14.015

Message relatif à la révision totale de la loi sur la signature électronique (SCSE)

du 15 janvier 2014

Messieurs les Présidents,
Mesdames, Messieurs,

Par ce message, nous vous soumettons, en vous priant de l'approuver, un projet de révision totale de la loi sur la signature électronique.

Nous vous prions d'agréer, Messieurs les Présidents, Mesdames, Messieurs, l'assurance de notre haute considération.

15 janvier 2014

Au nom du Conseil fédéral suisse:

Le président de la Confédération, Didier Burkhalter
La chancelière de la Confédération, Corina Casanova

Condensé

Le présent projet règle l'utilisation des certificats numériques destinés à des personnes morales et des autorités, répondant en cela à un besoin des milieux économiques et des administrations, qui désirent une règlementation moderne et facile à appliquer.

Contexte

La loi fédérale de 2003 sur la signature électronique (SCSE) réserve aux personnes physiques la signature électronique qualifiée, qui est équivalente à la signature manuscrite selon le CO. Cette restriction avait pour but d'éviter d'ouvrir une brèche dans les grands principes du droit de la représentation. On avait déjà, à l'époque, mené une discussion approfondie sur l'opportunité d'un certificat soumis à une règlementation légale et destiné aux personnes morales et aux autorités. On s'était demandé si, en réservant la signature électronique aux personnes physiques, on ne plaçait pas la barre trop haut, compliquant notamment son application dans les échanges en masse.

Contenu du projet

La révision proposée confère au Conseil fédéral la compétence de règlementer deux applications des certificats numériques en plus de la signature électronique qualifiée, qui continuera d'être réservée aux personnes physiques: la signature électronique dite «règlementée», qui devra répondre à des critères moins stricts que la signature qualifiée, et le «cachet électronique règlementé», instrument réservé aux personnes morales et aux autorités. A la différence de la signature électronique qualifiée, ces deux instruments n'auront pas d'effets juridiques directs et serviront uniquement à prouver la provenance d'un document et à garantir que son contenu n'a pas été modifié par la suite.

Le Conseil fédéral règlera une autre application du certificat numérique, l'authentification sûre. La révision vise également une simplification et une harmonisation des dispositions législatives qui portent sur la signature ou le cachet électronique.

La nouvelle loi demeure fondée sur les mêmes conceptions et principes que ceux qui prévalent actuellement. Notamment, les produits fondés sur des certificats numériques ne sont pas réglés de manière exhaustive. La législation suisse restera en outre compatible avec la directive européenne.

Bien que la modification soit, matériellement, assez limitée, elle prend la forme d'une révision totale, en raison du grand nombre d'adaptations terminologique et de l'instauration de la signature règlementée qui requiert de reformuler de nombreux articles.

Table des matières

Message

1 Présentation du projet

1.1 Contexte

1.1.1 Analyse de la problématique

La loi du 19 décembre 2003 sur la signature électronique (SCSE; RS *943.03*) réserve la signature électronique qualifiée, que le code des obligations (CO; RS *220*) assimile à la signature manuscrite, aux personnes physiques. Cette restriction avait pour but d'éviter d'ouvrir une brèche dans les grands principes du droit de la représentation. La question d'un certificat règlementé destiné aux personnes morales et aux autorités avait déjà été longuement débattue à l'époque; on s'était demandé si, en réservant la signature électronique qualifiée aux personnes physiques, on ne plaçait pas la barre trop haut, compliquant notamment son application dans les échanges en 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 de procéder à un examen approfondi et d'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.

Le bilan de cette analyse est présenté dans le Rapport 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 ch. 3.3.3), qui a été rédigé par le groupe de travail interdépartemental constitué à cette occasion. Le 11 juin 2010, le Conseil fédéral a pris acte de ce rapport et chargé le DFJP d'examiner quelles mesures législatives devaient être prises concrètement.

De fait, un certificat des entreprises ou des autorités serait grandement nécessaire pour leurs échanges électroniques. Dans les échanges en masse, notamment, il est difficile de signer chaque écrit selon les règles, sur la base d'un certificat attaché à une personne physique. Dans ces cas-là, on utilise habituellement la signature dite avancée, qui se réfère à l'entreprise, voire au serveur, en excluant, si nécessaire, par contrat les exceptions pour vice de forme. L'inconvénient de cette méthode est que la qualité du certificat ne répond pas à des critères fixés par l'Etat mais qu'il faut la déterminer dans le cas d'espèce.

Le problème décrit ne touche pas uniquement les entreprises privées; il touche aussi les autorités, par exemple concernant la production automatique d'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 (préposé au registre par exemple), certificat qui, en cas de changement de personnel, est renouvelé, soit un certificat avancé ne répondant à aucun critère de qualité défini dans la loi.

Dans le seul cas où il existe un important volume d'échanges entre les entreprises et les autorités, à savoir la transmission des factures des entreprises aux services de la TVA à des fins de déduction de l'impôt préalable, le Département fédéral des finances a défini par voie d'ordonnance et imposé son propre certificat, destiné aux

entreprises. Cette initiative a été à l'origine de la motion Baumann évoquée précédemment et en partie aussi de la présente révision.

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.

L'objectif principal de la présente révision est donc de prévoir un instrument permettant de garantir la provenance et l'intégrité d'un document émanant d'une personne morale ou d'une autorité.

Elle vise également à régler l'authentification électronique, à éliminer quelques incertitudes concernant l'utilisation des documents signés électroniquement et à harmoniser la terminologie.

1.1.2 Objectifs de la révision

La révision devait répondre à trois objectifs principaux.

- Premièrement, introduire dans la loi un nouveau type de signature qui pourra être utilisé aussi par les personnes morales et les autorités pour garantir la provenance et l'intégrité d'un document, et qui sera éventuellement adapté aux exigences d'une utilisation commerciale dans les dispositions d'exécution. Lorsqu'il devra définir des exigences de forme, le législateur pourra ainsi choisir entre la signature électronique qualifiée qui existe déjà et le nouvel instrument.
- 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 accompagnée d'un horodatage.

Les délégations de compétence prévues par la SCSE actuelle 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 applications des certificats, en particulier l'authentification, et d'élaborer des prescriptions techniques en la matière.

Le but n'est pas de modifier les conceptions et les principes existants (notamment la règlementation non exhaustive des produits de certification) 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, on s'est 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 (ci-après fournisseurs) 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 règlementé, du certificat qualifié et de l'horodatage qualifié.
- *Tout fournisseur reconnu au sens de la SCSE* pourra proposer tous les produits susmentionnés, plus les trois produits régis par la SCSE, à savoir:
  - le certificat règlementé (nouveau):
    - pour les personnes physiques, les personnes morales et les autorités
    - pour toute sorte d'utilisations (sauf pour la signature électronique qualifiée) selon les dispositions d'exécution du Conseil fédéral ou de l'Office fédéral de la communication (OFCOM);
  - le certificat qualifié (inchangé)
    - uniquement pour les personnes physiques
    - uniquement pour la signature électronique qualifiée;
  - l'horodatage qualifié (nouveau).

1.2 Nouvelle règlementation proposée

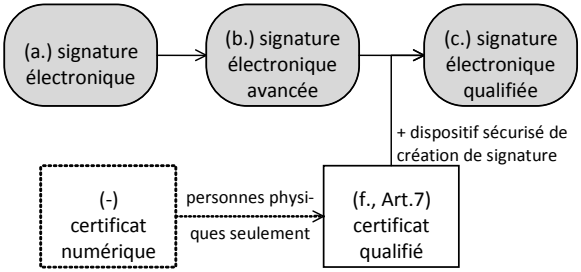
1.2.1 Certificat règlementé, signature électronique règlementée et cachet électronique règlementé

La *loi actuelle* définit – en conformité avec la directive de l'UE – la signature électronique qualifiée, créée sur la base d'un certificat qualifié, et confère, dans son art. 6, au Conseil fédéral la compétence de régler l'élaboration des clefs cryptographiques nécessaires 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 SCSE 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 à plus d'exigences que la signature électronique avancée, laquelle doit remplir des conditions plus strictes que la signature électronique.

Graphique 1

Schéma des signatures électroniques dans la loi actuelle

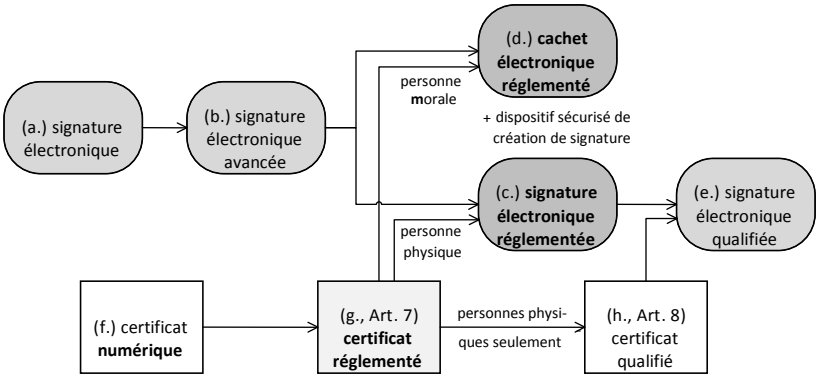


Le *projet de loi* ne modifie pas fondamentalement cette structure, mais il insère un nouvel échelon entre la signature avancée et la signature qualifiée: la «signature règlementée», pour les personnes physiques, et le «cachet règlementé», pour les personnes morales et les autorités.

En d'autres termes, les deux premiers niveaux de signature sont conservés: ce sont la signature électronique et la signature électronique avancée. Un troisième niveau est créé – signature électronique règlementée, pour les personnes physiques, et cachet électronique règlementé, pour les personnes morales et les autorités – avant la signature électronique qualifiée, qui fait office de quatrième niveau. Cette dernière doit satisfaire à plus d'exigences que la signature électronique règlementée, laquelle doit remplir des conditions plus strictes que la signature électronique avancée.

Graphique 2

Schéma des signatures électroniques dans le projet de loi



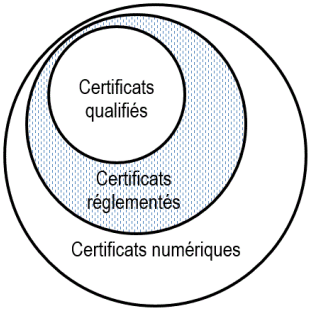
Comme dans le droit actuel, la signature électronique qualifiée continuera de reposer sur un certificat qualifié. Le projet crée en outre un «certificat règlementé» répondant à des exigences moins strictes. Il sera utilisé:

– pour la signature électronique règlementée, réservée aux personnes physiques;
– pour le cachet électronique règlementé, réservé aux personnes morales et aux autorités;
– pour d'autres applications définies par les dispositions d'exécution, notamment l'authentification sûre.

Le Conseil fédéral aura la compétence de régler l'élaboration et l'utilisation des clefs correspondant à ce type de certificat et la question du format.

Graphique 3

Schéma des certificats numériques dans le projet de loi



Il faut noter que le certificat numérique, qui est déjà à la base du certificat qualifié, n'avait pas été jusque-là défini dans la loi.

Le certificat règlementé est une forme particulière de certificat numérique et le certificat qualifié une forme particulière de certificat règlementé. On peut en déduire qu'un certificat qualifié est aussi un certificat règlementé 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 règlementé réside dans le fait que le premier ne sera destiné qu'aux personnes physiques, contrairement au deuxième. Il y a lieu de noter que le certificat règlementé ne peut pas être un pur certificat machine, c'est-à-dire qu'il ne peut être établi simplement pour une machine telle qu'un serveur.

Pour alléger la formulation des dispositions, on précisera dans la définition du certificat règlementé et du certificat qualifié que ceux-ci doivent être délivrés par un fournisseur reconnu de services de certification (art. 2, let. g et h), ce qui permettra de désigner plus simplement 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 en effet 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 pourrait donc être délivré par un fournisseur 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 exclut cette hypothèse par la nouvelle définition. Grâce à la précision apportée dans la SCSE, on pourra simplement dire: « Est considérée comme reconnue la signature électronique qualifiée au sens de la SCSE ».

Même si le 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, le stockage et l'utilisation des clefs cryptographiques à chaque fois qu'il est question d'une nouvelle forme d'utilisation d'un certificat – signature électronique règlementée, cachet électronique règlementé, signature électronique qualifiée, authentification, etc. –, l'art. 6 a été reformulé de manière à s'appliquer à n'importe quelle utilisation des 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 règlera l'élaboration, le stockage et l'utilisation des clefs cryptographiques pour un deuxième type de certificat, propre à la Suisse, et pour d'autres applications.

1.2.2 Délégation de compétence concernant l'authentification

Afin que les échanges électroniques entre particuliers et avec les autorités se développent en Suisse, il importe que les partenaires impliqués soient certains de l'identité de leur interlocuteur, c'est-à-dire qu'ils soient sûrs que cet interlocuteur est bien celui qu'il prétend être.

Lorsque la SCSE a été conçue, il y a de cela une dizaine d'années, on partait du principe que les échanges électroniques seraient principalement basés sur des 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 l'identité de l'expéditeur. Ce modèle de communication ne s'est toutefois imposé que dans certains domaines et est plutôt utilisé pour les échanges entre partenaires d'affaires professionnels. En revanche, un autre modèle de communication en ligne se développe de plus en plus, celui où une partie – la plupart du temps, le client ou le citoyen – s'inscrit sur un système d'application ou le portail de l'autre partie – 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 l'authentification entre programmes, 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 réclament depuis longtemps, pour certains types d'authentification, un certificat qui, par son caractère officiel et les exigences légales de qualité auxquelles il serait soumis, apporterait une sécurité accrue aux échanges. Plusieurs applications utilisées ou développées aujourd'hui répondent à des critères élevés de protection des données et de sécurité de l'information, notamment le dossier du patient dans le domaine de la cybersanté, domaine

dans lequel une authentification forte fondée sur un haut niveau de certification serait fort souhaitable.

Aujourd'hui, le certificat qualifié sert à créer 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, nous prévoyons de continuer à limiter son usage à la signature électronique.

Le nouveau certificat règlementé, lui, soumis à des exigences un peu moins sévères et ne donnera pas lieu à une utilisation aussi spécialisée. Il pourra, sur le plan juridique, être utilisé pour les signatures et cachets électroniques applicables dans divers domaines, notamment l'archivage, la préservation de l'intégrité de logiciels ou la signature de courriers électroniques, mais aussi pour l'authentification ou d'autres applications de sécurité telles que celles qui requièrent un certificat SSL.

De ce fait, 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 plus de «clefs de signature» ni de «clefs de vérification de signature» mais de «clefs cryptographiques publiques» et de «clefs cryptographiques privées». Cette formulation, plus ouverte, ne change rien sur le plan matériel pour le certificat qualifié, dont la seule application possible reste la signature.

1.2.3 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 accompagne obligatoirement la signature électronique qualifiée. L'horodatage consiste à associer une date et une heure officielles à un ensemble de 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, la date et l'heure 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 sont 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 horodater 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, apposer sur place sa signature sur les statuts ou les procès-verbaux pour les authentifier. Cette condition est devenue aujourd'hui beaucoup plus facile à remplir et ne devrait plus être un problème du tout dans quelques années.

Dans le cadre des travaux préparatoires, on a examiné trois options pour ce qui est de l'horodatage de la signature électronique qualifiée; elles ont été soumises à la consultation:

1. la signature électronique qualifiée s'accompagne obligatoirement de l'horodatage opéré par un fournisseur reconnu;
2. la loi définit deux types de signatures électroniques qualifiées, l'une avec horodatage, l'autre sans;
3. l'horodatage n'est pas requis par la SCSE, mais le CO en fait une condition pour que la signature électronique qualifiée soit assimilée à la signature manuscrite.

A l'issue de la consultation, nous avons opté pour la troisième solution. La SCSE ne s'exprimera pas sur la question, l'obligation d'horodater devant être fixée selon les nécessités du domaine. En l'occurrence, l'art. 14, al. 2bis, CO, qui règle les conditions auxquelles la signature électronique qualifiée est assimilée à la signature manuscrite en vue du respect de la forme écrite, requiert l'horodatage.

1.2.4 Adaptations terminologiques

Comme on l'a dit au ch. 1.2.1, la modification de la définition des certificats permettra d'utiliser une expression beaucoup plus courte dans les autres actes législatifs lorsque ceux-ci règlent les exigences de la forme écrite, à savoir «signature qualifiée (ou règlementée) au sens de la SCSE», sans plus de référence aux fournisseurs reconnus.

D'une manière générale, on a veillé à ce qu'il soit possible à l'avenir de se référer simplement aux notions de la SCSE. On a précisé à l'art. 13 (actuel art. 12) que l'horodatage électronique était «qualifié» lorsqu'il est offert par des fournisseurs reconnus, pour le distinguer clairement de l'horodatage de fournisseurs quelconques.

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 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 puisqu'opéré par un fournisseur reconnu, on pourra directement utiliser l'expression «horodatage électronique qualifié au sens de la SCSE».

1.2.5 Modification d'autres actes législatifs

Plusieurs lois et ordonnances actuelles se réfèrent aux notions de la SCSE, en particulier bien évidemment à celle de signature électronique qualifiée. Il y sera à l'avenir question, généralement, de la signature ou du cachet électronique règlementés. La signature électronique qualifiée ne sera requise que dans les cas 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 que nécessaire.

Au cours de ces dernières années, toutes les lois de procédure de la Confédération ont été complétées par des dispositions réglant la transmission électronique des écrits à l'autorité et des décisions aux justiciables. Les conceptions et les formulations ne sont pas entièrement uniformes. Nous saisissons l'occasion du présent

projet pour harmoniser autant que possible ces dispositions. Les participants à la consultation ayant souhaité une harmonisation plus forte que ce que prévoyait l'avant-projet, nous avons fait un effort en ce sens. Cependant, aller plus loin demanderait une intervention trop importante dans les codes de procédure et requerrait une règlementation plus globale de la transmission électronique. Le Conseil fédéral réalisera ces objectifs dans un projet à part, qu'il a demandé au DFJP, fin 2012, de réaliser conjointement avec le Département fédéral de l'environnement, des transports, de l'énergie et de la communication et le Département fédéral des finances.

1.3 Motivation et appréciation de la solution retenue

1.3.1 Création du certificat règlementé et du cachet électronique pour les entreprises et les autorités

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 pourraient également être délivrés à des personnes morales. Le projet sur lequel portait le message de 2001 prévoyait encore que ces dernières pouvaient l'obtenir; 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. De fait, 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 au nom de laquelle le certificat était délivré. Afin de respecter un principe fondamental du droit de la représentation, qui est que les personnes morales ne peuvent agir en fin de compte qu'à travers des personnes physiques (organes et auxiliaires, notamment), le législateur a finalement restreint l'utilisation du certificat qualifié aux personnes physiques. Ces considérations restent de mise.

Toutefois, depuis l'entrée en vigueur de la SCSE, la pratique a montré la nécessité, dans le domaine du commerce électronique et des échanges électroniques avec les pouvoirs publics, d'un certificat propre aux entreprises et aux autorités, obéissant à des règles fixées par l'Etat et garantissant par là le respect d'exigences minimales (preuve de la provenance, intégrité des données, etc.). Il n'est en effet guère pratique, lorsqu'on effectue des opérations de masse, de devoir signer les communications par une signature qualifiée en introduisant à chaque fois un code NIP, alors qu'elles ne doivent satisfaire qu'à des exigences minimales.

La présente révision vise à combler ce manque. L'option choisie n'a pas été d'étendre le cercle des titulaires potentiels du certificat qualifié, comme on l'avait envisagé à une époque, mais de créer un certificat «intermédiaire» entre le certificat avancé et le certificat qualifié. Ce certificat, nommé «certificat règlementé», correspondra à peu de choses près aux critères du certificat qualifié et pourra être délivré tant au nom de personnes morales et d'autorités qu'au nom de personnes physiques.

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 ces produits dans les relations juridiques, notamment les effets juridiques du certificat règlementé et du cachet ou de la signature règlementée qu'il sert à produire, seront fixés dans les lois concernées, par exemple dans les lois

de procédure. L'art. 1, al. 2, le spécifie explicitement. Dans les transactions qui ne sont soumises à aucune exigence légale de forme, les parties pourront convenir que leur déclaration de volonté n'est valable que si elle est munie d'un cachet électronique règlementé (basé sur un certificat règlementé), en se fondant sur l'art. 16 CO. Elles disposeront pour ce faire, ce qui n'est pas le cas aujourd'hui, d'un certificat et d'une procédure soumis à des exigences définies de manière uniforme, conformément aux vœux des milieux économiques.

Néanmoins, seule la signature électronique qualifiée sera assimilée à la signature manuscrite, comme le prévoit l'art. 14, al. 2bis, CO. Le document portant le cachet électronique ne remplira donc pas les exigences légales de la forme écrite (art. 12 ss CO). Par ailleurs, celui qui reçoit un document portant le cachet électronique d'une entreprise ne peut pas en déduire automatiquement que l'entreprise en question se trouve engagée juridiquement (cela vaut d'ailleurs également pour la signature électronique). Cette question se détermine exclusivement selon les principes du droit de la représentation, qui demeureront intouchés. Le destinataire sera néanmoins protégé par la clause de responsabilité de l'art. 59*a* CO, dont le champ d'application sera étendu aux certificats règlementés et donc au cachet électronique (voir le ch. 1.3.2).

Le cachet électronique instauré par la révision se fonde techniquement sur la même procédure que la signature électronique. Il vise le même but, au moins en partie, c'est-à-dire la preuve de la provenance et de l'intégrité des données. Un terme spécifique a été choisi dans le projet, mais l'avant-projet parlait encore de signature électronique à l'usage des personnes morales et des autorités.

Le terme «cachet électronique» s'inspire d'une proposition de règlement de l'Union européenne[1] qui a été adoptée par la Commission européenne le 4 juin 2012 et qui devrait remplacer la directive actuelle de l'UE. Il désigne le pendant de la signature électronique pour les personnes morales. Ce nouveau terme, choisi après la consultation, évitera les risques de mauvaise interprétation du terme de signature que nous avons exposés plus haut.

On notera toutefois que tant les spécialistes que le grand public utilisent depuis de nombreuses années le terme «signature électronique» en relation avec des certificats qui ne se rapportent pas à des personnes physiques. Il sera sans doute difficile au nouveau terme de s'implanter, même s'il convient mieux pour des raisons juridiques. Le cachet électronique s'appellera donc encore longtemps «signature électronique» dans les programmes de courrier électronique et les lecteurs de fichiers PDF, sans distinction entre les personnes physiques et les autres. Il n'y aurait pas de sens à ce que la Suisse introduise seule ce nouveau terme, mais elle emboîte ici le pas à l'UE.

1 Proposition de règlement du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, COM(2012) 238 final.

1.3.2 Remarque concernant la responsabilité du titulaire de clefs de signature selon l'art. 59*a* CO

L'art. 59*a* CO, instauré lors de l'adoption de la SCSE, fonde une responsabilité des titulaires de clefs cryptographiques à l'égard des tiers; il s'agissait là d'un élément essentiel de la notion de signature électronique qualifiée. Cette disposition s'applique exclusivement dans le cas particulier de la signature électronique: le destinataire du document signé n'est généralement pas lié par une relation contractuelle avec le fournisseur du certificat ni avec le signataire. Pour que la signature qualifiée corresponde à un degré élevé de confiance, tant le fournisseur du certificat (art. 17 du projet, art. 16 SCSE) que le titulaire du certificat (art. 59*a* CO) ont envers lui la responsabilité de faire preuve d'une certaine diligence dans l'accomplissement de leurs obligations.

Cette disposition est contestée depuis le début. Durant la consultation, plusieurs participants ont demandé qu'elle soit assouplie, voire supprimée, principalement pour le motif qu'elle est trop sévère pour les titulaires de certificats et qu'elle empêche de nombreux utilisateurs potentiels de se servir de la signature électronique. Le Conseil fédéral a donc étudié en profondeur s'il fallait conserver, modifier ou abroger cet article.

L'analyse a porté sur l'ensemble de l'art. 59*a* CO, et non uniquement sur l'al. 1, seul touché par la révision. L'al. 2 précise que le titulaire est libéré de sa responsabilité s'il peut établir de manière crédible qu'il a pris les mesures de sécurité raisonnablement imposées par les circonstances pour éviter que la clef de signature ne soit utilisée de façon abusive. L'al. 3 charge le Conseil fédéral d'arrêter les mesures de sécurité à prendre. Les documents relatifs à la SCSE, en particulier le message, ne commentent pas tous les aspects de la disposition, car l'art. 59*a* CO a été considérablement modifié au cours des délibérations parlementaires. Il n'existe manifestement pas de jurisprudence relative à cet article et la doctrine ne s'est prononcée que de manière fragmentaire sur le sujet.

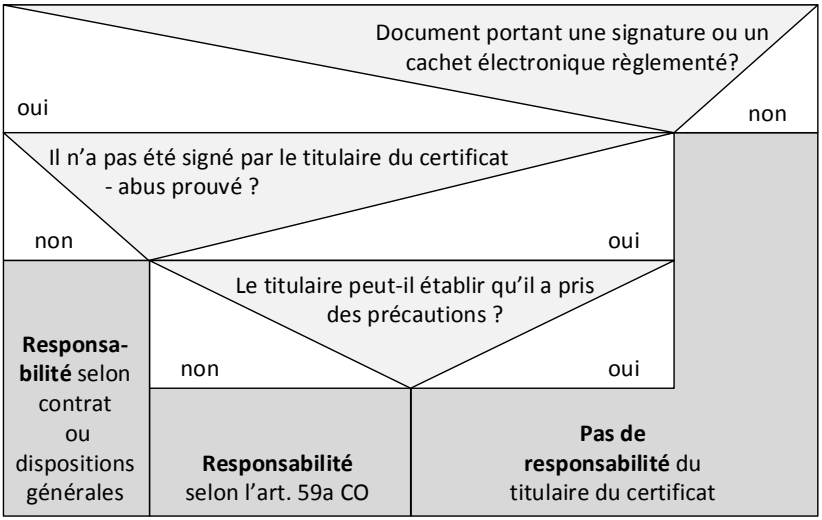
La signature électronique remplit son objectif lorsque le destinataire du document obtient une certitude supplémentaire quant à l'authenticité de l'expéditeur et du contenu. Sur le plan technique, elle est très fiable à cet égard. Pour générer une signature valable, il faut connaître le code NIP et avoir en même temps accès à la carte de signature (qui ne doit pas avoir été annulée). Le point faible de la procédure est que le destinataire ne peut pas savoir si c'est bien le titulaire de la signature lui-même ou une autre personne qui a rempli ces conditions. Si une personne imprudente ne prend pas les précautions voulues pour conserver en lieu sûr son code et sa carte, ou qu'elle les utilise sur un ordinateur mal protégé, un détournement par un tiers est possible.

C'est à cet égard que l'art. 59*a* CO donne au destinataire du document une sécurité supplémentaire, tout en incitant le titulaire de la signature à faire preuve d'un minimum de précautions. En cas d'abus, si le titulaire ne peut pas établir de manière crédible qu'il a pris des précautions raisonnables, il devra répondre du dommage que le destinataire du document signé a subi du fait qu'il s'est fié à un certificat qualifié.

Nous avons maintenu la conception de l'art. 59*a* CO, en l'étendant à tous les certificats règlementés et aux signatures et cachets fondés sur ces certificats, car, contrairement aux craintes exprimées par certains participants à la consultation, le domaine d'application de la responsabilité du titulaire des clefs est très limité.

- Pour que cet article s'applique, il faudra tout d'abord que le destinataire du document puisse produire un document électronique pourvu d'une signature ou d'un cachet électronique fondé sur un certificat règlementé (ou qualifié) valable de l'expéditeur. Il disposera alors d'une preuve très sûre, sur le plan technique, de l'authenticité du destinataire et du contenu.
- L'expéditeur pourra contester l'authenticité du document en arguant que ce n'est pas lui, mais un tiers, qui a signé le document électronique. La contestation devra reposer sur des motifs suffisants (art. 178 du code de procédure civile; RS *272*). S'il ne parvient pas à fournir des motifs suffisants, il sera considéré juridiquement comme le signataire du document et devra répondre d'éventuels dommages selon les normes générales régissant la responsabilité.
- C'est seulement si le titulaire légal du certificat prouve que le document n'émane pas de lui que la règle spéciale de responsabilité de l'art. 59*a* CO s'appliquera. Sans cette disposition, le titulaire du certificat ne pourrait guère être amené à répondre du dommage selon les règles généralement applicables (par ex. de la responsabilité pour faute), car l'illicéité du fait dommageable est douteuse (on pourrait éventuellement invoquer l'art. 11 de l'ordonnance du 3 décembre 2004 sur la signature électronique; RS *943.032*); le destinataire devrait supporter les dommages éventuels. Rappelons que l'art. 59*a* CO ne s'appliquera pas si le document n'est pas signé sur la base d'un certificat règlementé (ou qualifié).
- Si le titulaire du certificat peut établir de manière crédible qu'il a usé de précautions, comme l'exige l'art. 59*a*, al. 2, CO, il ne sera pas tenu responsable. S'il n'y parvient pas, il répondra du dommage subi par le destinataire parce que celui-ci se sera fié à la signature (donc à un intérêt contractuel dit négatif).

Le cas classique, avec une signature électronique qualifiée, est le suivant: la titulaire établit de manière crédible qu'elle n'a pas pu signer parce qu'elle était hospitalisée, mais il n'est pas exclu qu'un collègue ou une autre personne soit entré dans son bureau et ait signé avec sa clef, car sa carte de signature et son code NIP sont laissés à la vue de tous. Si l'art. 59*a* CO était supprimé, elle ne devrait pas répondre du dommage, qui serait supporté par le destinataire du document portant sa signature. Conformément à l'al. 1, elle répond du dommage car elle n'a pas pris les mesures de précaution visées aux al. 2 et 3.



Un des objectifs importants de la législation sur les signatures ou les cachets électroniques fondés sur un certificat règlementé ou qualifié est l'instauration d'un certain degré de fiabilité; la clause de responsabilité y contribue. Le titulaire de la clef doit faire preuve d'un certain degré de diligence, ce qui n'est pas sans promouvoir la sécurité de la procédure. A son tour, cela accroît la confiance dans ce type de signatures, ce qui augmente leur valeur et leur intérêt.

1.3.3 Révision totale formelle

La révision qui nous occupe ici était supposée, à l'origine, être une révision partielle. Compte tenu du nombre relativement restreint d'objectifs (voir ch. 1.1.2), on pourrait continuer à la considérer comme telle. Cependant, comme la plupart des dispositions valent désormais non seulement pour le certificat qualifié, mais aussi pour les certificats règlementés, et que les clefs font l'objet d'une dénomination neutre dans tout le texte («clef cryptographique» en lieu et place de «clef de signature», etc.), la plupart des articles sont touchés. Voilà pourquoi, selon les critères usuels, la modification prend la forme d'une révision totale.

1.3.4 Procédure de consultation

Le projet a été soumis à une consultation du 29 mars au 6 juillet 2012. On trouvera la synthèse des résultats de la procédure de consultation sur le site de la Chancellerie (www.admin.ch > Droit fédéral > Procédures de consultation > Procédures de consultation terminées > 2012 > Département fédéral de justice et police).

Au cours de cette consultation, tous les cantons, tous les partis gouvernementaux, plusieurs organisations faîtières de l'économie et de nombreux autres organismes intéressés se sont prononcés. Les objectifs du projet, en particulier l'instauration

d'un certificat règlementé pour les personnes morales et les autorités, ont été très largement approuvés.

Les divergences les plus importantes concernaient les points suivants (qui ne relèvent pas tous de la SCSE):

- Trois cantons et quelques entreprises spécialisées rejettent l'*idée d'un horodatage qualifié* comme condition de l'égalité entre signature électronique et signature manuscrite à l'art. 14, al. 2bis, CO. Ils ne contestent pas le gain de sécurité, mais ils considèrent comme trop contraignante la nécessité d'une liaison Internet au moment de la création de la signature.
- Trois cantons et de nombreuses associations et entreprises du domaine de l'informatique désirent que la responsabilité du titulaire de la clef de signature au sens de l'art. 59*a* CO soit assouplie ou abolie. Le Conseil fédéral a donc demandé une étude spécifique de ce point. Elle a fait paraître que l'interprétation de l'article était peu claire et que la responsabilité était souvent comprise à tort comme étant plus stricte qu'elle n'est supposée l'être. Le ch. 1.3.2 fournit des explications détaillées sur la question de cette responsabilité.
- Plusieurs organismes intéressés, notamment la Fédération suisse des avocats, souhaitent que les échanges avec les autorités soient règlementés de manière exhaustive et bien plus poussée. Le Conseil fédéral est ouvert à ces remarques mais elles ne sauraient s'intégrer dans ce projet relativement pointu. Entre-temps, une partie des exigences formulées a été reprise dans d'autres projets de loi.

Deux éléments nouveaux sont venus s'ajouter au projet:

- le terme spécifique de «cachet électronique» pour la signature électronique des personnes morales et des autorités, inspiré de la proposition de règlement de l'UE, qui n'a été publiée qu'après la consultation;
- l'harmonisation plus poussée des dispositions relatives à la transmission électronique dans les lois de procédure de la Confédération; elle était encore rudimentaire dans l'avant-projet.

1.4 Corrélation entre les tâches et les ressources

La SCSE confie aux acteurs privés la production des certificats qui obéissent aux critères légaux et des produits fondés sur ces certificats. L'Etat ne met à leur disposition aucune infrastructure ni aucune prestation, se contentant de règlementer ce domaine dans la SCSE et dans un ensemble assez fourni de dispositions d'ordonnance et de prescriptions techniques et administratives. Ces tâches peuvent être accomplies avec les moyens existants.

1.5 Comparaison avec le droit étranger, notamment européen

La compatibilité avec le droit européen est un des axiomes de la législation sur la signature électronique et sur les autres applications des certificats numériques. Cela va de soi, vu le caractère international des transactions électroniques et les intenses échanges commerciaux entre la Suisse et ses voisins européens (voir le ch. 1.1.2 sur les objectifs de la révision). La SCSE est un acte de mise en œuvre autonome de la directive de l'UE, avec quelques simplifications soigneusement choisies. Le souci d'assurer la compatibilité avec le droit européen et de garantir une reconnaissance internationale explique pourquoi la terminologie et certains aspects formels de la directive ont été repris dans une mesure supérieure à l'usage, ce qui fait de la SCSE un instrument exotique au sein du droit suisse. Il ne fallait pas ajouter à la grande complexité technique de cette règlementation les difficultés inhérentes à une adaptation aux us suisses en matière de législation. Cette façon de procéder avait semblé acceptable au regard de la technicité de la loi.

L'UE travaille depuis quelques années à la révision de sa directive, dont elle entend étendre considérablement l'objet. Le 4 juin 2012, peu avant l'ouverture de la consultation relative à la présente révision, la Commission européenne a adopté une proposition de règlement en la matière, à l'intention du Parlement européen et du Conseil[2]. La question s'est donc posée de savoir s'il fallait tenir compte de ces adaptations dans les travaux législatifs en cours, mais cela n'a finalement pas semblé souhaitable. Il s'écoulera encore beaucoup de temps avant que le règlement européen soit définitivement adopté, que son contenu ait été soigneusement étudié et qu'il soit transposé dans le droit suisse. La proposition de règlement de l'UE porte en outre sur deux domaines importants sur lesquels la Suisse doit mener un débat avant de savoir si elle entend les reprendre: la transmission électronique sûre et l'identité électronique. Le Conseil fédéral a lancé des travaux législatifs sur ces questions fin 2012. Il serait dommage de retarder la présente révision de plusieurs années alors que les exigences qui la motivent sont connues depuis un certain temps. A l'heure actuelle, aucune disposition de la révision n'est contraire à la future règlementation européenne.

1.6 Mise en œuvre

La nouvelle loi donne au Conseil fédéral la compétence de régler d'autres produits fondés sur les certificats que la signature électronique qualifiée. Les spécialistes de la branche désirent une règlementation relativement complète du cachet électronique règlementé. Il faudra aussi définir les modalités de l'identification électronique forte.

La révision ne déploiera d'effets que si les fournisseurs développent et commercialisent des produits.

2 Proposition de règlement du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, COM(2012) 238 final.

1.7 Classement d'interventions parlementaires

La présente révision ne concrétise aucune intervention parlementaire, mais elle a été suscitée entre autres par la motion Baumann 08.3741 «Certification obligatoire contraire au droit dans l'ordonnance relative à la loi sur la TVA», liquidée depuis lors.

2 Commentaire des dispositions

2.1 Loi sur la signature électronique

2.1.1 Titre de la loi

L'extension du champ d'application de la SCSE à d'autres produits fondés sur des certificats se reflète dans le nouveau titre. Il s'agit aujourd'hui principalement de l'authentification et du cachet électronique, mais d'autres applications pourraient être concernées, raison pour laquelle on a opté pour une formulation ouverte.

2.1.2 Section 1 Dispositions générales

Art. 1 Objet et but

L'objet de la SCSE a souvent donné lieu à des erreurs d'interprétation. Certains considèrent 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 (let. a) à l'al. 1 vise à clarifier son objet.

La nouvelle loi ne règlera et ne favorisera plus seulement la signature électronique (qualifiée) en tant qu'application des certificats; elle couvrira aussi les signatures électroniques en général et d'autres applications de certificats règlementés. Aussi les al. 1, let. a (al. 1, let. b, du projet), et 2, let. b (al. 3, let. b, du projet), ont-ils été complétés.

Le nouvel al. 2 tient compte des craintes exposées au ch. 1.3.1 concernant le fait qu'on puisse croire à tort qu'un certificat règlementé 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 la loi ou éventuellement par un contrat en fonction du contexte.

A l'al. 3, la let. b est étendue en fonction du nouveau champ d'application de la loi.

Art. 2 Définitions

Les nouvelles définitions ont été placées en fonction des règles de la systématique, si bien que certaines lettres ont été déplacées (let. e, h. k et l du projet).

- *Let. c: signature électronique règlementée*
  La définition de la signature règlementée – insérée entre celle de la signature électronique avancée et celle de la signature électronique qualifiée – s'inspire de la définition de la signature électronique qualifiée. La première forme particulière de signature avancée sera donc la signature électronique règlementée (et non plus la signature électronique qualifiée, comme c'est le cas actuellement). Elle se distingue du cachet électronique en ce qu'elle est limitée aux personnes physiques.
- *Let. d: cachet électronique règlementé*
  Pendant de la signature électronique règlementée, le cachet électronique règlementé est limité aux personnes morales et aux autorités. 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. On trouvera de plus amples explications à ce sujet dans le commentaire de l'art. 7.
- *Let. e: signature électronique qualifiée*
  Actuellement définie à la let. c, elle est une forme particulière de la signature électronique règlementée, mais elle requiert un certificat (c'est-à-dire une paire de clefs) qualifié.
- Les définitions de «clef de signature» et de «clef de vérification de signature» ont été supprimées (let. d et e de la loi en vigueur) parce que les applications de clefs cryptographiques sont désormais désignées de manière générique; on parlera donc uniquement de «clef cryptographique privée» et de «clef cryptographique publique».
- *Let. f: certificat numérique*
  Actuellement, cette notion apparaît dans la définition du «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. Elle n'est définie que dans la législation d'exécution. L'ajout de cette nouvelle définition dans la loi n'entraîne aucune modification matérielle mais permet d'assurer une meilleure compréhension et une meilleure cohérence.

  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 règlementé ou un certificat qualifié. Dans la terminologie spécialisée anglaise, on utilise souvent le concept d'«*entity*». Nous avons choisi le terme «titulaire», estimant que le calque de l'anglais («entité») ou une solution telle qu'«objet» n'étaient pas suffisamment clairs.
- *Let. g: certificat règlementé*
  La définition du certificat règlementé 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 généralement utilisable que le certificat qualifié, dont il constitue la base.

Pour simplifier les citations dans les autres actes, on a précisé que tout certificat règlementé devait être délivré par un fournisseur reconnu.

– *Let. h: 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 règlementé introduit à la let. g 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 à tout certificat règlementé –, les exigences auxquelles il sera soumis sont les mêmes qu'aujourd'hui.

– *Let. i: horodatage électronique*
  Alors qu'il apparaît aujourd'hui directement à l'art. 12, il a semblé préférable, pour des raisons de systématique, de le définir avec les autres termes de la loi.

– *Let. j: horodatage électronique qualifié*
  L'horodatage peut être qualifié, c'est-à-dire qu'il peut être opéré par un fournisseur reconnu. L'art. 13 du projet ne règlera plus que l'obligation d'offrir un horodatage qualifié.

2.1.3 Section 2 Reconnaissance des fournisseurs

Aucun changement n'est 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 proposant des certificats règlementés mais non qualifiés et une autre pour les fournisseurs proposant 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 règlementés, puisque les certificats qualifiés sont des certificats règlementés soumis à des exigences supplémentaires. Les fournisseurs déjà reconnus pourront donc à l'avenir proposer un autre type de certificat réglé par la loi. Ils pourront bien entendu continuer de délivrer d'autres types de certificats qui ne sont pas prévus par la loi.

On s'est contenté, à l'art. 3, al. 1, let. f, d'adapter les renvois aux règles en matière de cessation d'activité (nouvel art. 14) et de responsabilité (nouvel art. 17). L'art. 4, al. 2, a été retouché pour tenir compte du fait qu'il existe aujourd'hui un organisme d'accréditation.

2.1.4 Section 3 Elaboration, stockage et utilisation de clefs cryptographiques

Le titre actuel «Elaboration et utilisation de clés de signature et de vérification de signature» doit être remplacé par un titre plus général car, dans cette section, il sera également question des clefs utilisées pour l'authentification, pour le cachet électronique ou pour d'autres applications des 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 règlementés sont ici visées.

Art. 6

L'art. 6 de la loi en vigueur, qui reprend le contenu de l'annexe III de la directive de l'UE, traite seulement de la signature. S'y ajoutera désormais le cachet électronique. Le projet confère au Conseil fédéral – comme on l'a expliqué au ch. 1.2.1 – la compétence de régler d'autres applications des certificats et des clefs, en particulier l'authentification. C'est pourquoi cet article ne parle plus de «signature» ou de «vérification de signature» mais d'«utilisation des clefs cryptographiques» en général.

Cette délégation de compétence habilitera le Conseil fédéral à régler toute combinaison de certificats et d'applications, sans se limiter par exemple à une application par type de certificat. Toutefois, les produits en question sont aujourd'hui:

1. le certificat qualifié pour la signature électronique qualifiée, réservé aux personnes physiques (déjà soumis à la loi);
2. le certificat règlementé pour la signature électronique règlementée, réservé aux personnes physiques;
3. le certificat règlementé pour le cachet électronique règlementé, réservé aux personnes morales et aux autorités;
4. le certificat règlementé pour l'authentification forte (preuve de l'identité en ligne, eID), réservé aux personnes physiques.

Il ne faut pas oublier qu'à côté des produits obéissant à des critères définis dans la loi, qui veut peut offrir une multitude de certificats non règlementés et de produits analogues pour des usages divers.

Actuellement, le titre de la section cite «l'élaboration et l'utilisation» de clefs, alors que l'al. 1 de l'art. 6 règle l'élaboration et l'al. 2 la création des clefs. Rien ne justifie ces variations, aussi avons-nous utilisé l'expression «élaboration, stockage et utilisation» de manière uniforme.

L'al. 2, let. a, exige que les clefs cryptographiques (dans la loi actuelle les clefs de signature) «ne puissent, pratiquement, se rencontrer qu'une seule fois». Lors de la consultation, plusieurs fournisseurs ont souligné qu'ils devaient faire une copie de sauvegarde de la clef privée afin de garantir la sécurité de la production de signatures sur le serveur et qu'ils craignaient que cette disposition ne les en empêche. Ce n'est pas le cas. L'étude de la genèse de cette norme montre qu'il s'agissait d'exiger que la clef soit unique et que deux clefs identiques ne puissent pas être attribuées à deux personnes différentes. Il n'est donc pas interdit de faire une copie de sauve-

garde d'une clef du moment que celle-ci demeure attribuée à une personne unique et que la copie est conservée dans les mêmes conditions de sécurité que l'original.

L'art. 6, al. 3, actuel concernant le processus de vérification de la signature est repris presque mot pour mot de l'annexe IV de la directive de l'UE. A plusieurs égards, il fait figure de corps étranger dans la loi car il ne formule qu'une recommandation et s'adresse à des destinataires particuliers, difficilement identifiables, principalement les fournisseurs de lecteurs de fichiers 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, en la formulant sous forme d'habilitation du Conseil fédéral. Finalement, on a préféré la supprimer, considérant qu'elle n'avait qu'une valeur déclaratoire, était impossible à mettre en œuvre et ne répondait à 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 règlementés

Comme cette section portera désormais sur le certificat règlementé, dont le certificat qualifié ne sera plus qu'une forme particulière, le titre original «Certificats qualifiés» a été remplacé par «Certificats règlementés».

Art. 7 Conditions applicables aux certificats règlementés

La nouvelle disposition reprend, sur le plan matériel, l'essentiel des exigences posées aux certificats qualifiés (art. 7 actuel). 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 règlementés non qualifiés peuvent aussi être délivrés au nom de personnes morales et d'autorités. Cette spécificité, bien qu'elle ressorte de l'al. 2, a été mise en évidence à l'al. 1.

Les «entités IDE» au sens de la LIDE englobent la grande majorité des personnes morales mais aussi les autorités. Elles comprennent les sujets de droit inscrits au registre du commerce (art. 3, al. 1, let. c, ch. 1, LIDE) mais aussi d'autres personnes morales. Parmi les entités IDE figurent entre autres les autorités administratives et les tribunaux (art. 3, al. 1, let. c, ch. 7, LIDE). Les seules personnes morales à ne pas être ici concernées seront 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, les exclure délibérément. Une personne morale qui n'a pas un profil public suffisant pour remplir 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 pas se voir attribuer une identité électronique sous forme de certificat règlementé. La vérification de l'identité par le fournisseur pourrait en effet se révéler compliquée. Si une telle personne veut tout de même prendre part à des échanges électroniques formels – ce qui est assez improbable –, elle pourra très bien le faire par le biais d'une personne physique qui la représente.

Al. 2:

Le champ d'application de la let. b a été étendu aux certificats règlementés, 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 le 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 plus question du «titulaire de la clef de vérification de signature» 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 des certificats et, en outre, de corriger un défaut datant de l'époque où la loi a été élaborée; il aurait en effet dû être question de «clef de signature» – comme à l'actuel al. 2, let. a – et non de «clef de vérification de signature». 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 autorise les pseudonymes, comme aujourd'hui. Elle vaut seulement pour les personnes physiques. La let. e prévoit que le certificat contient le numéro unique d'identification des entreprises des identités IDE.

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

L'actuelle let. g, qui prévoit que le certificat doit contenir des informations sur la reconnaissance du fournisseur, a été biffée car seule la Suisse exige cet élément.

Let. h: la création du cachet règlementé fondé sur un certificat règlementé, qui donne la possibilité aux personnes morales d'utiliser une signature répondant à des exigences de qualité définies par la loi, permet de corriger une anomalie: aujourd'hui, les fournisseurs sont les seules personnes non physiques à recevoir un certificat qualifié et donc à avoir une signature qualifiée. Il en ira de même pour l'horodatage.

Al. 3:

L'actuel al. 2, let. a, est scindé en deux pour des raisons de technique législative: la nouvelle let. a mentionne les qualités spécifiques du titulaire de la clef, qui peuvent être inclues dans le certificat, et cite à titre d'exemple les qualifications professionnelles, qui sont souvent indiquées dans la pratique.

La let. b mentionne les pouvoirs de représentation, qui restent naturellement réservés aux personnes physiques. Dans le cadre des travaux préparatoires, on a examiné la possibilité de ne faire figurer cette mention que dans les certificats qualifiés, mais on n'a trouvé aucune raison majeure pour imposer une telle restriction.

Les let. c et d reprennent les actuelles let. b et c, avec quelques retouches visant à clarifier le texte.

Art. 8 Conditions supplémentaires applicables aux certificats qualifiés

L'art. 8 ne contient que les conditions supplémentaires que les certificats qualifiés, en tant que forme particulière des certificats règlementés (voir art. 2, let. g), doivent remplir. Ajoutées aux conditions énumérées à l'art. 7, elles correspondent sur le fond aux conditions auxquelles doivent actuellement satisfaire les certificats qualifiés, mais quelques points ont été explicités.

L'al. 1 énonce la principale différence entre le certificat qualifié et le certificat règlementé non qualifié, à savoir que le certificat qualifié 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 contraire au principe de la présente révision, qui veut que seules soient effectuées les modifications qui sont nécessaires pour remplir les objectifs visés. Cependant, à l'heure actuelle, elle est uniquement formulée dans les prescriptions techniques et administratives concernant les services de certification dans le domaine de la signature électronique (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 Adaptations opérées dans les sections 5 à 9

Renumérotation des articles

A partir de l'art. 9, les articles sont décalés d'un chiffre.

Remplacement de «certificat qualifié» par «certificat règlementé»

En principe, toutes les dispositions de la loi en vigueur qui portent sur le certificat qualifié concerneront à l'avenir les deux certificats réglés par la loi, à savoir le certificat règlementé (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 règlementé» (qui recouvre les deux notions) à chaque fois que cela s'avérait pertinent. On a exceptionnellement opté pour une formulation plus élégante mais le but visé était le même.

Cette adaptation concerne les (nouveaux) art. 9 à 14, 17, 18 et 21.

Remplacement de «signature électronique» et de «clef de signature» par des expressions plus générales

Comme la loi régira non seulement la signature, mais aussi d'autres applications des certificats numériques, les expressions «signature électronique» et «clef de signature» ont été remplacées par des expressions plus générales 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 des renvois (voir art. 16, 17, al. 3, et 18).

2.1.7 Section 5
Devoirs des fournisseurs reconnus

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

Les règles relatives à la procédure de demande d'un certificat règlementé vaudront également pour les entités IDE. A l'al. 1, la let. a règle la procédure applicable aux personnes physiques de la même manière qu'aujourd'hui; la let. b règle la procédure pour les entités IDE. Les personnes physiques qui sont également des entités IDE devront se présenter en personne, conformément à la let. a, pour demander un certificat règlementé.

Les al. 2 et 3 reprennent une partie de l'actuel al. 1, qui est quelque peu pléthorique. Les actuels al. 2, 3 et 4 deviennent donc les al. 4, 5 et 6.

Lors de la consultation, les fournisseurs et d'autres organismes intéressés ont souligné qu'il serait très compliqué, pour une grande entreprise, d'envoyer un représentant en personne pour chaque demande de certificat règlementé; ils ont suggéré que des demandes par la voie électronique soient possibles, du moins lorsque le pouvoir de représentation est inscrit dans le registre du commerce.

Le Conseil fédéral estime que ces questions peuvent être réglées au niveau de l'ordonnance, grâce à la délégation de compétence contenue dans cet article (al. 2 actuel, al. 4 du projet). Il sera indiqué de prévoir à ce niveau qu'une demande par la voie électronique est possible si le représentant de l'entreprise pourvoit la demande d'une signature électronique qualifiée et que son pouvoir de représentation est inscrit dans un registre public, qu'il s'agisse du registre du commerce ou d'un autre registre des autorités.

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

L'al. 1, let. b, a été complété: les fournisseurs pourront aussi 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.

Naturellement, les fournisseurs se fieront aux renseignements que leur auront fournis les organismes compétents cités à l'art. 9, al. 2. Ils ont d'ailleurs insisté sur ce point lors de la consultation. Par exemple, si l'appartenance d'une personne à une organisation professionnelle, confirmée par cette dernière, a été inscrite dans le certificat et que l'organisation en question communique ultérieurement que cette personne n'est plus membre, le fournisseur pourra annuler le certificat sur la foi de cette information.

Art. 12 (actuel art. 11) Service d'annuaire pour les certificats règlementés

La version allemande de l'al. 2 a été clarifiée.

Art. 13 (actuel art. 12) Horodatage électronique qualifié

L'horodatage électronique et l'horodatage électronique qualifié étant désormais définis à l'art. 2, let. i et j, l'art. 13 ne règle plus que l'obligation pour les fournisseurs reconnus d'offrir ce service.

Art. 15 (actuel art. 14) Protection des données

Une modification rédactionnelle a été apportée dans la version allemande.

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

On a ajouté l'adjectif qualificatif «reconnu», car cette disposition ne s'applique pas aux services de certification de n'importe quel type de fournisseur.

Art. 19 (actuel art. 18) Prescription

Une révision du droit de la prescription est en cours; elle prévoit une modification de cet article. Si elle est adoptée plus rapidement que le présent projet par les Chambres fédérales, il faudra reporter l'adaptation qu'elle prévoit dans la présente révision totale.

Art. 20 (actuel art. 19)

Quelques adaptations terminologiques ont été apportées à la disposition.

Art. 21 (actuel art. 20) Exécution

L'al. 3 actuel prévoit la possibilité pour le Conseil fédéral de charger une unité administrative de délivrer des certificats qualifiés couvrant aussi les rapports juridiques de droit privé; on pensait notamment à l'hypothèse dans laquelle aucun fournisseur privé ne se mettrait sur les rangs. Or, au cours de la consultation, plusieurs cantons ont signalé qu'il existe des services cantonaux expérimentés dans l'établissement de certificats et aptes à remplir cette tâche. Le projet mentionne donc les unités administratives fédérales et cantonales.

Art. 22 (actuel art. 21) Abrogation et modification d'autres actes

La formulation de cette disposition a été adaptée aux nouvelles règles de technique législative.

2.2 Abrogation et modification d'autres actes

2.2.1 Abrogation de la SCSE du 19 décembre 2003

La loi du 19 décembre 2003 sur la signature électronique est remplacée par la nouvelle loi.

2.2.2 Loi fédérale du 20 décembre 1968 sur la procédure administrative (PA)

Art. 21a 2. En cas de transmission électronique

Titre marginal: à des fins d'harmonisation, le terme de «transmission électronique» a été utilisé uniformément dans les dispositions modifiées des lois de procédure pour désigner l'envoi d'un document par un particulier à l'autorité (il remplace ici

«communication électronique»). On a choisi ce terme pour ne pas créer de confusions avec certaines acceptions précises de «communication» ou de «notification».

Lorsque l'art. 21*a* PA avait été édicté, on était parti du principe que chaque tribunal ou autorité développerait et mettrait en œuvre son propre système de transmission, qui établirait des accusés de réception. En pratique, il s'est développé des plateformes reconnues de transmission qui créent les accusés de réception et qui redirigent les écrits vers les autorités. L'autorité reçoit donc les documents depuis la plateforme sans que son système n'envoie d'attestation de réception. Ce transfert indirect crée une incertitude juridique quant aux délais et doit être corrigé.

Le nouvel art. 21*a* comporte trois éléments de la transmission électronique d'un écrit à l'autorité, qui se retrouveront dans toutes les lois de procédure:

- l'écrit lui-même doit être muni de la signature électronique qualifiée de la partie ou de son mandataire;
- le moment déterminant pour l'observation du délai est défini de manière techniquement neutre;
- le Conseil fédéral règle le format des écrits et des pièces qui leur sont jointes ainsi que les modalités techniques de la transmission électronique. Il pourra aussi fixer en détail, sur le plan technique, quand les écrits sont réputés remis à l'autorité;
- il règle les conditions auxquelles l'autorité peut exiger, en cas de problème technique, que des documents lui soient adressés ultérieurement sur papier.

De cette manière, le Conseil fédéral pourra tenir compte des exigences concrètes en matière de sécurité et d'automatisation des transmissions et adapter rapidement les dispositions à l'évolution de la technique.

Art. 34, al. 1bis

Cette disposition est le modèle des règles applicables à la notification électronique dans les lois de procédure. Elle contient les éléments suivants:

- la notification électronique requiert l'assentiment de la partie;
- la décision est munie d'une signature électronique, mais c'est au Conseil fédéral qu'il revient de fixer dans une ordonnance quel type de signature sera utilisé;
- comme pour la transmission d'écrits, le Conseil fédéral règle le format de la décision et des pièces jointes, les modalités de la transmission électronique et le moment auquel la décision est réputée notifiée.

2.2.3 Loi du 17 juin 2005 sur le Tribunal fédéral

Art. 39, al. 2

La terminologie est harmonisée dans la version allemande.

De même que le Conseil fédéral a édicté les dispositions d'exécution des normes relatives à la transmission électronique dans l'ordonnance du 18 juin 2010 sur la communication électronique dans le cadre de procédures administratives

(RS *172.021.2*) et 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*), le Tribunal fédéral a édicté le règlement du 5 décembre 2006 sur la communication électronique avec les parties et les autorités précédentes (RCETF; RS *173.110.29*). Ces trois actes devront être adaptés à la nouvelle terminologie (voir ch. 2.2.8) et seront fondés sur les mêmes principes.

La seule exception se trouve à l'art. 3, al. 2, RCETF, qui prévoit que l'inscription sur une plate-forme de distribution vaut acceptation de recevoir les notifications par voie électronique. Cette règle, qui donne aujourd'hui satisfaction, pourra être conservée. L'exigence d'une déclaration de consentement serait un obstacle administratif inutile, propre, aux yeux du Tribunal fédéral, à empêcher que les échanges électroniques se généralisent.

On examinera si cette disposition doit être reprise dans les autres ordonnances dans le cadre du projet d'uniformisation des dispositions sur la notification (voir ch. 1.2.5).

Art. 42, al. 4, 48, al. 2, et 60, al. 3

Les nouvelles dispositions sont similaires à celles de la PA, *mutatis mutandis*. Les termes spécifiques à la LTF ont été conservés pour préserver la cohérence interne de la loi. Les compétences déléguées ailleurs au Conseil fédéral appartiendront ici au Tribunal fédéral.

2.2.4 Code des obligations

Art. 14, al. 2bis

Le fait de préciser dans les définitions de la SCSE que le certificat utilisé pour la signature électronique qualifiée doit être délivré par un fournisseur reconnu permet de simplifier considérablement cette disposition (voir art. 2, let. d, f et g, et ch. 1.2.1).

Comme nous l'avons mentionné au ch. 1.2.3, on a de plus en plus tendance à considérer comme sûres uniquement les signatures électroniques accompagnées d'un horodatage fourni par un service indépendant. Nous avons examiné la possibilité de soumettre la signature électronique qualifiée au sens de la SCSE à cette exigence, mais cette solution est trop restrictive.

Etant donné qu'en Suisse – contrairement à ce qui se passe dans plusieurs pays voisins – la reconnaissance juridique de la signature électronique est réglée non pas dans la SCSE mais dans la législation propre à chaque domaine, on peut tout à fait exiger, dans un domaine déterminé, que la signature électronique soit horodatée pour être reconnue. Ce sera précisément le cas en vertu du nouvel art. 14, al. 2bis, CO, qui exige un horodatage qualifié pour qu'une signature électronique qualifiée soit assimilée à la signature manuscrite.

Art. 59a F. Responsabilité en matière de clef cryptographique

La responsabilité du titulaire de la clef sera étendue aux certificats règlementés, car elle contribue de manière essentielle à ce que les destinataires d'un document aient

confiance dans la signature ou le cachet électronique et lui accordent de la valeur (voir le ch. 1.3.2). Toutefois, la disposition sera limitée à la signature et au cachet et ne vaudra pas pour l'authentification ou les autres applications des certificats.

Comme dans la SCSE, le terme «clef de signature» utilisé dans le titre et les al. 1 et 2 de l'article actuel a été remplacé par «clef cryptographique», car il ne sera plus défini nulle part. Le projet précise par conséquent que la disposition ne s'applique que dans le cas des signatures et cachets électroniques.

2.2.5 Code de procédure civile

Art. 130, 139 et 143, al. 2

Les dispositions de la PA sont reprises ici *mutatis mutandis*.

2.2.6 Loi fédérale du 11 avril 1889 sur la poursuite pour dettes et la faillite

Art. 33a et 34, al. 2

Les dispositions de la PA sont reprises ici *mutatis mutandis* et le terme «transmission électronique» intégré dans le titre marginal. L'art. 33*a*, al. 2, 2e phrase, précise en outre que le Conseil fédéral peut déroger à l'obligation de munir les actes d'une signature électronique qualifiée dans le cas des échanges en masse.

2.2.7 Code de procédure pénale

Art. 86, 91, al. 3, et 110, al. 2

Les dispositions de la PA sont reprises ici *mutatis mutandis*.

2.2.8 Adaptations terminologiques au niveau règlementaire

Suite à la révision, il faudra reporter dans un certain nombre d'ordonnances les nouveaux termes et les expressions simplifiées qui ont été créées. La notion de «signature électronique» ou la loi sur la signature électronique sont citées 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, et 27*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. 12*a*, al. 3 et 4, art. 12*c*, al. 1, let. b, art. 18, al. 4, art. 20, al. 2, et art. 21, 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, al. 2, phrase introductive et 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. 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 et annexe de l'ordonnance de l'OFCOM du 6 décembre 2004 sur les services de certification dans le domaine de la signature électronique (RS *943.032.1*).

Les adaptations devront être faites entre la date de l'adoption de la nouvelle loi par le Parlement et la date de son entrée en vigueur.

3 Conséquences

3.1 Pour la Confédération

3.1.1 Conséquences financières

Aucune.

3.1.2 Conséquences en termes de personnel

La charge, en matière de personnel, induite par les travaux d'élaboration des dispositions d'ordonnance, des directives techniques et administratives et des formulaires pour les procédures civiles représentera plusieurs mois-personnes. L'office chef de file sera l'OFCOM, mais de nombreux autres offices seront concernés.

Le projet n'entraînera, selon toutes prévisions, aucune économie ni aucune augmentation de personnel.

3.1.3 Autres conséquences

Les nouveaux produits seront utiles à divers services de la Confédération. En particulier, les certificats destinés aux autorités offriront une bonne solution aux services qui gèrent des registres, pour la signature des extraits électroniques tels que les actes de naissance ou encore les extraits du casier judiciaire ou du registre du commerce.

3.2 Conséquences pour les cantons et les communes, ainsi que pour les villes, les agglomérations et les régions de montagne

Ni la SCSE actuelle, ni le projet ne représentent de charges pour les cantons, les communes et les autres corporations de droit public.

Ces derniers, ainsi que les organisations, pourront bénéficier des nouveaux produits en tant que clients.

3.3 Conséquences pour les tribunaux et les autres autorités de l'harmonisation de la transmission électronique dans les lois de procédure

L'harmonisation concernant surtout les formulations, qui seront plus précises et plus uniformes, les autorités ne seront guère touchées par la révision. Seules celles qui continuent de demander une livraison ultérieure sur papier, pratique contraire à l'esprit de la règlementation actuelle, devront à l'avenir imprimer elles-mêmes ces dossiers. Elles n'auront plus à supporter cette dépense supplémentaire dès qu'elles seront passées à la gestion électronique interne des dossiers.

3.4 Conséquences pour l'économie

Les applications des certificats numériques sont de nature à favoriser la sécurité et la fiabilité des échanges électroniques entre les autorités et les particuliers. Elles contribuent à l'avènement de la société de l'information.

3.5 Conséquences pour la société

La loi permettra à l'Etat de régler les instruments de l'identification électronique forte, ce qui contribuera à la prévention des conséquences négatives de la société de l'information globalisée telles que le vol d'identité.

3.6 Conséquences environnementales

Aucune.

3.7 Autres conséquences

Aucune.

4 Relation avec le programme de la législature et avec les stratégies nationales du Conseil fédéral

4.1 Relation avec le programme de la législature

Le présent objet est annoncé dans le message du 25 janvier 2012 sur le programme de la législature 2011 à 2015[3].

4.2 Relation avec les stratégies nationales

Pendant longtemps, la règlementation de la signature électronique a été un élément important de la stratégie du Conseil fédéral pour une société de l'information en Suisse et de la stratégie suisse de cyberadministration. Tel n'est plus le cas. Depuis l'adoption de la SCSE, le problème est considéré comme résolu. En soi, le cachet règlementé destiné aux personnes morales et aux autorités n'est qu'une adaptation mineure d'une législation existante.

La présente révision donne cependant au Conseil fédéral la compétence de régler d'autres applications des certificats numériques, dont, en particulier, l'authentification forte. Or la mise en place d'un instrument d'identification électronique forte est contenue dans plusieurs stratégies de la Confédération, directement ou indirectement, en tant qu'étape de la réalisation d'autres objectifs:

– la stratégie du Conseil fédéral pour une société de l'information en Suisse de mars 2012 mentionne l'élaboration de solutions permettant de prouver les identités parmi les axes prioritaires de la Confédération pour lutter contre la cybercriminalité;

3 FF **2012** 349 475

- la stratégie suisse de cyberadministration précise, pour le projet prioritaire B2.07, que «la mise à disposition d'identités et d'identifications digitales pour l'authentification lors de transactions électroniques administratives et privées est la pierre angulaire de l'évolution de l'espace économique suisse»;
- la stratégie Cybersanté Suisse, élaborée conjointement par la Confédération et les cantons, cite, comme objectif A5 du champ d'activité «Dossier électronique du patient», l'établissement d'une authentification sécurisée avec une option pour la signature électronique légale;
- le Conseil fédéral a décidé de soumettre la présente révision totale au Parlement le 19 décembre 2012, dans le cadre d'un train de mesures législatives visant à encourager les échanges électroniques.

5 Aspects juridiques

5.1 Constitutionnalité et légalité

La loi se fonde sur les art. 95, al. 1, et 122, al. 1, de la Constitution, qui donnent à la Confédération la compétence de légiférer sur l'exercice des activités économiques lucratives privées et en matière de droit civil.

5.2 Compatibilité avec les obligations internationales

La Suisse n'a pas d'obligations internationales dans le domaine visé. Bien qu'elle ne soit pas membre de l'UE, ses rapports étroits avec de nombreux Etats communautaires justifient pleinement qu'elle recherche la conformité et la compatibilité avec les règles européennes en la matière.

5.3 Forme de l'acte à adopter

Selon l'art. 164 de la Constitution, toutes les dispositions importantes qui fixent des règles de droit doivent être édictées sous la forme d'une loi fédérale.

5.4 Frein aux dépenses

Le présent projet n'entraîne pas de dépenses qui justifieraient le recours au frein aux dépenses.

5.5 Conformité à la loi sur les subventions

Les principes de la loi sur les subventions ne sont pas applicables ici.

5.6 Délégation de compétences législatives

Tant la loi actuelle que la nouvelle loi comprennent essentiellement des délégations de compétence législative au Conseil fédéral. La compétence de ce dernier d'édicter des dispositions d'exécution sera étendue à de nouveaux produits, notamment à une nouvelle catégorie de certificats numériques.

Les produits soumis à la règlementation fédérale ne sont pas les seuls autorisés. Tout fournisseur peut offrir des produits non règlementés de toutes catégories. Mais la reconnaissance de fournisseurs remplissant un certain cahier des charges et les critères de qualité fixés par l'Etat pour certains produits sont un gage de fiabilité qui répond aux attentes des milieux économiques et qu'il serait difficile d'obtenir autrement dans le domaine des échanges électroniques de données.

5.7 Conformité à la législation sur la protection des données

Les certificats numériques, les signatures électroniques et l'authentification électroniques sont directement associés avec des données personnelles; ils doivent donc faire l'objet d'une attention particulière du point de vue de la protection des données.

En réponse à cette exigence, tout d'abord, ces produits sont fondés sur une base légale formelle. Ensuite, les moyens choisis pour assurer la sécurité et la fiabilité des échanges électroniques sont les plus favorables à une bonne protection des données; il n'existe notamment pas d'obligation d'utiliser des moyens d'identification et d'authentification lorsqu'ils ne sont pas absolument nécessaires.

L'art. 15 de la loi, consacré à la protection des données, n'est pas modifié matériellement.