Reconnaissance transfrontalière des méthodes d'authentification/des signatures électroniques

Robert Boekhorst, Madrid, 15 décembre 2005

Introduction

Reconnaissance transfrontalière des méthodes d'authentification / des signatures électroniques:

- Qu'est-ce que la "reconnaissance transfrontalière"? Pourquoi est-elle pertinente?
- Quelles sont les lois internationales relatives aux signatures électroniques?
- Comment l'Union européenne a-t-elle abordé la reconnaissance transfrontalière dans la directive sur les signatures électroniques (Directive 1999/93/EC ("les Directives sur les Signatures Electroniques, DSE")?
- Normalisation: est-elle nécessaire, que peut-on dire sur le niveau de normalisation?
- Au vu des réponses aux questions susmentionnées, existe-t-il des solutions concrètes?

Pourquoi la reconnaissance transfrontalière est-elle pertinente?

La reconnaissance transfrontalière comprend différents aspects:

- Un aspect technique : l'interopérabilité
- Plusieurs aspects juridiques: un produit portant la signature électronique d'un fournisseur d'un pays A sera-t-il reconnu par les lois nationales d'un pays B?
- Quels sont les effets juridiques de l'utilisation d'une signature électronique lors d'une opération transfrontalière?

Législation internationale

- Initiatives des Nations Unies, et de la CPI et l'OCDE
- Toutefois, aucune de ces initiatives ne prévoit des lois nationales juridiquement contraignantes
- Une initiative importante est la Loi type de la CNUDCI sur le commercie électronique et la Loi type de la CNUDCI sur les signatures électroniques (LSE)
- En ce qui concerne la reconnaissance transfrontalière, l'article 12 de la LSE est déterminant. Le principe de "non discrimination sur base du lieu"
- Depuis le milieu des années 1990, beaucoup de lois nationales sont adoptées dans le monde
- La directive européenne sur la signature est actuellement la seule législation contraignante au niveau international. Cette directive ne lie apparemment que les Etats membres

Reconnaissance transfrontalière dans l'Union européenne

Dans l'Union européenne, la DSE a créé un cadre légal destiné à faciliter l'utilisation de la signature électronique et sa reconnaissance juridique

Les articles suivants sont pertinents en ce qui concerne la reconnaissance transfrontalière

- Accès au marché (article 3 DSE)
- Contrôle de l'état d'origine, libre circulation des produits portant une signature électronique dans le marché intérieur (article 4 DSE)

- Effets juridiques des signatures électroniques (article 5)
- Reconnaissance internationale de pays tiers (article 7)

Effets juridiques dans l'Union européenne

Article 5 DSE

- Qu'est-ce qui a fait l'objet d'une harmonisation?
- Que n'a-t-on pas harmonisé?

Article 5 Effets juridiques des signatures électroniques (1)

1. *Les Etats membres* doivent veiller à ce que des signatures électroniques avancées basées sur un certificat qualifié et créées par un système sécurisé de création de signature:

   a) répondent aux exigences légales d'une signature à l'égard de données électroniques de la même manière qu'une signature manuscrite répond à ces exigences à l'égard de données manuscrites ou imprimées sur papier et
   b) soient recevables comme preuves en justice.

Ce qui signifie que les critères suivants doivent être conformes à:

.....

Article 2 DSE

2) «signature électronique avancée» une signature électronique qui satisfait aux exigences suivantes:

a) être liée uniquement au signataire;

b) permettre d'identifier le signataire;

c) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif

et

d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable;

Annexe I

ANNEXE I

Exigences concernant les certificats qualifiés

Tout certificat qualifié doit comporter:

a) une mention indiquant que le certificat est délivré à titre de certificat qualifié;

b) l'identification du prestataire de service de certification ainsi que le pays dans lequel il est établi;

c) le nom du signataire ou un pseudonyme qui est identifié comme tel;

d) la possibilité d'inclure, le cas échéant, une qualité spécifique du signataire, en fonction de l'usage auquel le certificat est destiné;

e) des données afférentes à la vérification de signature qui correspondent aux données pour la création de signature sous le contrôle du signataire;

f) l'indication du début et de la fin de la période de validité du certificat;

g) le code d'identité du certificat;

h) la signature électronique avancée du prestataire de service de certification qui délivre le certificat;

i) les limites à l'utilisation du certificat, le cas échéant et

j) les limites à la valeur des transactions pour lesquelles le certificat peut être utilisé, le cas échéant.

Annexe II

ANNEXE II

Exigences concernant les prestataires de service de certification délivrant des certificats qualifiés

Les prestataires de service de certification doivent:

a) faire la preuve qu'ils sont suffisamment fiables pour fournir des services de certification;

b) assurer le fonctionnement d'un service d'annuaire rapide et sûr et d'un service de révocation sûr et immédiat;

c) veiller à ce que la date et l'heure d'émission et de révocation d'un certificat puissent être déterminées avec précision;

d) vérifier, par des moyens appropriés et conformes au droit national, l'identité et, le cas échéant, les qualités spécifiques de la personne à laquelle un certificat qualifié est délivré;

e) employer du personnel ayant les connaissances spécifiques, l'expérience et les qualifications nécessaires à la fourniture des services et, en particulier, des compétences au niveau de la gestion, des connaissances spécialisées en technologie des signatures électroniques et une bonne pratique des procédures de sécurité appropriées; ils doivent également appliquer des procédures et méthodes administratives et de gestion qui soient adaptées et conformes à des normes reconnues;

f) utiliser des systèmes et des produits fiables qui sont protégés contre les modifications et qui assurent la sécurité technique et cryptographique des fonctions qu'ils assument;

g) prendre des mesures contre la contrefaçon des certificats et, dans les cas où le prestataire de service de certification génère des données afférentes à la création de signature, garantir la confidentialité au cours du processus de génération de ces données;

h) disposer des ressources financières suffisantes pour fonctionner conformément aux exigences prévues par la présente directive, en particulier pour endosser la responsabilité de dommages, en contractant, par exemple, une assurance appropriée;

i) enregistrer toutes les informations pertinentes concernant un certificat qualifié pendant le délai utile, en particulier pour pouvoir fournir une preuve de la certification en justice. Ces enregistrements peuvent être effectués par des moyens électroniques;

j) ne pas stocker ni copier les données afférentes à la création de signature de la personne à laquelle le prestataire de service de certification a fourni des services de gestion de clés;

k) avant d'établir une relation contractuelle avec une personne demandant un certificat à l'appui de sa signature électronique, informer cette personne par un moyen de communication durable des modalités et conditions précises d'utilisation des certificats, y compris des limites imposées à leur utilisation, de l'existence d'un régime volontaire d'accréditation et des procédures de réclamation et de règlement des litiges. Cette information, qui peut être transmise par voie électronique, doit être faite par écrit et dans une langue aisément compréhensible. Des éléments pertinents de cette information doivent également être mis à la disposition, sur demande, de tiers qui se prévalent du certificat;

l) utiliser des systèmes fiables pour stocker les certificats sous une forme vérifiable de sorte que:

— seules les personnes autorisées puissent introduire et modifier des données,

— l'information puisse être contrôlée quant à son authenticité,

— les certificats ne soient disponibles au public pour des recherches que dans les cas où le titulaire du certificat a donné son consentement et

— toute modification technique mettant en péril ces exigences de sécurité soit apparente pour l'opérateur.

Annexe III

ANNEXE III

Exigences pour les dispositifs sécurisés de création de signature électronique

1. Les dispositifs sécurisés de création de signature doivent au moins garantir, par les moyens techniques et procédures appropriés, que:

   a) les données utilisées pour la création de la signature ne puissent, pratiquement, se rencontrer qu'une seule fois et que leur confidentialité soit raisonnablement assurée;

   b) l'on puisse avoir l'assurance suffisante que les données utilisées pour la création de la signature ne puissent être trouvées par déduction et que la signature soit protégée contre toute falsification par les moyens techniques actuellement disponibles;

   c) les données utilisées pour la création de la signature puissent être protégées de manière fiable par le signataire légitime contre leur utilisation par d'autres.

2. Les dispositifs sécurisés de création de signature ne doivent pas modifier les données à signer ni empêcher que ces données soient soumises au signataire avant le processus de signature.

Article 5 Effets juridiques des signatures électroniques (2)

2. Les États membres veillent à ce que l'efficacité juridique et la recevabilité comme preuve en justice ne soient pas refusées à une signature électronique au seul motif que:

- la signature se présente sous forme électronique, ou
- qu'elle ne repose pas sur un certificat qualifié, ou
- qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité de service de certification, ou
- qu'elle n'est pas créée par un dispositif sécurisé de création de signature.

Reconnaissance transfrontalière des Etats tiers

L'article 7 contient trois alternatives à la reconnaissance de certificats qualifiés émis par un prestataire de service de certification établi dans un pays tiers:

- Le prestataires de service de certification doit remplir les conditions visées dans la présente directive *et* doit avoir été accrédité
- Un prestataire de service de certification établi dans la Communauté garantit le certificat
- Reconnaissance par des accords bilatéraux ou multilatéraux

Note: Il n'existe pas d'obligation envers le produit de signature électronique, ni de certificat ordinaire. Ici, chaque loi nationale de l'Etat membre de l'UE donnera la réponse

Ce type d'exigences supplémentaires apparaît souvent dans la législation sur la signature électronique dans le monde

Normes

Des initiatives en matière de normalisation ont été prises par:

- L'UIT (Union internationale des télécommunications (x.509)
- La Coopération économique Asie-Pacifique (CEAP)
- The Internet Engineering Task Force (IETF)
- Le consortium W3C (World Wide Web Consortium)
- Les services de signature électronique de l'OASIS

- La Commission européenne: l'EESSI (initiative européenne sur la normalisation de la sécurité juridique). Résultat: les normes du Comité Européen de Normalisation (CWA) (comme CWA 14167 et CWA 14167) (article 3 sous-paragraphe 5 de la DSE)

- L'Institut européen des normes de télécommunication (ETSI) a produit de nombreuses spécifications techniques par exemple, les formats de signatures électroniques définis par la norme ETSI TS 101 733, le format des certificats qualifiés définis par la norme TS 101 862, et les exigences concernant la politique mise en œuvre par les autorités de certification délivrant des certificats qualifiés déterminés par la norme TS 101 456 (voir: www.ict.etsi.org)

Toutefois, aucune norme internationale n'existe pour le moment

Solutions concrètes pour des transactions B2B

- Choisir une législations
- Insérer une Politique de signature dans l'accord électronique
- Etudier les possibilités d'insérer des clauses en matière de preuves

Conclusions

Dans le contexte de l'UE, la validité créée par la directive représente le plus stricte minimum:

- Le nombre d'exigences à satisfaire pour une équivalence fonctionnelle (Article 5) sont (trop?) considérables
- Tous les autres types de signatures électroniques ne sont pas sûrs en ce qui concerne les effets juridiques ou la recevabilité, cela dépend à nouveau de l'interprétation donnée par les cours et les règles nationales
- La reconnaissance par des pays tiers de signatures électroniques réalisées dans l'Union européenne varie et nécessite une évaluation préalable des lois applicables dans tel ou tel pays
- La reconnaissance dans l'Union européenne de signatures électroniques qui ne sont pas réalisées dans des pays de l'UE dépend des lois nationales appliquées dans l'UE. En ce qui concerne la DSE, les certificats qualifiés ne sont seulement reconnus lorsque les conditions mentionnées à l'article 7 sont respectées
- Cependant, les signatures électroniques vont rester et bon nombre des incertitudes existantes peuvent être levées concrètement