RAPPORT DE LA FSA SUR LE PROJET
D'ORDONNANCE SUR L'INFRASTRUCTURE A CLE PUBLIQUE SUISSE (OICP)

PLAN

I. Introduction

1.- Au vu du peu de temps à disposition pour la rédaction du présent rapport, celui-ci sera nécessairement bref. Il ne traite en particulier pas de la nécessité d'une réglementation dans le domaine de l'infrastructure à clé publique, ni même de son opportunité, mais porte uniquement sur l'étude des modalités d'une telle réglementation à la lumière du projet d'ordonnance publié par l'OFCOM le 3 juin 1999.

Comme l'OFCOM le relève lui-même, la consultation concerne spécialement la question de l'introduction d'une root obligatoire ou non (infra II).

Par ailleurs, une mention particulière sera faite du traitement envisagé dans l'ordonnance de la responsabilité du fournisseur de service de certification (FSC)(infra III).

D'autres points, plus spécifiques, seront encore abordés (infra IV), avant de conclure (infra V).

2.- Il est nécessaire d'insister d'emblée sur l'importance considérable que revêtent dès aujourd'hui les différentes initiatives dans le domaine de l'infrastructure à clé publique en cours au sein d'instances internationales (Union Européenne, CNUDCI, OCDE) ou élaborées par des législateurs nationaux (Allemagne, Etats-Unis). Dans le domaine de la sécurisation du commerce électronique, il ne fait aucun doute qu'*une éventuelle réglementation suisse doit impérativement s'aligner sur un consensus international, pour autant que celui-ci existe, tout en protégeant les intérêts essentiels de la Suisse et des utilisateurs qui y résident*. Dès lors, il s'agit dans ce rapport d'apprécier la conformité de la solution retenue dans l'ordonnance par rapport à celles qui ont cours dans d'autres juridictions plutôt que de chercher à mettre en place le système le plus adéquat, qui resterait lettre morte s'il ne correspond pas à la tendance générale de réglementation existant dans les pays alentours.

3.- Quant au choix de *l'instrument de réglementation*, le rapport explicatif souligne l'urgence à réglementer l'infrastructure à clé publique en Suisse. Dès lors, la question de la reconnaissance juridique des signatures numériques est dissociée de la mise en place d'une réglementation consacrée exclusivement à l'infrastructure à clé publique, qui seule peut trouver sa place dans une ordonnance du Conseil Fédéral, à l'inverse de la reconnaissance juridique des signatures numériques, qui exigerait la modification non seulement du Code des Obligations mais encore

d'autres dispositions éparses tant du droit privé que du droit public, voire l'introduction d'une loi spéciale.

4.- Ce choix des priorités dicté par l'urgence a pour conséquence que le projet d'ordonnance soumis à consultation apparaît comme une *étape intermédiaire* vers un système législatif et réglementaire cohérent pour traiter de l'ensemble des questions résultant de la mise en place et de la généralisation du recours à la signature numérique dans le commerce électronique. On peut en particulier penser à la protection des consommateurs, à des aspects de droit de la concurrence, à la modification des formes prévues par le droit privé, écrites ou authentiques, ainsi que des moyens de communication entre l'administration et ses concitoyens, sans même aborder le domaine fiscal (production de factures TVA sous forme électronique par exemple).

5.- C'est donc sur un projet en construction, loin d'être achevé, que l'on nous demande de nous prononcer (voir également rapport explicatif, chiffre 1 in fine). C'est dire qu'il faut *privilégier les solutions souples ainsi qu'une approche minimaliste de l'intervention étatique*, ce qui laisse bien évidemment une plus grande marge de manoeuvre pour l'adaptation nécessaire des textes à l'évolution du consensus politique, des besoins du marché et de l'évolution technique. Dans cette perpective, le choix d'une réglementation par voie d'ordonnance paraît tout à fait pertinent. Dans la mesure toutefois où la réglementation est appelée à évoluer rapidement, il s'agirait d'éviter de créer par la voie de cette ordonnance, des situations de fait ou de privilégier les scénarios où l'industrie privée investirait lourdement sans être certaine d'être suivie dans les années à venir.

6.- C'est pourquoi il faudrait immédiatement songer à établir *un certain nombre de principes* sur lesquels s'appuierait cette réglementation ainsi que ses développements envisageables (voir par exemple "International Consensus Principles for electronic authentication" édictés par l'Internet Law and policy Form (ILPF) au mois d'avril 1999, http://www.ILPF.org/digsig/intlpril.html). Parmi ces principes se retrouveraient certainement celui de la *neutralité technique* de la réglementation et du *respect de l'autonomie privée, dans la mesure compatible avec les buts d'intérêts publics visés*. Ainsi tant le projet de règles uniformes de la CNUDCI que le projet de directive de l'Union Européenne renoncent à privilégier une méthode d'authentification électronique par rapport à une autre, tout en édictant des règles spécifiques pour l'infrastructure à clé publique. De même les deux textes mentionnent le respect de l'autonomie privée comme priorité. En choisissant de réglementer uniquement l'infrastructure à clé publique, l'OFCOM, indirectement tout au moins, favorise le recours à de tels systèmes et les investissements dans ce domaine. On ne peut donc que regretter que l'ordonnance ne permette pas la reconnaissance, toujours sur une base volontaire, d'autres systèmes de sécurisation électronique liés à des techniques d'authentification qui fourniraient un niveau équivalent de sécurité. Il est vrai que d'autres ordonnances pourraient être édictées le moment venu.

II. Introduction souhaitable d'un root obligatoire ?

1.- Au vu notamment de l'approche minimaliste préconisée plus haut, qui laisse le maximum de marge de manoeuvre pour une réglementation future plus complète, il conviendrait de *renoncer à l'introduction d'une root obligatoire*, pour l'instant prévue à la section 4 de l'ordonnance.

2.- En faveur de l'introduction d'une telle root obligatoire, le rapport explicatif (sous chiffre 3.4 in fine) mentionne tout d'abord la possibilité qui serait ainsi offerte aux utilisateurs de vérifier les signatures numériques en remontant la chaîne de certifications jusqu'à l'autorité primaire. Il s'agit certes d'une garantie supplémentaire, pour reprendre les termes du rapport explicatif, mais d'une valeur toute relative, car elle dépend de la confiance qu'ont les utilisateurs dans l'autorité primaire elle-même. Or, il me semble précisément que le "label de qualité" découle déjà de la reconnaissance d'un fournisseur de service de certification (FSC) au sens de la présente ordonnance, s'il en respecte les exigences essentielles. En reconnaissant officiellement un tel FSC, l'Etat renforce certainement la confiance que les utilisateurs pourraient avoir dans le système de l'infrastructure à clé publique. Il n'y a pas lieu de fournir une garantie supplémentaire en obligeant l'OFCOM ou toute autre entité à signer numériquement le certificat du FSC lui-même. Il convient cependant de relever qu'une telle certification faciliterait probablement l'accès au marché à de nouveaux FSC en leur donnant d'emblée une référence reconnue.

3.- Le deuxième argument avancé par le rapport explicatif en faveur de l'introduction d'une root obligatoire tient à la facilitation qui en découlerait pour la reconnaissance internationale du FSC. Là encore, l'argument ne me paraît de loin pas décisif. En effet, un système de root obligatoire nécessiterait, comme le précise le rapport explicatif lui-même, qu'un accord international soit signé avant que l'autorité de certification étrangère puisse être reconnue par l'OFCOM, ce qui ralentira bien entendu considérablement une telle mesure. Ce système de root obligatoire me semble aller donc *à l'encontre des soucis de flexibilité et d'urgence à légiférer* qui prévalaient à la rédaction de cette ordonnance. De plus, il est tout à fait possible que des autorités de certification étrangères ne puissent tout simplement pas être certifiées par une autorité étatique suisse, au vu de leur propre législation interne ou encore d'accords privés exclusifs passés entre différentes autorités de certification.

4.- Même si le système de root obligatoire devait être retenu, on voit mal pourquoi il serait nécessaire d'interdire les sous-certifications, comme le prévoit pour l'instant l'article 17 de l'ordonnance. En effet, il suffirait pour l'utilisateur de remonter la chaîne de certifications jusqu'à l'autorité primaire, celle-ci étant libre de ne pas signer les certificats de FSC qui procèdent à des sous-certifications douteuses. Il en va de même pour l'exclusion des certifications croisées. Les arguments sécuritaires avancés à l'appui de l'interdiction des sous-certifications par le rapport explicatif ne me semblent pas convaincants et limitent encore à mes yeux l'attrait d'une root obligatoire, système qui n'est par ailleurs pas privilégié à l'étranger (à l'exception notable de l'Allemagne).

5.- En résumé, la recherche d'un label de qualité poursuivie par l'ordonnance dans le cadre de l'introduction d'un système d'accréditation volontaire est tout à fait satisfaite par la procédure d'accréditation et le respect des exigences essentielles posées dans l'ordonnance et n'implique pas l'introduction d'une garantie additonnelle,

toute relative, qui consisterait à ériger l'OFCOM comme autorité primaire obligatoire, sans même mentionner les coûts supplémentaires engendrés par une infrastructure plus lourde.

III. Questions de responsabilité

1.- Un traitement adéquat des questions de responsabilité du FSC est *essentiel au succès de la mise en place d'une infrastructure à clé publique*. En effet, dans une perspective de renforcement de la confiance des utilisateurs dans le commerce électronique, il faut impérativement éviter que les FSC n'aient pas à rendre compte de leurs éventuels agissements illicites.

2.- Dans le cadre d'une infrastructure à clé publique, la question de la responsabilité du FSC doit s'analyser vis-à-vis de son client, en faveur duquel un certificat a été émis, ainsi que vis-à-vis des tiers qui se fient à ce certificat dans le cadre des transactions électroniques.

3.- Dans le projet d'ordonnance, l'article 20 constitue le siège de la matière.

Il convient en premier lieu de remarquer que cette disposition renvoie simplement au Code des Obligations, ce qui n'a rien de surprenant dans la mesure où le système de la hiérarchie des normes empêcherait de toute manière une réglementation prenant la forme d'une ordonnance de déroger aux règles en tout cas impératives du Code des Obligations.

4.- Seulement, la question n'est pas aussi simple. En effet, nous avons déjà eu l'occasion d'insister sur le caractère global et non pas national du commerce électronique et de la nécessité de prendre en compte les solutions internationales en cours d'élaboration ou déjà adoptées à l'étranger. A cet égard, il importe de relever qu'*il n'est absolument pas certain que le droit suisse soit systématiquement applicable au traitement de la responsabilité du FSC sans modifications législatives*.

5.- Vis-à-vis de son client, le FSC entretient une relation de mandat ou de contrat d'entreprise (dans la mesure où l'on devait considérer que l'établissement d'un certificat à des conditions données constitue une obligation de résultat consistant en la livraison d'un ouvrage). Dans ce cadre, l'application des règles générales de la LDIP, en particulier ses articles 112 et 117 amènera certainement à la compétence des tribunaux et à l'application du droit du domicile du FSC. Dans la plupart des cas, il s'agira du droit suisse. Mais la solution sera peut-être différente, au vu des art. 114 et 120 LDIP et de l'éventuelle législation spéciale étrangère, dans le cadre de la protection d'un consommateur domicilié à l'étranger mais client d'une FSC établie en Suisse. (N.B. L'inverse, à savoir un client suisse d'une FSC étrangère doit aussi être envisagé).

6.- En outre, la responsabilité du FSC envers les tiers qui se fient au certificat publié, en l'absence d'une quelconque relation contractuelle, sera de nature délictuelle. Dans un tel cas, l'application des articles 129 et 133 LDIP amène à la compétence possible des tribunaux du lieu de commission de l'acte illicite (en l'occurrence, lieu de l'hébergement du site publiant la liste des certificats et la liste de révocation ou lieu du siège du FSC, ou lieu de réception de la certification erronnée), ou également du lieu où les effets dommageables se font ressentir (lieu à partir duquel la consultation s'est effectuée). La réglementation prévue dans la Convention de Lugano ne change pas fondamentalement ce système. Il n'est donc pas certain que

le droit suisse s'applique en tous les cas, sans modifications législatives, à supposer que les tribunaux helvétiques soient compétents, ce qui pourrait aussi rendre souhaitable certaines modifications législatives dans ce domaine.

7.- La question de la compétence et du droit applicable se posera certainement de manière encore plus intense *pour le cas où le FSC, domicilié à l'étranger, est reconnu en vertu de l'article 21 de l'ordonnance*. Certes, cette disposition prévoit qu'une telle reconnaissance ne pourrait intervenir que sur la base d'un traité international, qui pourrait régler les questions de compétence et de droit applicable. A défaut, on pourrait se poser la question de savoir si la reconnaissance par l'organisme d'accréditation au sens de l'ordonnance implique que ce FSC soit soumis au droit suisse, celui-ci devant respecter toutes les exigences essentielles posées par l'ordonnance, y compris l'article 20 concernant la responsabilité.

8.- Il ressort de ce qui précède que l'ordonnance, tout comme la législation ultérieure sur la responsabilité des autorités de certification, devra *étudier attentivement les questions de droit international privé liées à la reconnaissance internationale des systèmes de certification dans le cadre d'une infrastructure à clé publique*.

A supposer que le renvoi de l'article 30 de l'ordonnnace à l'application du Code suisse des obligations soit efficace, quelle est l'étendue de la responsabilité du FSC ?

Responsabilité vis-à-vis du client

9.1.- Comme nous l'avons déjà mentionné, la relation entre le FSC et son client est de nature contractuelle. Il peut s'agir d'un mandat ou d'un autre contrat sui generis assimilé au mandat, ainsi que, éventuellement, d'un contrat d'entreprise. En tous les cas, les articles 100 et 101 du Code des Obligations sont a priori applicables.

Or, l'article 20 alinéa 3 de l'ordonnance stipule très clairement qu'aucune limitation de responsabilité n'est possible pour les obligations découlant de la présente ordonnance. Bien évidemment, cette disposition ne peut pas être comprise dans le sens d'une règle dérogeant au régime instauré par les articles 100 et 101 du Code des obligations, loi fédérale qui l'emporte de toute manière sur une réglementation du Conseil Fédéral. En revanche, dans le cadre du régime préconisé d'accréditation volontaire, mais qu'il faudrait peut-être rendre obligatoire, il est évident que l'absence de clause limitative de responsabilité pour les obligations découlant de la présente ordonnance pourrait tout à fait être considérée comme une exigence essentielle pour la reconnaissance du FSC au sens de la présente ordonnance.

9.2.- Il reste à déterminer quelles sont les obligations auxquelles l'article 20 alinéa 3 de l'ordonnance fait référence.

a) Il s'agit en premier lieu de l'**article 7**, dont l'alinéa 1er oblige le FSC à publier ses conditions générales. Or, cela n'est certainement pas les conditions générales du rapport contractuel entre le FSC et son client qui sont visées, mais bien les conditions générales qui ont prévalu à l'établissement du certificat et qui sont destinées aux tiers qui seront amenés à s'y fier. Le rapport explicatif, en page 5, ne prétend pas autre chose lors qu'il fait référence au "Certification Practice Statement". *Il conviendrait donc d'être précis dans la formulation définitive de l'ordonnance sur ce point*.

Quant à l'alinéa 2ème de l'article 7, il oblige le FSC à rendre attentifs ses clients aux "conséquences que peut avoir la divulgation ou la perte de leur clé privée". En outre, le FSC doit leur indiquer les mesures appropriées pour maintenir secrète leur clé privée. L'étendue de cette obligation est incertaine. S'agit-il uniquement de rendre attentif le client au fait que la perte du caractère secret de la clé privée permettrait à toute personne qui en aurait connaissance de se faire passer auprès des tiers comme étant l'expéditeur légitime du message ? S'agit-il plutôt de rendre attentif le client qu'en cas de perte du caractère secret de la clé privée, c'est lui qui devra supporter les conséquences, notamment en cas de certification erronée ? Dans cette dernière hypothèse, dans la mesure où, comme nous le verrons, le FSC est tenu de garantir l'identité entre le détenteur de la clé privée et la clé publique contenue dans le certificat qu'il a lui-même signé, cette obligation serait contradictoire avec le principe exprimé à l'article 20 alinéa 3 de l'ordonnance.

b) L'**article 9**, consacré à la révocation des certificats électroniques, pose également problème. En effet, le risque le plus important assumé par le FSC, tant vis-à-vis de son client que vis-à-vis des tiers qui se fient au certificat est soit de maintenir un certificat alors qu'il devrait être révoqué, laissant par là perdurer l'illusion de sa validité continue, soit de révoquer à tort un certificat par ailleurs valable, empêchant par là au client de s'identifier correctement vis-à-vis des tiers.

Or, l'article 9 alinéa 1er de l'ordonnance prévoit l'obligation pour le FSC de révoquer "immédiatement" les certificats électroniques à la demande des personnes en faveur desquelles ils ont été émis. Cette dernière formulation est malheureuse, dans la mesure où il serait certainement moins ambigu de recourir aux termes de "titulaires". De plus, *l'obligation imposée à l'alinéa 1er est irréaliste*. En effet, l'alinéa 2ème de l'article 9 de l'ordonnance impose au FSC saisi d'une demande de révocation, de s'assurer de la légitimité de cette demande. Que faut-il entendre par là ? S'il faut envisager que le FSC doit s'assurer non seulement que la demande de révocation émane de la personne autorisée au moment où la demande est effectuée (et non pas au moment de l'enregistrement du certificat, seule information dont elle dispose), mais également que le FSC doit s'assurer que la demande de révocation intervient sur la base d'une cause légitime, une telle obligation s'étend bien au-delà de ce qui est raisonnablement exigible de la part des FSC. Par ailleurs, il est évident qu'une telle recherche de légitimité est contradictoire avec l'exigence de révoquer *immédiatement* le certificat contenue à l'alinéa 1er. Ce système est donc insatisfaisant et risque de dissuader plus d'un FSC qui désirerait être reconnu de requérir son accréditation.

Par ailleurs, il est clair qu'un FSC désirera recourir aux possibilités que lui offre l'article 100 et l'article 101 du Code des Obligations dans le cadre de son obligation de révocation du certificat. Ces limitations pourraient porter tant sur le délai que sur l'étendue de la vérification nécessaire avant de donner suite à la demande de révocation. Or, en vertu de l'article 20 alinéa 3, aucun de ses éléments ne pourrait faire l'objet d'une clause limitative de responsabilité. Il s'agit là à nouveau d'un élément susceptible de dissuader un FSC de recourir sur une base volontaire à la réglementation prévue dans l'ordonnance.

c) A cela s'ajoute que l'alinéa 3 de l'article 9 prévoit encore une obligation plus étendue. Tout d'abord, il importe de signaler que le délai prévu à l'alinéa 3 de l'article 9 est un délai semble-t-il moins strict que celui prévu à l'alinéa 1er, puisqu'il est fait mention d'une obligation de révoquer "sans tarder" et non plus "immédiatement".

Surtout, cette révocation devrait intervenir s'il s'avère que le certificat a été obtenu de manière frauduleuse. Or, il est difficile pour le FSC de s'en assurer. Ses seules obligations, dans le cadre de la régularité de l'enregistrement du futur client, résultent de l'article 6 de l'ordonnance. L'alinéa 3 de l'article 9 prévoit également une obligation de révoquer le certificat sans tarder si celui-ci comportait des indications fausses ou que, de toute autre manière, il ne soit plus apte à garantir le lien entre une personne déterminée et sa clé publique. Là également, l'ordonnance prévoit une obligation à la charge du FSC, qu'il ne pourra limiter au vu de l'article 20 alinéa 3 de l'ordonnance. En effet, tel qu'il est formulé, le 3ème alinéa de l'article 9 oblige le FSC à s'assurer de l'exactitude des indications fournies pour l'établissement du certificat non seulement au moment où il est créé mais également pendant toute sa durée (comme les banques doivent vérifier dans la durée que les indications fournies par les clients lors de l'ouverture des comptes restent valables pendant la durée des relations contractuelles) le FSC ayant l'obligation de le révoquer s'il découvre que les indications deviennent fausses à un moment ou à un autre (comme les banques peuvent devoir mettre fin aux rapports contractuels avec leurs clients, s'il s'avère que les indations initiales sont devenues fausses). Indirectement, le FSC pourrait devenir *garant de l'exactitude de l'ensemble des informations contenues dans le certificat*, ce qui va évidemment bien au-delà que d'exiger le respect des exigences essentielles contenues dans la présente ordonnance, notamment au stade de l'enregistrement du certificat. Cette formulation va également au-delà de celle contenue à l'article 20 alinéa 1er in fine de l'ordonnance, qui laisse certes entendre que la FSC est avant tout responsable du lien entre une personne déterminée et sa clé publique, mais seulement au moment de l'établissement du certificat.

Responsabilité du FSC vis-à-vis des tiers qui se fient au certificat publié

10.- Comme nous avons déjà eu l'occasion de le mentionner, la responsabilité du FSC vis-à-vis des tiers qui se fient au certificat publié est de nature extra-contractuelle, sauf circonstances spéciales. On pourrait en effet imaginer que le tiers en question soit par ailleurs client du même FSC; il serait alors envisageable de lui opposer les conditions générales qu'il a souscrites avec le FSC, non seulement en tant que client, mais également en tant que tiers se fiant au certificat par rapport à une transaction donnée.

11.- Mis à part ce cas de figure, la responsabilité du FSC, à supposer que le droit suisse soit applicable, sera certainement analysée sur la base des articles 41 et suivants du CO - sous réserve peut-être d'une responsabilité causale découlant de la loi fédérale sur la responsabilité de la Confédération et de ses agents si l'OFCOM certifie les FSC qui attestent de certificats erronés, ce qui constitue encore un argument à l'encontre d'une root obligatoire.

Dans le cadre des articles 41 et suivants CO, si le dommage subi correspond au gain manqué parce que, par exemple, un contrat n'a pas pu être conclu ou exécuté du fait d'une révocation erronée du certificat, le préjudice est purement patrimonial. Dans cette hypothèse, l'application de la théorie de l'illicéité objective, qui a cours en Suisse, ne permettrait la réparation d'un tel dommage qu'en cas de violation d'une norme protectrice du bien juridique atteint. En l'absence d'une quelconque réglementation étatique pouvant fonder cette illicéité objective, elle est incertaine.

Or, par l'introduction d'une ordonnance fixant les exigences essentielles à respecter par les FSC dans le cadre de leur activité réglementée, on pourrait certainement plus facilement fonder une illicéité objective en cas de non-respect des prescriptions prévues dans l'ordonnance, celle-ci ayant précisément pour but de protéger les tiers qui se fient au certificat publié. Ainsi, *l'introduction de l'ordonnance aurait pour conséquence de renforcer la responsabilité des FSC vis-à-vis des tiers*. Il s'agit là d'un aspect qui n'est pas abordé dans le rapport explicatif mais qui me semble important, dans la mesure où il est à nouveau de nature à dissuader les FSC de solliciter leur reconnaissance sur une base volontaire et à rendre donc la reconnaissance obligatoire.

12.- Un dernier point reste à aborder dans le cadre de l'étude des articles 41 et suivants CO : celui de l'influence de la publication d'un "Certification Practice Statement" sur la responsabilité du FSC. En effet, on se souvient que l'article 7 alinéa 1er oblige le FSC à publier ses conditions générales, ce par quoi il faut entendre précisément le "Certification Practice Statement". Or, il est évident qu'une telle publication ne peut avoir le même effet que les articles 100 et 101 du Code des Obligations, à défaut de relations contractuelles. En revanche, en tant que "disclaimer" général, la mention des limitations de responsabilité sur les certificats telles qu'elles sont également prévues à l'article 20 alinéa 2 de l'ordonnance, aurait pour effet de permettre la reconnaissance, peut-être, d'une faute concomitante du tiers qui se fie au certificat au-delà des indications de prudence qui y sont mentionnées.

13.- Il demeure que de telles limitations de responsabilité sont également exclues, en vertu de l'article 20 alinéa 3 de l'ordonnance, pour ce qui est des obligations essentielles découlant de la présente ordonnance, ce qui renvoie la discussion menée plus haut dans le cadre de l'étude de la limitation de la responsabilité vis-à-vis du client.

IV. Autres points

1.- L'article 8 du projet d'ordonnance interdit au FSC de générer ou de sauvegarder eux-mêmes les clés privées de leurs clients. La nécessité de cette réglementation n'est pas évidente. Le rapport explicatif mentionne simplement le souci de renforcer la sécurité (sous chiffre 3.3). De fait, il existe un risque d'abus de la part du FSC s'il n'offre pas la possibilité au titulaire de la clé privée de la révoquer ou de la modifier en tout temps. Cependant, la pratique qui consiste à gérer la clé privée pour le compte d'autrui et à la conserver par devant soi (key escrow) est très répandue. Cette interdiction ne semble dès lors pas nécessaire, ce d'autant plus que l'art. 14 du projet réserve la loi fédérale sur la protection des données.

2.- Le renvoi de l'article 11 alinéa 2 à l'article 11 alinéa 3 de l'ordonnance signifie que la consultation prévue à l'article 11 alinéa 1 est garantie envers les tiers par des moyens de télécommunication publics et sans autres frais supplémentaires, mais pour les six premières années seulement, sans explication quant à cette limite.

Par ailleurs, pourquoi ne pas faire correspondre exactement la prescription publiée à l'article 962 alinéas 1 et 3 CO ? Ainsi, le délai pourrait être de 10 ans à partir de la fin de l'année civile qui suit la transaction en question.

V. Conclusions

1.- Dans son ensemble, le projet d'ordonnance sur l'infrastructure à clé publique est satisfaisant. Il faut certainement approuver la démarche qui consiste à ménager le maximum de flexibilité dans une telle réglementation, dans la perspective d'une réglementation plus complète et cohérente à moyen terme, par la modification notamment du Code des Obligations.

2.- Dans cette perspective, il y a lieu de privilégier une infrastructure sans root obligatoire, pour éviter la mise en place d'une structure dont les avantages attendus (plus grande légimité des FSC) me semblent loin de compenser les inconvénients (plus grande lourdeur, absence de flexibilité pour la reconnaissance internationale, coûts supplémentaires, non alignement sur la majorité des initiatives internationales).

3.- Un des aspects où la réglementation apparaît la moins satisfaisante est certainement celui de la responsabilité du FSC, à qui *le projet d'ordonnance impose un certain nombre d'obligations dont l'étendue n'est pas claire, sans qu'il puisse pour autant limiter sa responsabilité, même vis-à-vis de ses clients*. Ce est en particulier le cas pour l'article 9 pour ce qui est de la révocation du certificat, tant sur requête de l'ayant-droit que d'office si ce certificat apparaît erroné. Il s'agit là d'obligations extrêmement lourdes imposées au FSC, qui pourraient être incompatibles avec un système d'accréditation volontaire

   Toujours vis-à-vis des tiers, la mise en place de cette ordonnance pourrait également, indirectement, renforcer la responsabilité du FSC, en constituant la base pour l'instant incertaine susceptible de fonder une responsabilité pour acte illicite, ce qui n'est pas en soi critiquable mais a peut-être été sous-estimé dans le projet actuel.

4.- Enfin, il n'y a également pas lieu d'interdire au FSC qui désirerait être reconnu de fournir au client des prestations annexes, soit pour ce qui est de la génération, soit pour ce qui est de la conservation des clés privées.

Lausanne, le 6 juillet 1999