

Ordonnance sur l'infrastructure à clé publique suisse

Projet du 03.06.1999

Rapport explicatif

1 Pourquoi légiférer?

Le commerce électronique est promis à un bel avenir. Un des principaux obstacles qui risquent cependant de compromettre son développement à grande échelle a trait à la confiance des utilisateurs et à la sécurité des services offerts dans ce domaine. A côté des besoins de confidentialité, existe la nécessité de s'assurer de l'identité de son interlocuteur ainsi que de l'intégrité du message reçu. La cryptographie à clé publique permet de répondre à ces besoins. Il convient toutefois, dans l'intérêt tant des utilisateurs que des fournisseurs de services de certification qui légitiment les clés publiques, de fixer un cadre légal donnant l'assurance que certaines exigences essentielles sont remplies.

Dans sa stratégie pour une société de l'information en Suisse du 18 février 1998, le Conseil fédéral a chargé le Département fédéral de justice et police (DFJP), le Département fédéral des finances (DFF) et le Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC) de l'introduction de la signature numérique en concevant un système de clé publique (Public Key Infrastructure) et en élaborant les règles nécessaires. Dans ce sens, un questionnaire général a été soumis aux milieux intéressés au printemps 1998 afin de déterminer la direction que devaient prendre les travaux. Après analyse des réponses et sur la base des travaux internes déjà entrepris en vue de la mise en place d'une infrastructure de certification pour l'administration fédérale (groupe de travail BV-TTP), un modèle d'infrastructure à clé publique a été élaboré et présenté le 24 novembre 1998, lors d'une conférence publique, en même temps qu'un avis de l'Office fédéral de la justice sur la valeur juridique de la signature numérique. Les quelque 80 personnes qui participaient à cette conférence ont pour l'essentiel appuyé les travaux en cours. La mise sur pied d'une infrastructure à clé publique a été considérée comme urgente, tandis que la question de la valeur juridique de la signature numérique devrait, selon les avis exprimés, être examinée sans tarder en identifiant les domaines prioritaires.

Sur le plan international, plusieurs organismes se préoccupent de l'harmonisation des règles en matière de commerce électronique, notamment en ce qui concerne les procédés d'authentification. On peut citer ici la Commission des Nations Unies pour le droit commercial international (CNUDCI/UNCITRAL), qui a adopté une loi type sur le commerce électronique en 1996 et qui est en train d'élaborer des règles uniformes sur les signatures électroniques. Sous l'égide de l'Organisation de coopération et de développement économiques (OCDE), s'est tenue à Ottawa en octobre 1998 la Conférence ministérielle «Un monde sans frontières: concrétiser le potentiel du commerce électronique mondial». Un des résultats de cette conférence s'est traduit par l'adoption d'une Déclaration sur l'authentification pour le commerce électronique. Quant à l'Union européenne, un projet de directive sur un cadre commun pour les signatures électroniques vient d'être adopté par le Conseil et est maintenant soumis au Parlement européen en deuxième lecture. En outre, la Commission européenne a publié une proposition de directive du Parlement européen et du Conseil relative à certains aspects juridiques du commerce électronique dans le Marché intérieur. Ces efforts d'harmonisation au niveau international marquent l'importance du sujet et la nécessité d'élaborer en Suisse une réglementation compatible.

A cet égard, la valeur juridique de la signature numérique et son équivalence avec la signature manuscrite constituent un élément important. Selon l'avis précité de l'Office fédéral de la justice, on ne saurait en Suisse, *de lege lata*, dénier toute valeur juridique à la signature numérique, même si son équivalence avec la signature manuscrite n'est pas consacrée par la loi. La plupart des affaires conclues par voie électronique ne nécessitant pas la forme écrite au sens des articles 12 et suivants du Code des obligations, en principe rien n'empêche d'utiliser dès aujourd'hui les nouvelles technologies de l'information et de la communication pour passer des contrats ou effectuer des commandes.

Il s'agit, le plus rapidement possible, d'élaborer une infrastructure de clé publique qui soit sûre et reconnue par l'État afin de promouvoir le commerce électronique en Suisse, pour trois raisons: l'évolution dynamique des nouvelles technologies de l'information et de la communication, le fait qu'une réglementation concernant l'identification sûre des parties et l'intégrité des données échangées est considérée comme urgente, et les efforts d'harmonisation à l'échelle internationale. Nous sommes parfaitement conscients que la base légale formelle à cet effet est encore relativement faible, mais outre la loi sur les télécommunications et celle sur les obstacles techniques au commerce, on peut relever en particulier que la création de réglementations au niveau de l'ordonnance, d'une durée limitée et servant à créer des bases de décision solides, constitue une pratique éprouvée depuis plusieurs années (quelque vingt réglementations à titre d'essai en 1995 déjà).

Le présent projet d'ordonnance est prévu pour une durée limitée dans le sens où les principes qu'elle contient sont destinés à être intégrés dans une loi cadre qui comprendra notamment les aspects des actes juridiques de droit privé concernant l'égalité de la signature numérique et de la signature manuscrite (droit des contrats, droit des registres et droit en matière d'exécution forcée). Elle fournira des bases solides dans la mesure où les expériences faites avec l'infrastructure de clé publique pourront servir à élaborer une réglementation globale en connaissance de cause. En outre, le fait d'élaborer une infrastructure de clé publique qui soit sûre exercera sans aucun doute, dès à présent dans le cadre de la législation existante, une influence positive sur la reconnaissance juridique de la signature numérique.

2 Caractéristiques du projet

Le présent projet d'ordonnance ne traite donc que de la mise sur pied d'une infrastructure à clé publique pour la Suisse. Une infrastructure à clé publique peut se concevoir de manière plus ou moins élaborée. Une reconnaissance de la part de l'Etat n'est ainsi nullement nécessaire, mais elle augmentera considérablement la confiance du grand public dans l'utilisation des possibilités liées au commerce électronique. On ne saurait cependant aller jusqu'à rendre la reconnaissance obligatoire et soumettre systématiquement la fourniture de services de certification à autorisation préalable. Le projet prévoit donc que les fournisseurs de services de certification qui le désirent seront reconnus s'ils remplissent certaines exigences essentielles. Ils seront alors considérés comme sûrs et pourront se prévaloir de cette reconnaissance pour offrir leurs services aux personnes et entreprises intéressées. De même, les tiers qui se fieront aux certificats électroniques émis par un fournisseur de services de certification reconnu auront une garantie supplémentaire du sérieux avec lequel ces certificats auront été établis.

L'examen de la conformité aux exigences essentielles nécessite des ressources et des connaissances qui en font l'affaire de spécialistes. C'est pourquoi le modèle proposé fait appel au système éprouvé de l'accréditation (voir plus loin sous ch. 3.2), déjà utilisé dans le domaine de la sécurité informatique pour l'accréditation de laboratoires d'essais en relation avec les critères ITSEC. La tâche de juger de la conformité aux exigences essentielles et de reconnaître les fournisseurs de services de certification est confiée à des organismes de certification accrédités. Le secteur privé aura ainsi un rôle primordial à jouer dans le système d'infrastructure à clé publique envisagé.

Quant à l'OFCOM, son rôle se limitera en principe à enregistrer les fournisseurs de services de certification reconnus et à en publier la liste. Il est toutefois également proposé, comme solution alternative, de lui attribuer la fonction d'autorité de certification primaire («root») en le chargeant de certifier, au moyen de sa propre signature numérique, la clé publique des fournisseurs de services de certification reconnus. Ces derniers seraient ainsi rattachés à une chaîne de certification électronique organisée hiérarchiquement qui rendrait inutiles les certifications croisées. Cette structure verticale limiterait certes la liberté des fournisseurs de services de certification reconnus. Dans la mesure où ces derniers appartiendraient à un système clairement délimité, elle serait toutefois garante d'un haut niveau de sécurité et de transparence. Bien que les textes internationaux, en particulier le projet de directive européenne sur la signature électronique, n'imposent pas cette organisation hiérarchique, c'est le parti pris par la loi allemande du 22 juillet 1997.

Les milieux consultés sont tout particulièrement invités à se prononcer sur la pertinence de prévoir ou non un root obligatoire et à indiquer leur préférence. Les dispositions du projet d'ordonnance qui se réfèrent à un système de «root» obligatoire sont indiquées *en italique* et sont regroupées dans la **section 4** du projet d'ordonnance (pour les commentaires, voir plus loin sous ch. 3.4).

Au cas où un root obligatoire serait instauré, on pourrait en outre imaginer que l'OFCOM soit chargé d'autres tâches que celles mentionnées à l'article 16 du projet d'ordonnance, telles que garantir l'accès aux annuaires et aux listes de révocation des fournisseurs de services de certification reconnus, archiver tous les certificats électroniques échus ou révoqués ou encore archiver tous les journaux des activités. **Les milieux intéressés sont tout particulièrement invités à donner leur opinion à ce sujet également et à indiquer, le cas échéant, quels types de services ils aimeraient voir confier à l'OFCOM de manière centralisée.**

3 Commentaire des dispositions proposées

3.1 Dispositions générales

Selon l'**article premier, alinéa 1**, l'ordonnance doit contribuer à donner rapidement à un large cercle d'utilisateurs un instrument fiable pour participer au développement croissant du commerce électronique. Elle devrait également contribuer à plus de sécurité juridique en ce qui concerne l'utilisation de la signature numérique en Suisse et assurer la reconnaissance des fournisseurs de services de certification au-delà des frontières.

La reconnaissance des fournisseurs de services de certification est facultative (**article premier, alinéa 2**). Ceux-ci ne sont soumis aux dispositions de l'ordonnance que s'ils le désirent. Ils sont donc en principe libres de fournir des services de certification selon leurs propres critères. Ils peuvent également se faire «reconnaître» par un organisme de certification accrédité selon d'autres critères que ceux résultant de l'ordonnance. Ce n'est que lorsqu'ils entendent se faire reconnaître au sens de l'ordonnance qu'ils entrent dans son champ d'application. L'ordonnance tend ainsi à conférer un label de qualité aux fournisseurs de services de certification qui le désirent.

Le champ d'application de l'ordonnance vise aussi bien les services de confidentialité que les services liés à la signature numérique en tant que procédés cryptographiques à clé publique. Certaines dispositions ne concernent cependant plus spécifiquement que la signature numérique ou les fournisseurs de services de certification reconnus offrant des services liés à la signature numérique (cf. articles 8, 11, 13, 16 à 18 et 22).

Bien que les travaux internationaux cités plus haut insistent sur le principe de la neutralité technologique, l'ordonnance ne traite que de la signature numérique comme catégorie particulière de signature électronique (**article 2, lettre a**). La signature numérique est aujourd'hui toutefois la technique d'authentification la plus évoluée et la plus utilisée.

L'ordonnance n'interdit bien évidemment pas le recours à d'autres méthodes et pourrait même les intégrer ultérieurement si le besoin s'en faisait sentir.

3.2 Reconnaissance des fournisseurs de services de certification

La reconnaissance des fournisseurs de services de certification est le fait d'un organisme de certification accrédité au sens du système suisse d'accréditation découlant de la loi fédérale sur les entraves techniques au commerce (LETC; RS 946.51) et de l'ordonnance sur l'accréditation et la désignation (OAccD; **article 3, alinéa 1**).

L'accréditation consiste à reconnaître formellement la compétence d'un organisme de procéder à des essais ou à des évaluations de la conformité conformément aux critères internationaux pertinents (art. 2 OAccD). La reconnaissance internationale des organismes accrédités et de leurs rapports ou autres attestations de conformité s'en trouve ainsi améliorée. Les organismes accrédités testent ou évaluent des produits ou exercent des activités analogues à l'égard de personnes, de services ou en matière de procédures (cf. art. 1^{er}, al. 1, let. a OAccD). Ils se répartissent en quatre catégories principales: les laboratoires d'essais, les laboratoires d'étalonnage, les organismes de certification et les organismes d'inspection. L'accréditation de ces organismes est délivrée par le directeur de l'Office fédéral de métrologie (OFMET) après évaluation par le Service d'accréditation suisse (SAS) et avis de la Commission d'accréditation (art. 14, al. 1 OAccD). Un réseau de contrat entre les systèmes nationaux d'accréditation assure la reconnaissance mutuelle des organismes accrédités ainsi que de leurs prestations telles que les certificats qu'ils émettent.

En l'occurrence, la reconnaissance des fournisseurs de services de certification fait appel à des organismes de certification, ce qui ne manque pas de prêter à confusion du point de vue de la terminologie. Il convient cependant de bien distinguer entre les fournisseurs de services de certification (*certification authorities, CA*), qui certifient électroniquement des clés cryptographiques, et les organismes de certification accrédités (*certification bodies, CB*), qui certifient¹, dans un document écrit, que certains produits, services ou procédures sont conformes à certaines normes. Pour se faire accréditer dans le but de reconnaître les fournisseurs de services de certification, les organismes de certification devront remplir les critères de la norme européenne EN 45011. En l'absence de normes internationales applicables, ils évalueront les fournisseurs de services de certification sur la base des exigences essentielles fixées dans la section 3 de l'ordonnance (**article 3, alinéa 2**) et dans ses dispositions d'exécution (cf. **article 15**).

Le système proposé est schématisé, dans ses deux variantes, dans le graphique figurant en annexe.

L'OFCOM, est chargé d'enregistrer les fournisseurs de services de certification reconnus et d'en tenir une liste publique (**article 4**).

3.3 Exigences essentielles pour la reconnaissance des fournisseurs de services de certification

Enoncées en termes généraux (cf. en particulier l'**article 5**), les exigences essentielles auxquelles devront satisfaire les fournisseurs de services de certification désireux de se faire reconnaître seront précisées dans des prescriptions édictées par l'OFCOM d'entente avec l'Office fédéral de l'informatique et le SAS (**article 15**).

L'essence même de l'activité des fournisseurs de services de certification consiste à émettre des certificats électroniques attestant qu'une clé publique est bien liée à une personne déterminée. L'**article 6, alinéa 1**, précise que cette dernière peut aussi bien être une personne morale qu'une personne physique. Dans le monde réel, une personne morale agit

¹ Afin de réduire les risques de confusion, l'ordonnance parle de *reconnaissance* et non de *certification* des fournisseurs de services de certification.

par ses organes, soit en définitive par l'intermédiaire de personnes physiques. Dans le monde virtuel, rien n'empêche qu'elle puisse posséder une paire de clés cryptographiques propre, différente de celles des personnes physiques qui agissent habituellement en son nom. L'utilisation correcte de la clé privée est une affaire à régler de manière interne par la personne morale, qui doit supporter, vis-à-vis des tiers, les conséquences d'éventuels abus. Cela n'exclut cependant pas que des certificats électroniques puissent être émis en faveur de personnes (physiques) en leur qualité de représentantes d'autres personnes (physiques ou morales). Le pouvoir de représentation devra dans ce cas clairement résulter du certificat. Lorsqu'une personne agit au nom d'une autre et dispose pour cela d'un certificat électronique, on peut se demander si les règles générales de la représentation (art. 32ss du Code des obligations) suffisent pour garantir les intérêts des tiers de manière transparente. C'est pourquoi l'**article 6, alinéa 3** impose soit la comparution personnelle du représenté et du représentant, soit l'envoi au fournisseur de services de certification d'un message muni de la signature numérique du représenté et confirmant les pouvoirs du représentant.

L'identification des requérants de certificats électroniques est une tâche, comme d'autres d'ailleurs, qui pourrait très bien être déléguée. Le fournisseur de services de certification reconnu resterait toutefois seul responsable de l'accomplissement correct de ses obligations par des tiers. L'obligation qui lui est faite d'enregistrer et de conserver les informations recueillies (par exemple le numéro de la carte d'identité ou une copie de l'extrait du registre du commerce; **article 6, alinéa 4**) devrait lui permettre d'apporter la preuve, le cas échéant, qu'il a satisfait à son obligation d'identification. Afin de garantir l'anonymat des personnes qui le souhaitent, il se justifie de prévoir la possibilité d'émettre des certificats électroniques comportant des pseudonymes (**article 6, alinéa 5**).

Pour plus de transparence, les fournisseurs de services de certification reconnus devront publier leurs conditions générales (*certification practice statement*; **article 7, alinéa 1**). Ils doivent en outre attirer l'attention de leurs clients sur les risques liés à la divulgation ou à la perte de la clé privée et sur les moyens permettant de réduire ou supprimer ces risques (**article 7, alinéa 2**). Il importe en effet que les utilisateurs soient conscients des conséquences que peut avoir l'utilisation abusive de leur clé privée.

Les fournisseurs de services de certification ne génèrent pas forcément eux-mêmes les clés de chiffrement. Pour plus de sécurité, cette activité leur est toutefois clairement interdite lorsqu'ils offrent des services liés à la signature numérique (**article 8**).

A côté de l'émission des certificats électroniques, leur révocation revêt une importance capitale. Elle peut intervenir à la demande de l'utilisateur (**article 9, alinéas 1 et 2**), par exemple en cas de perte de sa clé privée, ou être le fait du fournisseur de services de certification contre le gré de l'utilisateur (**article 9, alinéa 3**). La révocation d'un certificat électronique a un effet *ex nunc*. Autrement dit, elle ne remet pas en cause la validité des affaires passées entre le moment où le certificat a été émis et celui où il a été révoqué. Elle doit donc être décrétée immédiatement.

L'inscription d'un certificat électronique dans un annuaire est laissée à la liberté de son titulaire. Les fournisseurs de services de certification reconnus doivent toutefois mettre un tel service à la disposition de leurs clients (**article 10, alinéa 1**). Ils doivent en outre tenir à jour une liste de tous les certificats révoqués, même ceux qui n'ont pas été publiés dans un annuaire (**article 10, alinéa 2**). L'inscription de ces derniers dans une liste de révocation publique (**article 10, alinéa 3**) ne devrait pas poser de problèmes dans la mesure où seuls certains éléments impersonnels y seront mentionnés, tels que le numéro d'identification du certificat. Les tiers doivent pouvoir avoir accès à l'annuaire des certificats et à la liste des certificats révoqués 24 heures sur 24, sans autres frais que ceux découlant de l'utilisation des moyens de télécommunication publics.

La consultation des certificats électroniques peut s'avérer nécessaire alors même qu'ils sont échus ou révoqués. Il en va ainsi lorsqu'il s'agit d'apporter la preuve de manifestations de volonté échangées sous forme électronique durant la période de validité du certificat. Le délai de conservation de 11 ans prévu à l'**article 11, alinéa 1** correspond au délai de

prescription général de l'article 127 du Code des obligations (CO) et au délai de conservation des livres de l'article 962, alinéa 1 CO (10 ans), compte tenu de la suppression prévue à l'article 962, alinéa 3 CO.

Pour les besoins de la surveillance, il apparaît judicieux d'obliger les fournisseurs de services de certification reconnus de tenir un journal de leurs activités (**article 12**). Celui-ci peut également s'avérer utile en cas de cessation d'activité et de transfert des certificats électroniques à un autre fournisseur de services de certification reconnu. A ce sujet, l'**article 13**, qui ne s'applique qu'aux fournisseurs de services de certification offrant des services liés à la signature numérique, distingue entre la cessation volontaire d'activité d'une part, et la faillite du fournisseur ou la révocation de sa reconnaissance d'autre part. Dans le second cas (**article 13, alinéa 2**), l'OFCOM peut obliger un fournisseur de services de certification reconnu offrant des services liés à la signature numérique de révoquer les certificats électroniques du fournisseur en faillite ou dont la reconnaissance a été retirée et à tenir la liste des certificats révoqués et conserver les certificats échus ou révoqués. Cela n'ira naturellement pas sans occasionner des coûts supplémentaires au fournisseur désigné par l'OFCOM. Il se justifie donc de le dédommager de manière équitable en faisant participer tous les autres fournisseurs de services de certification reconnus offrant des services liés à la signature numérique (**article 13, alinéa 3**).

Les fournisseurs de services de certification reconnus devront assurer la protection des données personnelles de leurs clients (**article 14**). En tant que réglementation générale, la loi fédérale sur la protection des données (LPD) devrait permettre d'empêcher les abus dans ce domaine.

3.4 Certification électronique primaire des fournisseurs de services de certification reconnus

*Conçue comme variante, cette section vise à intégrer les fournisseurs de services de certification reconnus offrant des services liés à la signature numérique dans une hiérarchie de certification électronique. L'OFCOM jouerait alors la fonction de «root» (**article 16, alinéa 1**). Il fournirait ainsi lui-même des services de certification, au bénéfice cependant des seuls fournisseurs de services de certification reconnus offrant des services liés à la signature numérique, à l'exclusion des fournisseurs offrant des services de confidentialité et des utilisateurs. Afin que ces derniers puissent cependant remonter la chaîne de certification électronique pour vérifier de manière sûre les signatures numériques, l'OFCOM devrait notamment tenir un annuaire des certificats électroniques et une liste des certificats révoqués (cf. **article 16, alinéa 2**), conserver les certificats échus et publier sa propre clé publique. Il devrait donc également remplir les exigences essentielles et serait soumis à l'évaluation et à la surveillance d'un organisme de certification accrédité (**article 16, alinéa 4**). Au niveau international, il pourrait certifier, sur une base réciproque, les organes étrangers ayant une fonction de root, comme la RegTP (Autorité de régulation en matière de télécommunications et de la poste) en Allemagne, ou, en l'absence d'une telle autorité, certifier directement les fournisseurs de services de certification reconnus. Une telle possibilité dépendrait dans tous les cas de l'existence d'un accord international conclu par le Conseil fédéral au sens de l'article 21.*

*L'**article 17** interdirait les sous-certifications (certifications de fournisseurs de services de certification par d'autres) ainsi que les certifications croisées (reconnaissance mutuelle de deux fournisseurs de services de certification). Pour la sécurité du système, il importerait en effet que tous les fournisseurs de services de certification reconnus certifiés électroniquement par l'OFCOM tiennent leur légitimité directement de l'OFCOM et qu'ils ne puissent reconnaître eux-mêmes des fournisseurs non reconnus au sens de la présente ordonnance.*

*Pour les activités liées à sa fonction de root, l'OFCOM, soumis aux principes de la nouvelle gestion publique depuis le 1^{er} janvier 1999, percevrait des émoluments destinés à couvrir ses frais (**article 18, alinéa 1**). Le montant des émoluments serait fixé par le Département*

fédéral de l'environnement, des transports, de l'énergie et de la communication (**article 18, alinéa 2**).

Un système avec root permettrait aux utilisateurs de vérifier les signatures numériques en remontant la chaîne de certification jusqu'à l'autorité primaire. Cette transparence pourrait s'avérer être une garantie supplémentaire en cas de reconnaissance légale de la signature numérique en Suisse et à l'étranger. L'interopérabilité entre les fournisseurs de services de certification s'en trouverait également améliorée, de même que la reconnaissance internationale des fournisseurs de services de certification. Du côté des désavantages d'un tel système, il convient de mentionner les frais supplémentaires qui en résulteraient et qui seraient en définitive reportés sur les utilisateurs. Si le besoin s'en faisait sentir, les fournisseurs de services de certification pourraient en outre librement introduire un tel système sans qu'il soit obligatoirement imposé par l'Etat. Enfin, un système avec root comporterait le risque qu'une intrusion illicite au niveau de l'autorité de certification primaire porterait atteinte à l'ensemble de l'infrastructure à clé publique.

Les deux variantes proposées sont schématisées dans le graphique figurant en annexe.

3.5 Surveillance et responsabilité des fournisseurs de services de certification reconnus

Il incombera aux organismes de certification accrédités de veiller à ce que les fournisseurs de services de certification reconnus continuent de respecter les exigences essentielles selon les règles prévues à ce sujet par le système de l'accréditation (**article 19, alinéa 1**). La non-conformité aux exigences essentielles ou la violation de ses obligations par le fournisseur de services de certification peut entraîner le retrait de la reconnaissance (cf. **article 19, alinéa 2**).

Une ordonnance du Conseil fédéral ne peut sans doute pas régler de manière exhaustive les diverses questions qui se posent en matière de responsabilité civile des fournisseurs de services de certification, tant envers leurs clients qu'envers les tiers qui se fient à leurs certificats. C'est pourquoi l'**article 20, alinéa 1**, renvoie aux règles générales du Code des obligations, tout en précisant que la responsabilité des fournisseurs de services de certification porte en particulier sur l'identification correcte des titulaires des paires de clés. Il importe dans tous les cas de garantir la transparence lorsque les fournisseurs de services de certification reconnus limitent leur responsabilité, soit à un montant déterminé, soit à certaines utilisations qui peuvent être faites du certificat électronique. Aussi ces limitations doivent-elles être indiquées dans les certificats électroniques concernés (**article 20, alinéa 2**). Par ailleurs, les exigences essentielles imposent aux fournisseurs de services de certification reconnus de contracter une assurance couvrant leur responsabilité (cf. **article 5, lettre c**). Il va de soi que les limitations de responsabilité ne peuvent toucher les obligations, de droit public, découlant de l'ordonnance même (**article 20, alinéa 3**).

3.6 Fournisseurs de services de certification étrangers

Sur la base de l'article 14 de la loi fédérale sur les entraves techniques au commerce (LETC), le Conseil fédéral peut conclure des accords internationaux dans le but de reconnaître des fournisseurs de services de certification étrangers et leurs prestations. La liste de ces accords et des fournisseurs de services de certification concernés devra être tenue et mise à disposition des intéressés par l'OFCOM (**article 21**).

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

En vertu du principe de la libre appréciation des preuves par le juge, un document électronique comportant une signature numérique est susceptible d'être admis comme preuve en justice. Pour administrer une telle preuve, l'infrastructure technique et les connaissances nécessaires feront le plus souvent défaut, en tout cas tant que de telles

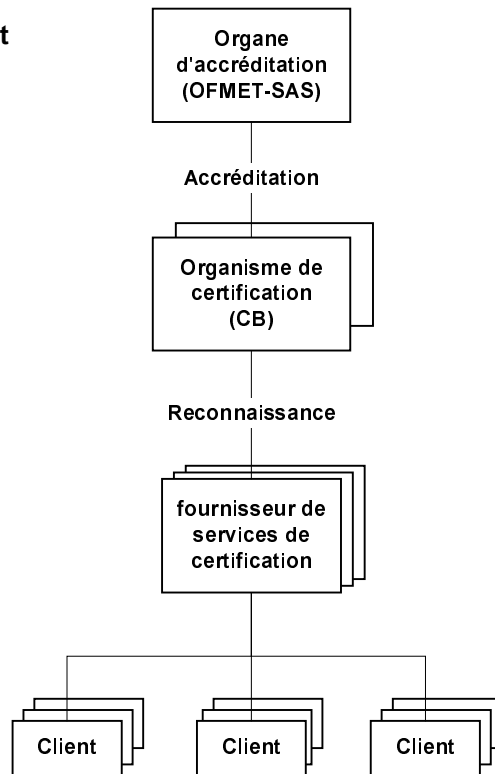
procédures ne se seront pas généralisées. C'est pourquoi il apparaît utile de prévoir un service centralisé fournissant une attestation officielle de la conformité d'une signature numérique apposée sur un document électronique avec les exigences fixées par l'ordonnance (**article 22**). La valeur juridique conférée *de lege lata* à la signature numérique s'en trouverait ainsi accrue. L'attestation pourrait se référer à la validité d'un certificat électronique à un moment donné, mais ne garantirait pas, à défaut d'enregistrement de la date et de l'heure (*time stamping*), que le document électronique lui-même a effectivement été transmis à ce moment-là. Contre paiement d'un émolument couvrant les frais, tout intéressé pourrait recourir à cette prestation. Celle-ci ne toucherait ni aux droits ni aux obligations des requérants, mais concernerait uniquement l'établissement d'un fait. Elle ne constituerait ainsi pas une décision au sens de l'article 5 de la loi fédérale sur la procédure administrative (RS 172.021).

3.8 Dispositions finales

L'OFCOM sera chargé de l'exécution de l'ordonnance (**article 23**). Il devra en particulier édicter les prescriptions de détail nécessaires. L'entrée en vigueur de l'ordonnance et de ses dispositions d'exécution est prévue pour le 1^{er} janvier 2000 (**article 24**).

Annexe : graphique

ICP sans root



ICP avec root

