Caprioli & ASSOCIÉS

C.N.U.D.C.I./U.N.C.I.T.R.A.L.
Nations Unies - New York, 14 février 2011

« De l'authentification à la signature électronique : quel cadre juridique pour la confiance dans les communications électroniques internationales ? »

Eric A. CAPRIOLI
Avocat à la Cour de Paris
Docteur en droit
Membre de la délégation française aux Nations Unies

Le Cabinet Caprioli & Associés est une société d'avocats en droit des affaires : conseil, contentieux et arbitrage.

Spécialisé en :

– Technologies de l'information et des communications électroniques
– Données à caractère personnel et vie privée
– Sécurité des systèmes d'information
– Dématérialisation des documents et des échanges
– Informatique,
– Propriétés intellectuelles (droit d'auteur, marques, dessins, noms de domaines, brevets, logiciels, bases de données, …)

Adresses : **6, rue Saulnier, 75009 Paris**
9, avenue Henri Matisse, 06200 Nice
Site Web : **www.caprioli-avocats.com**
Mail : **contact@caprioli-avocats.com (Nice)**
contactparis@caprioli-avocats.com (Paris)

Les opinions mentionnées dans la présentation n'expriment que les opinions personnelles de l'auteur et n'engagent en aucune façon celles de la délégation française.

I. Les principaux concepts liés à la gestion de l'identité

a. Eléments de définitions

i. Authentification (dont l'authentification forte : deux canaux)

ii. Identification

iii. Identité numérique

iv. Signature technique (garantie d'intégrité comme dans la facture électronique et le bulletin de paie)

v. Signature électronique

b. Exigences relatives à l'identité numérique

i. L'incontournable sécurité technique

ii. Exemple français en matière de lutte contre le blanchiment, et les jeux en ligne

II. Mise en œuvre juridique internationale

a. Besoin de nouvelles normes juridiques internationales

i. Authentification

ii. Signature technique

iii. Horodatage

iv. Signature des personnes morales

v. Certificat éphémères

vi. Responsabilités dans le cadre d'une ICP

b. Autres possibilités et moyens connexes

i. Reconnaissance mutuelle

ii. Fédération d'identité

iii. La labellisation

- Le label IDNum (France)
- Le Label SuisseID (Suisse)
- Autres expériences

Introduction : les enjeux juridiques et sociaux

- L'accès aux réseaux et aux données numériques, ainsi que les transactions en ligne constituent une nouvelle donne fondamentale des communications.
- Le besoin de confiance s'impose pour les communications électroniques internationales.
- Interrogations sur les manifestations de l'identité numérique, authentifications, signatures électroniques.
- Nouvelles exigences en termes de mesures de sécurité, notamment via des méthodes d'authentification : fraude, usurpation d'identité, …
- Problématique de la reconnaissance transfrontière des méthodes d'authentification et de l'harmonisation des règles nationales (ex. certificats émis par des tiers, dématérialisation des moyens de paiement).

Les principaux concepts liés à la gestion de l'identité
Eléments de définitions

Authentification et authentification forte

- L'authentification électronique des personnes prend le relais de l'identification physique traditionnelle
- Tendance de la jurisprudence vers le renforcement de la sécurité :
  - Affaire Shames Yeakel vs Citizen Financial Bank du 21 août 2009 : confirmation de l'authentification forte pour les opérations en ligne.
  - Affaire Natixis, Cour d'appel de Nancy 18 novembre 2010 : condamnation de la banque pour manquement à l'obligation de sécurité et de sécurisation des opérations de gestion informatique des comptes en ligne
- Ex : la Banque de France impose l'authentification avec deux canaux pour les paiements en ligne et les contrats de crédit.

Identification

- S'identifier, c'est communiquer une identité préalablement enregistrée, s'authentifier, c'est apporter la preuve de son identité qui peut être vérifiée par le destinataire (une personne ou une machine).

- L'authentification est la condition sine qua none de la sécurité des communications électroniques.

- Or, il n'existe pas de définition juridique hormis celle du Règlement communautaire du 10 mars 2004 : « *la confirmation de l'identité prétendue d'entités ou d'utilisateurs* ».

- Les risques liées à la dénégation des actes juridiques pris par voie électronique, à l'utilisation délictuelle des réseaux, à la diffusion des contenus illicites, à l'escroquerie en ligne etc.

Identité sous forme numérique

- Absence de définition légale.

- le délit d'usurpation d'identité numérique n'existe pas : des textes du code pénal protègent l'identité des personnes liée à l'Etat civil et au nom.

- Réfléxion nationale autour des problématiques de l'e-réputation, de protection des données personnelles, du respect de la vie privée sur Internet.

- Initiatives législatives liées à l'usage des données d'identification et à l'usurpation d'identité (LOPSI II en cours d'adoption).

- **Nouveau dispositif français pour le projet de la Carte Nationale d'Identité Electronique** : La carte d'identité électronique comportant un certificat d'authentification et un certificat pour la signature apporte des garanties nécessaires au développement des transactions en ligne.

Signature technique

- L'introduction de la facture électronique avec utilisation d'une signature avec certificat de serveur (SES en France et SEA dans la directive européenne)

- Le bulletin de paie électronique : article L. 3243-2 du code du travail
  - Accord préalable du salarié
  - Mécanisme de scellement électronique
  - Utilisation d'un coffre-fort électronique

- **La signature ou le scellement** : Exigence de garantie de l'intégrité des données

Signature électronique

- Définition et cadre juridique introduits par la loi du 13 mars 2000 transposant la directive 1999/93/CE du 13 décembre 1999 pour un cadre commun sur les signatures électroniques

- Consécration de la validité juridique des écrits sous forme électronique par la loi du 21 juin 2004

- Un **moyen d'authentification** permettant d'identifier le signataire, de manifester son consentement et de garantir l'intégrité du document

- Signature électronique sécurisée encadrée par le décret en Conseil d'Etat du 30 mars 2001, dont la fiabilité est présumée si on utilise un dispositif sécurisé de création et un certificat électronique qualifié.

Des obligations liées à l'identité numérique

L'incontournable sécurité technique

- Différentes garanties techniques sous forme de signature électronique, des protocoles d'authentification et de chiffrement des flux de données etc.

- Encadrement de l'authentification : contractuel (ex : carte bancaire, CGV des sites de ventes ou de services en ligne)

- Les exigences techniques applicables à la signature électronique : sécurité des composants des outils de création de certificats et de produits, tiers de confiance émetteurs de certificats etc.

- Initiatives européennes et nationales de normalisation: CEN, EESSI et mémento de ANSSI (Agence française de sécurité des SI).

Exemple français

➢ Les dispositions relatives au secteur bancaire répondant au souci de sécuriser l'accès à un compte et de faire face aux menaces de fraude (téléchargement des certificats pour signer des contrats).

➢ Authentification forte imposée aux banques en ligne : nécessité d'assurer la l'identification, la traçabilité et la non-répudiation.

➢ L'identification et la traçabilité des clients sont les deux éléments majeurs de la lutte contre le blanchiment d'argent et le financement du terrorisme.

➢ Les mesures de vérification d'identité mises en place dans le secteur des jeux en ligne, avec un rôle prépondérant des prestataires de services de paiement.

Mise en œuvre juridique internationale
Des règles normatives sur les éléments de base

- **Du fait de sa légitimité, la CNUDCI a un rôle majeur à jouer en matière d'authentification et de signature électroniques.**
- **Des élements de base doivent être encadrés au niveau international :**
  - Authentification : définition et effets juridiques
  - Signature "technique" : fonction de scellement/intégrité des données
  - Datation électronique : intégrité et traçabilité des opérations
  - Signature électronique des personnes morales avec un certificat de serveur
  - Signature électronique avec un certificat éphémère (sans CRL) et valable pour une transaction
  - Les responsabilités dans le cadre d'une Infrastructure à clé publique.

Autres possibilités et moyens connexes

Reconnaissance mutuelle

- Elément clef : considérations relatives aux mesures de sécurité, à la sécurité du stockage des données, aux critères d'acceptation des certifications transfrontières etc.
- La reconnaissance des certificats électroniques au niveau communautaire (l'article 5-2 de la directive 1999/93/CE)
- Commission européenne : Etude CROBIES de 2008-2010 sur l'interopérabilité, dans la certification croisée.
  - Lancement de la révision de la Directive européenne de 1999.
- WebNotarius®: un exemple polonais permettant la vérification et la reconnaissance de la signature électronique et des certificats transfrontières (UE et Russie).

Fédération d'identité

- Utilisation d'un login unique pour accéder aux différents services

- Standarisation à travers les "cercles de confiance" mis en place par des protocoles SAML 2.0 et élaborés par le consortium Liberty Alliance

- Principes de pseudonymisation et de recours à des tiers de confiance

- Les bases juridiques reposent sur des dispositions contractuelles

La labellisation : IDéNum en France

- L'amélioration de la sécurité des infrastructures, des échanges et des données comme un facteur clé de la transition vers un accès direct des citoyens par voie électronique aux autorités administratives

- IdéNum, lancé le 1 février 2010 : un dispositif labellisé permettant une fédération des outils d'authentification et de signature électronique, tout en garantissant un niveau homogène de sécurité et d'interopérabilité

- Des utilisations administratives et commerciales :
  - **Simplification des démarches en ligne et des formalités quotidiennes des administrés et des citoyens.**
  - **Signature des transactions électroniques.**

La labellisation: SuisseID en Suisse

- Combinaison de deux fonctions essentielles: la preuve d'identité électronique et la signature électronique valable juridiquement.

- Des transactions sécurisées peuvent être conclues directement en ligne entre les particuliers et les entreprises, entre les entreprises et entre les citoyens et l'administration.

- Un gain de temps et une garantie de sécurité contribuant au développement de la cyberadministration et de l'économie numérique.

Autres exemples de labellisation

- Le label IDéNum s'inspire des réalisations de différents pays européens :
  - Italie : des certificats sur des cartes à puces proposées par les régions,
  - Autriche : des certificats sur des cartes d'étudiants,
  - Suède : certificats sur des cartes remises à La Poste,
  - Norvège : certificats sur les cartes de la loterie nationale
  - Turquie et pays nordiques : des certificats transférables sur les téléphones mobiles.
- Aux Etats-Unis, plusieurs acteurs majeurs de l'internet (Google, Paypal, Verisign etc.), ont annoncé la formation de l'association **Open Identity Exchange** (OIX), qui vise à distribuer des certificats aux internautes. Plusieurs niveaux de confiance sont envisagés, dont le niveau supérieur peut être comparé à IDéNum. Les certificats seront utilisables dans les secteurs publics et privés.

Merci de votre attention !

Eric A. CAPRIOLI
Avocat à la Cour de Paris
Docteur en droit
e.caprioli@caprioli-avocats.com

Société d'avocats
6 rue Saulnier, 75009 Paris / Tél. 00 33 1 47 70 22 12
9 avenue Henri Matisse, 06200 Nice / Tél. 00 33 4 93 83 31 31
www.caprioli-avocats.com