demander qu'un horodatage fiable soit obligatoirement intégré à la signature électronique qualifiée. L'horodatage consiste à associer une date et une heure officielles à des données, ce qui permet – si le système est fiable – d'établir que ces données existaient à un moment donné ou que la signature a été créée à un instant précis. En l'absence d'horodatage, l'heure et la date auxquelles une signature est associée n'ont qu'une valeur relative. Horodater une signature électronique qualifiée constitue parfois le seul moyen d'éviter des attaques informatiques ou des fraudes. Voilà pourquoi les fournisseurs reconnus de services de certification sont déjà tenus, en vertu de l'actuel art. 12 SCSE, de proposer un tel service.

Les programmes de signature qu'on trouve aujourd'hui sur le marché offrent normalement la possibilité d'horodater la signature. La plupart du temps, il est possible d'en faire un paramètre par défaut.

Pour pouvoir intégrer l'horodatage dans la signature électronique, il faut être connecté à Internet au moment de la signature, ce qui était encore une condition difficile à remplir au temps de l'élaboration de la SCSE. On citait souvent l'exemple du notaire, qui devait, lors d'une assemblée constitutive sur place, apposer sa signature sur les statuts ou les procès-verbaux pour les authentifier. Entre-temps, cette condition est devenue beaucoup plus facile à remplir et ne devrait, dans quelques années, plus être un problème du tout.

Dans le cadre des travaux préparatoires, on a examiné trois options pour ce qui est de l'intégration de l'horodatage dans la signature électronique, dont voici la teneur :

1. La signature électronique qualifiée est obligatoirement munie de l'horodatage d'un fournisseur reconnu de services de certification.
2. La loi définit deux types de signatures électroniques qualifiées, l'une avec horodatage, l'autre sans.

3. L’horodatage n’est pas requis pour la signature électronique qualifiée dans la SCSE. C’est le CO qui règle la question de savoir si cet élément est obligatoire pour que la signature électronique qualifiée soit assimilée à la signature manuscrite.

La solution la plus draconienne a été rejetée par la plupart des représentants des milieux intéressés et des spécialistes car étant jugée trop restrictive, mais si elle n’a pas été retenue, c’est surtout parce qu’une telle obligation n’existe pas dans la directive de l’UE et la législation des pays voisins.

On a finalement opté ici pour la troisième solution, qui règle un point sur lequel la SCSE ne s’exprime pas et qui prévoit que l’obligation d’horodater peut être fixée selon les nécessités du domaine. En l’occurrence, le CO requiert ce système pour assimiler la signature électronique qualifiée à la signature manuscrite.

1.3.5 Adaptations terminologiques

Comme on l’a dit au chap. 1.3.1, la modification de la définition du certificat réglementé permettra d’utiliser une expression beaucoup plus courte dans les autres actes législatifs pour désigner la signature généralement considérée comme équivalente à la signature manuscrite, à savoir « signature qualifiée au sens de la SCSE ».

D’une manière générale, on a veillé à ce qu’on puisse à l’avenir se référer simplement aux notions de la SCSE. En plus de ce qui a déjà été fait et dont on a parlé précédemment, on a donc précisé à l’art. 13 (actuel art. 12) qu’il s’agissait d’horodatage « qualifié » pour le distinguer clairement de l’horodatage de fournisseurs quelconques dans la mesure où il est offert par des fournisseurs reconnus de services de certification.

L’horodatage électronique de haute qualité fourni par des tiers indépendants joue un rôle toujours plus important. A titre d’exemple, on peut citer l’horodatage de données à archiver, telles qu’une comptabilité, qui permet, en étant associée à la signature électronique, de prouver que les données existaient sous cette forme à un moment donné et qu’elles n’ont pas été modifiées depuis. Pour parler de ce type d’horodatage, qui est particulièrement fiable puisque fourni par un fournisseur reconnu, on pourra directement utiliser l’expression « horodatage qualifié au sens de la SCSE ».

1.3.6 A propos de la technique de révision

La révision qui nous occupe ici était censée être une révision partielle à l’origine. Compte tenu du nombre relativement restreint d’objectifs (voir chap. 1.1), on pourrait continuer à la considérer comme telle. Cependant, comme la plupart des dispositions ne valent plus seulement pour le certificat qualifié mais pour les certificats réglementés et que les clefs font l’objet d’une dénomination neutre dans tout le texte (p. ex. « clef cryptographique » en lieu et place de « clé de vérification »), la plupart des articles sont concernés par la révision. Voilà pourquoi, selon les critères usuels, cette dernière est en fait une révision totale.

1.3.7 Autres révisions

Plusieurs lois et ordonnances se réfèrent aux notions de la SCSE, en particulier bien évidemment celle de signature électronique qualifiée. Il sera à l’avenir normalement question de la signature électronique réglementée dans ces actes normatifs, ce qui permettra de prendre en compte les signatures de personnes morales et d’autorités. La signature électronique qualifiée ne sera requise que dans certains cas particuliers où il sera nécessaire d’établir un lien direct avec une personne physique. Ce procédé s’inscrit dans la stratégie générale qui vise à ne pas restreindre la communication électronique plus qu’elle ne devrait l’être objectivement.

2 Commentaire disposition par disposition

2.1 Loi fédérale sur la signature électronique

2.1.1 Titre de la loi

L'extension des possibilités d'utilisation des produits de certification définis par la SCSE et ses dispositions d'exécution doit se refléter dans le nouveau titre. Si l'authentification figure au centre des préoccupations, d'autres utilisations de certificats numériques sont aussi concernées, raison pour laquelle on a opté pour une formulation ouverte.

2.1.2 Section 1 : Dispositions générales

Art. 1 Objet et but

La définition actuelle de l'objet de la SCSE a souvent donné et donne encore souvent lieu à des erreurs d'interprétation. Certains considèrent ainsi que cette loi règle non seulement la signature électronique mais aussi ses effets. Or elle se borne pour l'essentiel à définir des normes de qualité en soumettant certains produits de certification mais aussi et surtout leurs fournisseurs à certaines exigences. L'ajout d'une nouvelle lettre à l'al. 1 vise à clarifier son objet spécifique et limité.

La loi ne règle et ne favorise plus seulement la signature électronique (qualifiée) en tant que possibilité d'utilisation des certificats mais aussi les signatures électroniques en général et d'autres applications de certificats réglementés. Aussi les al. 1, let. a (actuel al. 1, let. a), et 3, let. b (actuel al. 2, let. b), ont-ils été reformulés.

Le nouvel al. 2 tient compte des craintes dont il était question au chap. 1.3.2 concernant le fait qu'on puisse croire à tort qu'un certificat délivré au nom d'une personne morale ou d'une autorité pourrait conférer un pouvoir de représentation. Le fait qu'un certificat réponde aux exigences de qualité posées par cette loi – et les dispositions sur la responsabilité évoquées précédemment servent seulement à garantir cette qualité – ne donne aucune indication sur les effets juridiques déployés par l'utilisation qu'on fait de ce certificat. Ces effets doivent être définis par voie contractuelle ou légale en fonction du contexte d'utilisation.

L'al. 3, let. b, est lui aussi formulé de manière plus générale.

Art. 2 Définitions

Les nouvelles définitions ont été insérées à leur place logique, ce qui a nécessité une nouvelle numérotation des actuelles let. d et suivantes.

- let. c : signature électronique réglementée
  La définition de la signature réglementée – qui se trouve entre celle de la signature électronique avancée et celle de la signature électronique qualifiée – s'inspire de la définition de la signature électronique qualifiée qui figure à la let. c de la disposition en vigueur. La première forme particulière de signature avancée sera donc la signature électronique réglementée (et non plus la signature électronique qualifiée, comme c'est le cas actuellement).
- let. d : signature électronique qualifiée
  La signature électronique qualifiée, qui est définie à l'actuelle let. c, est créée de la même manière que la signature électronique réglementée, mais elle en est une forme particulière car elle requiert un certificat (ou une paire de clefs) qualifié.

- Les définitions de « clé de signature » et de « clé de vérification de signature » qui figurent dans la loi en vigueur (let. d et e) ont été supprimées parce qu'on parle de l'utilisation des clefs en général dans l'avant-projet et qu'on emploie donc les expressions « clef cryptographique privée » et « clef cryptographique publique ».

- let. e : certificat numérique
  La notion de « certificat numérique » apparaît dans la définition large de la notion de « certificat qualifié » sans pour autant être elle-même définie, ce qui rompt avec la logique et va à l'encontre de la directive de l'UE et de la législation des pays voisins. Une définition de cette notion figure même dans la législation d'exécution. L'ajout de cette nouvelle définition, qui n'entraîne aucune modification matérielle, est certes contraire au principe de cette révision, qui veut que seuls les changements nécessaires pour remplir les objectifs définis au chap. 1.1 soient effectués, mais il permet d'assurer une meilleure compréhension et une meilleure cohérence dans la systématique.
  Dans un certificat numérique quelconque, la paire de clefs peut en principe aussi bien être liée à une personne qu'à un objet, par exemple une machine ou un site Web – ce qui n'est pas le cas dans un certificat réglementé ou un certificat qualifié. Dans la terminologie spécialisée anglaise, on utilise ici souvent le concept d'« entity ». Nous avons choisi ici le terme de « titulaire ». Nous avons estimé que le calque de l'anglais (« entité ») ou une solution telle qu'« objet » n'étaient pas suffisamment clairs.

- let. f : certificat réglementé
  La définition du certificat réglementé s'inspire de celle du certificat qualifié figurant à l'actuelle let. f. Au vu des exigences posées par l'art. 7, on peut dire qu'il s'agit d'un certificat numérique plus simple et plus général que le certificat qualifié, dont il constitue la base. Par souci de simplification, on a précisé – ce qui n'est pas le cas dans la législation en vigueur – que tout certificat réglementé devait être délivré par un fournisseur reconnu de services de certification.

- let. g : certificat qualifié
  Il s'agit du certificat qualifié défini à l'actuelle let. f. Selon la nouvelle systématique, il constitue une forme particulière du certificat réglementé introduit à la let. f et doit, à ce titre, répondre à des exigences supplémentaires. Hormis le fait qu'il devra toujours être délivré par un fournisseur reconnu – condition applicable au certificat réglementé –, les exigences auxquelles il sera soumis sont les mêmes qu'aujourd'hui.

2.1.3 Section 2 : Reconnaissance des fournisseurs

Aucun changement ne sera apporté au système de reconnaissance actuel. Une solution qui a été envisagée mais qui n'a pas été retenue était de prévoir deux types de reconnaissance : une pour les fournisseurs ne proposant que des certificats réglementés simples et une autre pour les fournisseurs proposant aussi des certificats qualifiés. Elle n'aurait toutefois fait que compliquer un système déjà complexe sans pour autant répondre à un réel besoin.

Conserver le texte actuel, comme on le propose ici, implique qu'il n'y aura toujours qu'*un seul* type de reconnaissance. Pour être reconnus, les fournisseurs devront être en mesure de délivrer des certificats qualifiés, et donc automatiquement aussi des certificats réglementés, puisque les certificats qualifiés sont des certificats réglementés soumis à des exigences supplémentaires. Les fournisseurs déjà reconnus pourront donc à l'avenir proposer un autre type de certificat réglé par la loi et, bien entendu aussi, continuer de délivrer d'autres types de certificats qui ne sont pas prévus par la loi.

On s'est donc contenté d'adapter les renvois à la cessation d'activité (nouvel art. 14) et à la responsabilité (nouvel art. 17) qui figurent à l'art. 3, al. 1, let. f.

2.1.4 Section 3 : Elaboration, enregistrement et utilisation de clefs cryptographiques

Le titre actuel « Elaboration et utilisation de clés de signature et de vérification de signature » devait être remplacé par un titre plus général car, dans cette section, il est également question des clefs utilisées pour l'authentification ou pour d'autres utilisations de certificats. On a estimé que « clefs cryptographiques » était une expression suffisamment générale. Il convient de noter que seules les clefs cryptographiques pouvant faire l'objet des certificats réglementés sont ici visées.

Art. 6

L'art. 6 de la loi en vigueur, qui reprend le contenu de l'annexe III à la directive de l'UE, traite seulement de la signature. L'avant-projet confère – comme on l'a expliqué au chap. 1.3.1 – au Conseil fédéral la compétence de régler d'autres utilisations de certificats et de clefs, en particulier l'authentification. C'est pourquoi cet article ne parle plus de « signature » ou de « vérification de signature » mais d'« utilisation de clefs cryptographiques » en général.

L'art. 6, al. 3, de la SCSE en vigueur reprend presque intégralement le contenu de l'annexe IV à la directive de l'UE. A plusieurs égards, il fait figure de corps étranger dans une loi suisse car il ne formule qu'une recommandation et s'adresse séparément à des destinataires difficilement identifiables, principalement les fournisseurs de visionneuse PDF. On s'est demandé s'il fallait tout de même conserver cette disposition afin d'assurer la continuité et la conformité avec la directive de l'UE et la formuler de manière potestative, comme lignes directrices adressées au Conseil fédéral. Finalement, on a préféré la supprimer, considérant qu'elle n'avait qu'une valeur déclaratoire, était impossible à mettre en œuvre dans la pratique et n'avait aucune nécessité. Il est en effet dans l'intérêt du destinataire d'une communication signée au moyen d'une signature électronique d'utiliser des outils pertinents pour vérifier cette signature.

2.1.5 Section 4 : Certificats réglementés

Dans la mesure où cette section porte sur deux types de certificats, le certificat réglementé et sa forme particulière, le certificat qualifié, le titre original « Certificats qualifiés » a été remplacé par « Certificats réglementés ».

Art. 7 Conditions applicables aux certificats réglementés

Le nouvel art. 7 reprend, sur le plan matériel, l'essentiel des exigences posées aux certificats qualifiés dans l'actuel art. 7. Les conditions supplémentaires uniquement applicables aux certificats qualifiés figurent à l'art. 8.

Contrairement aux certificats qualifiés, qui ne peuvent être délivrés qu'au nom de personnes physiques, les certificats réglementés non qualifiés peuvent aussi être délivrés au nom de personnes morales et d'autorités. Cette spécificité n'a pas été mentionnée dans une lettre de l'al. 2 mais a été mise en évidence dans la disposition puisqu'elle fait l'objet du nouvel al. 1. Le fait de parler d'« entités IDE » au sens de la loi fédérale du 18 juin 2010 sur le numéro d'identification des entreprises (LIDE ; RS 431.03) permet d'englober la grande majorité des personnes morales mais aussi les autorités. Les sujets de droit inscrits au registre du commerce (art. 3, al. 1, let. c, ch. 1, LIDE) mais également les autres personnes morales se trouvent ainsi visés. Parmi les entités IDE, figurent entre autres aussi les autorités et les tribunaux (art. 3, al. 1, let. c, ch. 7, LIDE). Les seules personnes morales à ne pas être ici concernées sont celles qui ne figurent pas au registre IDE, comme certaines associations et fondations. Pour ces dernières, deux possibilités étaient envisageables : soit les mentionner à part, soit, et c'est la solution qui a été retenue ici, les exclure délibérément. Une personne morale qui ne remplit pas les conditions d'inscription au registre IDE fixées par l'art. 3, al. 1, let. c, LIDE, qui n'a par exemple de contact avec aucune autorité, ne pourra se voir attribuer une identité électronique sous forme de certificat réglementé. La vérification de l'identité par

le fournisseur de services de certification pourrait en effet se révéler compliquée. Si une telle personne veut toutefois prendre part au commerce électronique – ce qui est assez improbable –, elle peut très bien le faire par le biais d'une personne physique qui la représente.

Le champ d'application de la let. b a été étendu aux certificats réglementés, comme c'est le cas partout dans le texte.

La question de l'identité du titulaire, réglée aujourd'hui à la let. c, fait l'objet de trois lettres distinctes dans l'avant-projet (c, d et e). La let. c mentionne le nom ou, pour les personnes morales, la désignation du titulaire de la clef et prévoit l'ajout d'un élément distinctif pour éviter les problèmes liés à l'homonymie. Il n'est ici plus question du « titulaire de la clé de vérification de signature », comme c'est le cas dans la loi en vigueur, mais du « titulaire de la clef cryptographique privée ». Cette modification permet une fois de plus d'étendre le champ d'application de la loi à d'autres utilisations de certificats et de corriger un défaut datant de l'époque où la loi a été élaborée ; il aurait en effet depuis toujours dû être question de « clé de signature » – comme c'est le cas à l'actuel al. 2, let. a – et non de « clé de vérification de signature », qui est moins approprié. Quant à la clef publique qui doit être liée au titulaire, ce point est réglé à la let. f (actuelle let. d).

La let. d, qui autorise les pseudonymes, comme c'est le cas aujourd'hui, vaut seulement pour les personnes physiques.

La let. e, qui prévoit que le numéro unique d'identification des entreprises figure sur le certificat, ne s'applique, quant à elle, qu'aux identités IDE.

La let. f remplace l'actuelle let. d et parle non plus de « clé de vérification de signature » mais plus généralement de « clef cryptographique publique », car les certificats réglementés peuvent être utilisés non seulement pour la signature mais par exemple aussi pour l'authentification.

L'actuelle let. g, qui prévoit que le certificat doit contenir des informations concernant la reconnaissance du fournisseur, a été biffée au motif qu'il s'agissait d'une spécificité suisse.

Let. h : donner la possibilité à des personnes morales d'utiliser une signature répondant à des exigences de qualité définies par la loi, en l'occurrence la nouvelle signature réglementée, permet de corriger – comme pour l'horodatage – l'anomalie constituée par le fait que les fournisseurs de services de certification sont les seules personnes non physiques à recevoir un certificat qualifié et donc à avoir une signature qualifiée. Grâce à l'introduction de la signature électronique réglementée, qui est fondée sur un certificat réglementé, cette anomalie n'aura plus lieu d'être.

L'actuel al. 2, let. a, qui porte sur l'indication éventuelle de données supplémentaires et la représentation, fait l'objet de deux lettres dans l'avant-projet (let. a et b). La let. a mentionne les qualités spécifiques et donne en exemple les qualifications professionnelles, qui sont souvent indiquées dans la pratique.

La mention de la représentation dont il est spécifiquement question à la let. b est possible dans les certificats réglementés non qualifiés, mais seules les personnes physiques pourront en faire usage. Dans le cadre des travaux préparatoires, on a également examiné la possibilité de ne faire figurer cette mention que dans les certificats qualifiés, mais on n'a trouvé aucune raison valable pour une telle restriction.

Les lettres c et d reprennent les actuelles let. b et c. Le remaniement de cet alinéa vise uniquement à rendre le texte actuel plus clair.

Art. 8 Conditions applicables aux certificats qualifiés

Dans la mesure où l'essentiel des conditions auxquelles sont actuellement soumis les certificats qualifiés figurent à l'art. 7 relatif aux conditions applicables aux certificats réglementés, l'art. 8 ne contient que les conditions supplémentaires que les certificats qualifiés, en tant que forme particulière de ces derniers, doivent remplir. Ajoutées les unes aux autres comme le veut la définition (voir art. 2, let. g), ces conditions correspondent sur le fond aux conditions auxquelles doivent actuellement satisfaire les certificats qualifiés ; quelques points ont été explicités.

L'al. 1 énonce la principale différence entre le certificat qualifié et le certificat réglementé non qualifié, à savoir qu'il est réservé aux personnes physiques.

L'al. 2 précise expressément, ce qui n'est pas le cas dans la loi en vigueur, qu'un certificat qualifié ne peut être utilisé que pour la signature électronique. Cette précision est une fois de plus contraire au principe de cette révision, qui veut que seules soient effectuées les modifications qui sont nécessaires pour remplir les objectifs visés. Cependant, à l'heure actuelle, cette exigence est uniquement formulée dans les prescriptions techniques et administratives (PTA, RS 943.032.1, annexe), une valeur déterminée, celle servant à la signature de documents, étant requise pour le champ « key usage ». Les non-techniciens se sont toujours formalisés du fait qu'une restriction aussi importante, qui est manifestement dictée par des impératifs techniques et qui semble évidente uniquement pour les spécialistes, ne soit pas explicitement formulée dans la loi.

L'al. 3 reprend l'actuel art. 7, al. 1, let. b.

2.1.6 Section 5 : Devoirs des fournisseurs reconnus

Art. 9 (actuel art. 8) Délivrance des certificats réglementés

Les règles relatives à la procédure de demande d'un certificat réglementé vaudront également pour les entités IDE. C'est la raison pour laquelle l'al. 1 est composé de deux lettres. La let. a règle la procédure pour les personnes physiques de la même manière qu'aujourd'hui ; la let. b règle, quant à elle, la procédure relative à la délivrance de certificats réglementés aux entités IDE. Les personnes physiques qui sont également des entités IDE doivent se présenter en personne, conformément à la let. a, pour demander un certificat réglementé.

La deuxième partie de l'actuel al. 1, qui était quelque peu surchargé, fait à présent l'objet des al. 2 et 3. Les actuels al. 2, 3 et 4 deviennent donc les al. 4, 5 et 6.

Art. 11 (actuel art. 10) Annulation des certificats réglementés

L'actuel art. 10, al. 1, let. b, a été reformulé de sorte qu'il sera à l'avenir aussi possible d'annuler un certificat s'il s'avère que les renseignements professionnels ou autres visés à l'art. 7, al. 3, ne sont pas ou plus exacts.

Art. 13 (actuel art. 12) Système d'horodatage qualifié

L'ajout de l'adjectif qualificatif « qualifié » dans le titre permet d'établir une distinction entre un horodatage particulièrement fiable émanant d'un fournisseur reconnu et un horodatage quelconque.

Art. 17 (actuel art. 16) Responsabilité des fournisseurs

L'ajout de l'adjectif qualificatif « reconnu » vise à faire ressortir plus clairement le fait que cette disposition ne s'applique pas aux services de certification de n'importe quel type de fournisseur.

Art. 20 (actuel art. 19)

Par souci de précision, on a remplacé « certificat » par « certificat numérique ».

2.1.7 Diverses adaptations dans les sections 5 à 9

Trois adaptations, qui concernent la totalité ou plusieurs des dispositions de ces sections, sont ici brièvement évoquées.

Adaptation du numéro des articles

Jusqu'au dernier article, il faut ajouter un à tous les articles.

Remplacement de « certificat qualifié » par « certificat réglementé »

Normalement, toutes les dispositions de la loi en vigueur qui portent sur le certificat qualifié concerneront les deux certificats réglés par la loi, à savoir le certificat réglementé (au sens strict) et le certificat qualifié en tant que forme particulière de ce dernier. C'est la raison pour laquelle l'expression « certificat qualifié » a été remplacée par celle de « certificat réglementé » à chaque fois que cela s'avérait pertinent, ce qui permet d'inclure les deux types de certificats. On a exceptionnellement opté pour une formulation plus élégante mais le but visé était le même.
Cette adaptation concerne les (nouveaux) art. 9, 10, 11, 12, 14, 17, 18 et 21.

Remplacement de « signature électronique » et de « clé de signature » par des expressions neutres

Comme la loi ne régira plus seulement la signature mais aussi d'autres utilisations de certificats numériques, les expressions « signature électronique » et « clé de signature » ont été remplacées par des expressions plus neutres ou des formulations plus appropriées.
Cette adaptation concerne les (nouveaux) art. 10, 11, 16, 17 et 20.

La nouvelle numérotation des articles et des alinéas a par ailleurs nécessité l'adaptation de certains renvois (voir art. 16, 17, al. 3, et 18).

2.2 Modification d'autres actes législatifs

2.2.1 Code des obligations

Art. 14 Signature

Le fait de préciser dans l'article de la SCSE consacré aux définitions (voir art. 2, let. d, f et g, et chap. 1.3.1) que le certificat utilisé pour la signature électronique qualifiée doit être délivré par un fournisseur reconnu permet de simplifier considérablement l'art. 14, al. 2^{bis}, CO et de le rendre plus lisible.

Variante : signature électronique qualifiée avec horodatage obligatoire

Comme mentionné au chap. 1.3.4, certains souhaitent que seules les signatures électroniques munies d'un horodatage fourni par un service indépendant soient considérées comme valables. On a examiné la possibilité de soumettre la « signature électronique qualifiée » au sens de la SCSE à cette exigence, mais on a estimé que cette solution était trop restrictive.

Etant donné qu'en Suisse – contrairement à plusieurs pays voisins – la reconnaissance de la signature électronique n'est pas réglée dans la SCSE mais dans la législation propre aux différents domaines, on peut tout à fait exiger dans un domaine déterminé que la signature électronique soit munie d'un horodatage pour être reconnue. Comme le montre la variante

proposée ici, cette exigence peut par exemple être requise à l'art. 14, al. 2bis, CO pour pouvoir assimiler la signature électronique qualifiée à la signature manuscrite.

Art. 59a Responsabilité en matière de clé de signature

La responsabilité que la loi en vigueur confère au titulaire de la clé pour les certificats qualifiés doit être étendue aux certificats réglementés car cette responsabilité est une des principales conditions d'acceptation par les tiers ; sans elle, le certificat réglementé aurait peu de valeur aux yeux de la personne qui doit s'y fier. Toutefois, elle doit être limitée à la signature et non pas valoir pour l'authentification ou les autres utilisations de certificats. C'est la raison pour laquelle l'expression « clé de signature » n'a pas ici été remplacée par celle plus générale de « clef cryptographique ».

2.2.2 Extension de la compétence de délégation

Plusieurs lois de procédure fédérales prévoient que toute requête doit être munie d'une signature électronique reconnue. Une fois la nouvelle signature électronique réglementée introduite, on disposera d'une autre signature électronique reconnue au sens de la SCSE en plus de la signature électronique qualifiée qui existe déjà. Il faut donc régler par voie d'ordonnance la question de savoir laquelle de ces deux signatures doit être utilisée, ce qui nécessite, pour ce faire, de déléguer la compétence requise au Conseil fédéral.

Sont concernés
- les art. 21*a*, al. 2, et 34, al. 1bis, de la loi fédérale du 20 décembre 1968 sur la procédure administrative (RS 172.021),
- l'art. 130, al. 2, du code de procédure civile du 19 décembre 2008 (RS 272) et
- l'art. 110, al. 2, du code de procédure pénale du 5 octobre 2007 (RS 312.0).

La norme de délégation de l'art. 33*a*, al. 2, de la loi fédérale du 11 avril 1889 sur la poursuite pour dettes et la faillite (RS 281.1) est suffisante. Par contre, il faut en créer une en faveur du Tribunal fédéral à l'art. 42, al. 4, de la loi du 17 juin 2005 sur le Tribunal fédéral (RS 173.110).

La simplification terminologique dont doivent faire l'objet les dispositions relatives à la signature électronique ne pourra se faire sans une modification du contenu de plusieurs ordonnances. La notion de « signature électronique » apparaît notamment dans les dispositions d'exécution suivantes :
- art. 14*a*, al. 2, de l'ordonnance du 20 septembre 2002 sur les documents d'identité (RS 143.11) ;
- art. 27*d*, al. 2, let. a et b, et27*k*^{bis}, al. 2 et 3, de l'ordonnance du 24 mai 1978 sur les droits politiques (RS 161.11) ;
- art. 4, al. 2, let. f, art. 6, al. 1, 2 et 3, art. 9, al. 4 et 5, et art. 12, al. 1, let. c et d, de l'ordonnance du 18 juin 2010 sur la communication électronique dans le cadre de procédures administratives (RS 172.021.2) ;
- art. 2, let. d, et 4, al. 3, du règlement du Tribunal fédéral du 5 décembre 2006 sur la communication électronique avec les parties et les autorités précédentes (RS 173.110.29) ;
- art. 11, al. 3, de l'ordonnance du 17 octobre 2007 sur le registre du commerce (RS 221.411) ;
- art. 8, al. 2, et 13, al. 2, let. a, de l'ordonnance du 15 février 2006 sur la Feuille officielle suisse du commerce (RS 221.415) ;
- art. 2, let. a et b, 5, al. 2, let. c, 7, 10, al. 3, 13, al. 1, let. c et d, et 14, al. 2, de l'ordonnance du 18 juin 2010 sur la communication électronique dans le cadre de procédures civiles et pénales et de procédures en matière de poursuite pour dettes et de faillite (RS 272.1) ;
- art. 4, al. 1, de l'ordonnance du DFJP du 9 février 2011 concernant la communication électronique dans le domaine des poursuites pour dettes et des faillites (RS 281.112.1) ;

- art. 17, al. 3, let. c, et al. 4, de l’ordonnance du 21 novembre 2007 sur l’harmonisation de registres (RS 431.021) ;
- art. 2, phrase introductive al. 2, let. a, ch. 5, et al. 4, et art. 3, al. 1, let. a, c et d, de l’ordonnance du DFF du 11 décembre 2009 concernant les données et informations électroniques (RS 641.201.511) ;
- art. 5, al. 4, de l’ordonnance du DETEC du 24 novembre 2006 sur l’attestation du type de production et de l’origine de l’électricité (RS 730.010.1) ;
- art. 63, al. 2, let. c, de l’ordonnance du 7 décembre 1998 sur les paiements directs (RS 910.13) ;
- art. 20, al. 1bis, let. c, de l’ordonnance du 14 novembre 2007 sur les contributions d’estivage (RS 910.133) ;
- art. 8, al. 1bis, let. c, de l’ordonnance du 4 avril 2001 sur la qualité écologique (RS 910.14) ;
- art. 5, al. 1bis, let. c, de l’ordonnance du 7 décembre 1998 sur les contributions à la culture des champs (RS 910.17) ;
- art. 5, al. 3, 7, al. 2, et 9, al. 3, de l’ordonnance du 3 décembre 2004 sur la signature électronique (RS 943.032) ;
- art. 1 de l’ordonnance de l’OFCOM du 6 décembre 2004 sur les services de certification dans le domaine de la signature électronique et annexe (RS 943.032.1).