Stellungnahme zum Entwurf
Bundesgesetz über elektronische Signatur (BGES)
Loi fédérale sur la signature électronique (LFSél)

I. Remarques préliminaires

Les commentaires qui suivent ont été rédigés dans l'optique de la sécurité du droit pour l'utilisateur non-averti. Il s'agit **d'éviter dans la mesure du possible de créer de nouveaux risques juridiques pour les justiciables**, risques qui ne seraient pas compensés par des avantages évidents. A l'heure actuelle, chacun est conscient de la fragilité juridique des actes passés par voie électronique. La législation proposée risque de modifier cette impression en la remplaçant par **une fausse impression de sécurité**, par exemple parce que la distinction entre une signature valable et une signature dépourvue de protection juridique n'est pas suffisamment claire.

Vu le manque de temps, nous renonçons à une analyse article par article au profit de quelques remarques sur les points suivants :

1) Calendrier
2) Terminologie
3) Absence de neutralité technologique
4) Domaine couvert (droit privé/droit public)
5) Sécurité juridique (validité juridique)
6) Responsabilité (blanc-seing / représentation sans pouvoir)
7) For

Par ailleurs les commentaires formulés à l'occasion de la procédure de consultation relative à l'ordonnance sur les services de certification restent valables, soit notamment la nécessité d'assurer par la loi le respect de règles que le marché ne produit pas spontanément à savoir, en particulier, **garantir la sécurité du droit à long terme, protéger les parties les plus faibles et assurer l'équilibre confédéral tout en protégeant les intérêts de la Suisse dans le cadre international.**

II. Commentaires

1) Calendrier

A l'occasion de la procédure de consultation sur l'OSCert, nous avions souligné que „**eine umfassende Regelung der digitalen Signatur auf Gesetzesebene, einschliesslich der Frage der Rechtsverbindlichkeit von digitalen Signaturen ... ist sinnvoll. Die entsprechenden Arbeiten sollten raschmöglichst vorangetrieben werden**." Cette remarque reste valable. Il convient cependant de tenir compte des développements qui sont intervenus dans l'intervalle.

Die Zertifizierungsdienste-Verordnung vom 12. April 2000 ist am 1. Mai 2000 in Kraft getreten, doch liegen die technischen Vorschriften erst seit dem 9. Januar 2001 (im Entwurfstadium) vor. Das bedeutet, dass

praktische Erfahrungen mit den neuen Normen noch nicht haben gesammelt werden können und Zertifizierungsdienste-Anbieter noch nicht gemäss den Bestimmungen der Verordnung auf dem Markt tätig sind. Eine Beurteilung der technisch ausgerichteten Vorschriften des neuen Entwurfs erweist sich deshalb im jetzigen Zeitpunkt als praktisch ausgeschlossen. Aus diesem Grunde stellt sich die Frage, ob es sachgerecht ist, so kurzfristig die Verordnung durch ein Gesetz zu ersetzen, selbst wenn nicht übersehen werden kann, dass die Anerkennung der elektronischen Signatur einem grossen praktischen Bedürfnis entspricht. En tout cas, les développements, ou l'absence de développements, sur la base de l'OScert devront être pris en compte avant l'adoption définitive de la loi.

In diesem Zusammenhang lässt sich auch die Trennung der Gesetzesvorlagen in ein Bundesgesetz über die elektronische Signatur und ein Bundesgesetz über den elektronischen Geschäftsverkehr hinterfragen. Ein Zusammenhang zwischen den beiden Entwürfen ist offensichtlich gegeben, insbesondere bei den „Konsumenten-schutznormen" im Rahmen der elektronischen Signatur. Überschneidungen können sich auch im Bereich der Haftung ergeben. Diese Trennung könnte die Einheitlichkeit der beiden Gesetzesvorlagen gefährden.

2) Terminologie

Die Unterscheidung zwischen elektronischer und digitaler Signatur (Art. 3 lit.a und b) überzeugt nicht vollumfänglich. „Digital" (en français: „numérique") ist der Gegensatz zu „analog" und bezeichnet die Art und Weise, wie moderne Computersysteme rechnen; „elektronisch" ist ein mit Elektrizität arbeitendes Gerät. Abgesehen davon, dass die Signatur selber nicht elektronisch sein kann, ist es auch möglich, eine digitale Signatur auf Papier auszudrucken und hernach zur Überprüfung wieder in einen Computer einzulesen. Das sprachlich exakte Gegenstück zum „Prüfschlüssel" ist nicht der „Signaturschlüssel", sondern der „Signierschlüssel".

Ce problème de terminologie recouvre en fait la difficulté qui résulte de la volonté d'élaborer une loi sur la reconnaissance des signatures électroniques qui soit neutre du point de vue de la technologie utilisée, mais qui en fait repose quand même exclusivement sur l'utilisation de certificats électroniques.

Face à la nécessité d'assurer une certaine stabilité au niveau de la loi mais face également à la rapidité de l'évolution technologique et à la nécessité d'une coordination internationale on est amené à prévoir des **délégations de compétence très (dans certains cas trop) larges.** Cette façon de faire implique au moins que les dispositions d'exécution soient connues au moment où la loi est débattue.

3) Absence de neutralité technologique

Le principe de la neutralité technologique répond au souci du législateur de codifier des schémas juridiques susceptibles de survivre à l'évolution fulgurante des techniques. Son respect implique la recherche de critères de distinction objectifs, ne dépendant pas de la technique spécifique employée. Cet aspect est particulièrement important en matière de sécurisation des transmissions en ligne et, notamment, de signature électronique où les progrès techniques sont constants.

Les codifications existantes, en particulier la directive communautaire du 13 décembre 1999, ainsi que le projet de loi uniforme de la Commission des Nations Unies pour le droit commercial international (CNUDCI), insistent d'ailleurs sur le respect du principe de la neutralité technologique. La procédure de consultation menée par l'Office fédéral de la communication (OFCOM) avant l'adoption de l'ordonnance du 12 avril 2000, a également relevé l'importance de ce même principe. Il n'a pourtant pas été consacré dans le cadre de l'ordonnance elle-même, au motif en particulier que d'autres textes réglementaires pourraient être édictés le moment venu. Si cet argument était acceptable dans le cadre d'une ordonnance dont l'adoption ou la modification peut être relativement rapide, il ne l'est plus pour une loi fédérale.

De deux choses l'une : soit le Projet adopte la conception et la structure d'une loi cadre, comme c'est le cas de la directive communautaire du 13 décembre 1999, et le respect du principe de la neutralité technologique doit être impérativement suivi, soit le projet de loi fédérale sur la signature électronique se consacre exclusivement à un système de signature électronique fondé sur une cryptographie asymétrique (infrastructure à clé publique), mais la réglementation en matière de signature électronique est alors incomplète.

En l'espèce, il ressort du rapport explicatif accompagnant le Projet que le Conseil fédéral avait l'intention de respecter le principe de la neutralité technologique. Or, il faut malheureusement constater que la formulation actuelle de l'article 2 du projet n'atteint pas ce but. Il ressort en effet de cette disposition que la délégation de compétences en faveur du Conseil fédéral, *"habilité à arrêter des dispositions d'exécution dans la limite des principes dégagés par la présente loi"* ne pourra vraisemblablement pas être mise en œuvre sans violer le principe constitutionnel de la séparation des pouvoirs. A cet égard, il importe de rappeler que toute norme d'application générale qui serait édictée par le pouvoir exécutif doit reposer soit sur une base légale, soit sur une base constitutionnelle suffisante. Par ailleurs, la délégation ne peut intervenir que dans un cadre défini par le législateur ou le constituant. En l'espèce, la référence générale aux *"principes dégagés par la présente loi"*, paraît trop vague pour éviter le risque d'une délégation abusive. Certes, selon le rapport explicatif, ces principes concernent toutes les techniques susceptibles de s'assurer de l'intégrité des données transmises et de les authentifier (ch. 210.012). Néanmoins, tous les articles du Projet, sans exception, n'ont de sens que dans le cadre d'une infrastructure à clé publique et ne peuvent être étendus à d'autres techniques. Ainsi, sous une formulation prétendument neutre, c'est bien un système basé sur une infrastructure à clé publique, et lui seul, qui est réglementé par le législateur.

La question se pose en des termes encore plus aigus pour ce qui est de l'assimilation, dans certaines situations, de la signature électronique à la signature manuscrite. L'étendue de cette assimilation fait l'objet d'un certain nombre de critiques qui seront analysées ci-dessous séparément (voir ci-dessous, 4). Cependant, il faut déjà relever que l'introduction proposée par le Projet d'un nouvel article 15a du Code des obligations viole également le principe de la neutralité technologique. Sa formulation actuelle exclut en effet tout mécanisme d'authentification autre que la cryptographie asymétrique. Il paraît donc essentiel de modifier, sur ce point déjà, le projet d'article 15a du Code des obligations, en faisant, par exemple, référence à *"tout procédé de signature électronique réglementé par la loi fédérale sur la signature électronique".*

4) Domaine couvert

Le projet de LFSél donne la compétence au Conseil fédéral de conclure des conventions internationales sur la reconnaissance des signatures électroniques, mais il ne dit rien sur la reconnaissance de ces signatures en droit interne, malgré le titre de la loi ! C'est dans le code des obligations et dans d'innombrables lois qu'il faut rechercher la possibilité d'utiliser des signatures électroniques.

Der vorgeschlagene Art. 15a OR führt ausschliesslich im Zivilrecht zu einer rechtlichen Gleichstellung der elektronischen Unterschrift. Eine tatsächliche Gleichstellung der elektronischen Unterschrift erfordert jedoch auch deren Anerkennung im öffentlichen Recht sowie im SchKG. In **das EBGES sollte daher eine generelle Bestimmung aufgenommen werden, wonach die elektronische Signatur der eigenhändigen Unterschrift in der Schweiz gleichgestellt ist.**

Der Begleitbericht geht davon aus, dass mit der zivilrechtlichen Gleichsetzung der digitalen Signatur (Art. 15a OR) auch eine prozessuale Gleichsetzung bewirkt werde (Begleitbericht, 142.2). Dabei bleibt indessen unbeachtet, dass für eine prozessrechtliche Anerkennung eines Dokumentes als Urkunde nicht nur Schriftlichkeit, sondern auch eine Verkörperung notwendig ist. Die Gleichstellung lässt sich gegebenenfalls aber über Art. 21 (Bestätigung der Akkreditierungsstelle, allerdings gebührenpflichtig) erreichen.

Un article avec la teneur suivante devrait être inséré dans la LFSél : ***« Les communications électroniques lisibles sous forme de chiffres et de lettres ou sous forme graphique qui sont munies d'une signature électronique au sens de la présente loi déploient leurs effets juridiques en Suisse comme s'il s'agissait de documents écrits munis d'une signature manuscrite. »***

Cet article éviterait de devoir répéter pour chaque organisme public le principe de la validité de la signature électronique, sans pour autant exclure dans certains cas des prescriptions de forme particulières par exemple pour permettre le traitement électronique ultérieur des informations transmises. Simplement ces prescriptions de forme n'affectent pas la validité de la signature. Elles sont essentiellement liées aux impératifs du traitement ultérieur des données transmises, et le

respect des formes souhaitées peut se traduire par exemple par un émolument réduit qui tient compte des économies réalisées par l'administration grâce au respect de ses exigences de forme.

Cette formulation très générale n'impose pas l'obligation d'accepter des communications électroniques, mais si ce type de communication est utilisé, alors il ne devrait pas pouvoir l'être à sens unique, comme c'est malheureusement le cas encore aujourd'hui en matière judiciaire. En effet, les juges d'instruction et les offices des poursuites communiquent, par exemple, depuis longtemps leurs ordonnances de séquestre par fax, mais les recours contre ces décisions ne sont pas possibles par ce même canal.

5) Sécurité juridique

Trois éléments sont essentiels pour assurer la sécurité juridique en matière d'utilisation des signatures électroniques, si l'on se place **du point de vue de l'utilisateur non expérimenté : une validité juridique générale, une distinction claire entre les signatures électroniques juridiquement valables et celles qui ne le sont pas, et la possibilité de déterminer exactement quand la signature électronique a été utilisée.**

a) **Les documents munis d'une signature électronique au sens de la LFSél doivent être valables en Suisse comme des documents écrits munis d'une signature manuscrite.** Il est impossible de demander aux utilisateurs de consulter à chaque fois la législation fédérale ou cantonale applicable pour savoir si dans un cas la transmission est juridiquement valable ou si elle ne l'est pas, ou si elle ne l'est qu'à condition de respecter des conditions de forme supplémentaires. Seule l'adoption d'un principe clair et général offre la sécurité juridique nécessaire.

b) **La distinction entre une signature valable au sens de la LFSél et une signature certifiée en apparence comme une signature valable, mais en réalité dépourvue de validité juridique au sens de la LFSél doit être évidente pour tout un chacun.** Le degré de sécurité suffisant ne peut être atteint :

   1° que s'il est interdit aux fournisseurs de services de certification de faire état de leur qualité de fournisseurs reconnus pour promouvoir aussi l'offre de certificats non conformes à ceux de la LFSél et,
   2° que si **l'obligation leur est faite d'indiquer expressément sur les certificats non conformes qu'ils ne valent pas comme signature au sens du droit suisse.**

   Un simple renvoi aux conditions générales du fournisseur de services de certification n'offre aucune protection réaliste pour un utilisateur ordinaire.

   A titre de sanction pour d'éventuelles violations, il serait souhaitable de prévoir dans la LFSél que, outre d'éventuelles sanctions administratives, les fournisseurs de services de

certification (et pas seulement les fournisseurs reconnus) répondent des dommages qui résultent des confusions qui pourraient exister en Suisse entre les certificats valant signatures au sens de la LFSél et ceux qui n'ont pas cette portée.

c) Un autre point essentiel pour assurer la sécurité de la signature électronique, est **la possibilité de déterminer de façon sûre le moment de son utilisation.**

Ein handelsübliches Computersystem lässt sich zurückdatieren. Zu Problemen führt dieser Umstand, wenn zwar ein Zertifikat widerrufen wird, es aber einer Drittperson gelingt, eine Rückdatierung vorzunehmen in eine Zeit der noch bestehenden Gültigkeit. In einer solchen Situation wirkt sich die Beweislastumkehr von Art. 17 zuungunsten des Zertifikatsinhabers aus. Aus diesem Grund stellt sich zumindest die Frage, ob es richtig ist, den Aspekt der **Zeitstempel** als „weiteren Dienst" von Zertifikatsanbietern ausserhalb des Geltungsbereichs des neuen Bundesgesetzes „anzusiedeln".

L'ajout automatique de l'indication du moment de l'utilisation de la signature électronique serait de nature à augmenter la sécurité juridique de documents transmis par voie électronique par rapport aux documents transmis par voie traditionnelle.

6) Responsabilité

Pour que les utilisateurs comprennent bien les risques qu'ils encourent en relation avec l'utilisation de certificats, il serait préférable de se référer à des situations existant déjà, plutôt que de créer de nouvelles normes de responsabilité. Il suffirait ainsi de préciser que **le titulaire du certificat répond d'une utilisation abusive de sa signature électronique comme il répondrait de l'utilisation abusive de blanc-seing, l'effet juridique de documents ainsi signés étant en principe identique à celui de documents produits à partir de blanc-seings, à l'insu du signataire.** Cela n'exclut pas a priori l'application également des règles sur la représentation sans pouvoir comme proposé dans le projet de loi.

Un cas différent de l'utilisation abusive est celui de l'utilisation de **la signature électronique par un représentant, avec le consentement du titulaire,** par exemple parce que le représentant n'a pas encore de signature propre et que le titulaire ne peut momentanément signer lui-même. Vu l'absence de signature sociale et l'exclusion des pseudonymes**, un document produit de cette façon pourrait être considéré comme un faux au sens du droit pénal.** Il serait aussi possible de considérer qu'il s'agit d'un cas de représentation légitime, mais dans ce cas il faudrait modifier les dispositions sur la représentation.

Die Bestimmungen des Obligationenrechts über die Stellvertretung (Art. 32 ff. OR) sollten mit einer Bestimmung ergänzt werden, wonach das befugte Handeln unter fremdem Namen, insbesondere **das befugte**

Verwenden fremder Legitimationsmittel unter Abwesenden, die gleichen Rechtswirkungen hat, wie das Handeln im fremden Namen im Sinne von Art. 32 Abs. 1 OR.

La responsabilité propre du fournisseur de certification et de ses auxiliaires requiert des dispositions particulières sur la responsabilité, en particulier pour limiter strictement les cas d'exclusion de responsabilité. Il convient aussi **d'empêcher les reports de responsabilité abusifs sur le titulaire suisse en cas de procès contre le fournisseur de certification à l'étranger,** car cela pourrait priver le titulaire suisse de ses droits, notamment en matière de for. Ainsi par exemple, le client de Swisskey s'engage-t-il à indemniser Swisskey à tous égards si celle-ci se trouve impliquée dans un litige juridique entre le client et des tiers ou simplement incriminée par un tiers, donc même sans faute aucune du client de Swisskey. Cela peut être la ruine pour une petite entreprise qui devrait assumer la défense de Swisskey dans un procès aux USA.

7) For

L'activité de certification de signatures s'apparente à la légalisation d'une signature par un notaire. Il s'agit d'une activité quasi-officielle, même si elle est exercée par des sociétés privées. En raison des contraintes imposées par la LFSél, il est peu probable que les fournisseurs de services de certification soient nombreux. **Il y a donc un risque sérieux que les différentes régions linguistiques n'aient pas un accès égal aux services de certification de signature.** En l'absence de dispositions dans la LFSél comparables à celles que l'on trouve dans la législation sur les assurances (cf. RS 961.01 – chapitre 5), **les Suisses de langue française ou italienne ne pourront probablement avoir accès aux services de certification qu'en acceptant d'être liés par des contrats dont seule la version allemande fera foi et qui seront de surcroît soumis au for exclusif de Zurich.** Sans intervention du législateur, il y a **un risque réel de créer une Suisse à deux vitesses.** Les conditions générales de Swisskey sont un exemple éloquent de cette évolution.

Enfin, pour limiter la tentation de transfert des activités de certification à l'étranger, et surtout pour protéger les utilisateurs suisses, il conviendrait de prévoir **un for impératif au domicile de l'utilisateur suisse pour les procédures judiciaires relatives aux services de certification.** Pour le surplus, le fournisseur étranger qui refuserait le for en Suisse pourrait accompagner son certificat d'une déclaration excluant de ses services les résidents suisses (comme les banques suisses doivent exclure les résidents US des offres de souscription non conforme à la législation US).

III. Conclusion

Le projet de loi mis en consultation n'offre pas la sécurité juridique indispensable du point de vue de l'utilisateur inexpérimenté. Toutefois et moyennant quelques ajouts importants, il constitue néanmoins une base utile pour atteindre l'objectif souhaité d'une reconnaissance juridique des signatures électroniques.

Bern, 2. April 2001