

L'Internet de confiance au cœur même de la stratégie de La Poste

Jean-Paul Bailly (65),
président du groupe La Poste

Depuis sa création, La Poste est placée au cœur des échanges : échanges de biens, mais aussi échanges de services financiers par exemple.

De par cette position privilégiée, La Poste a rapidement compris les défis spécifiques, et les enjeux, de la révolution numérique, ainsi que la nécessité de concevoir les nouveaux outils et services induits par cette révolution.

La Poste s'est ainsi fixé pour objectif de demeurer l'opérateur de référence du courrier sous toutes ses formes, physique comme numérique. C'est pourquoi La Poste s'est engagée dans le développement de "l'Internet de confiance", et plus largement du marché de la confiance et de la preuve électronique.

CHACUN en convient, la révolution numérique, et la démultiplication des canaux d'échanges qu'elle autorise, aura considérablement facilité la rencontre de l'offre et de la demande. Elle constitue ainsi une formidable opportunité, au sens où elle permet de multiplier les contacts, d'accélérer les flux et de créer de la valeur.

Cependant, ce formidable potentiel ne sera pleinement utilisé que si ces nouveaux canaux ou médias offrent des garanties formelles équivalentes à celles qui protègent aujourd'hui les échanges traditionnels écrits.

Retrouver les vertus du courrier

De tout temps, le courrier a été reconnu comme un échange non répudiable parce que signé, daté et authentifiable de manière certaine.

C'est ce qui fait la force d'un média dont il faut rappeler qu'il fut inventé par Cyrus le Perse, au VI^e siècle... avant notre ère.

Or, il est clair que le "mail" Internet classique est un média qui, aujourd'hui, n'offre pas les mêmes garanties.

Avec la transposition partielle de la directive européenne du 12 décembre 1999 et la loi du 13 mars 2000 la France s'est dotée d'un cadre législatif formel qui autorise enfin la reconnaissance juridique de la preuve et de la signature électroniques. À travers cette avancée législative décisive s'ouvre donc un dispositif technique et juridique qui précise les compétences et responsabilités des acteurs de la "certification électronique", nécessaire à la construction de la preuve électronique, et qui permet la naissance d'un nouveau marché.

La Poste dispose donc désormais du cadre nécessaire lui permettant, tout simplement, de faire son métier ; porter, dans le monde des échanges électroniques, les valeurs qu'elle porte dans le monde des échanges physiques : la proximité et l'accessibilité, bien sûr, mais aussi et surtout la sécurité et la confiance.

Le cas de La Poste, de ce point de vue, est probablement représentatif d'une évolution culturelle majeure bien plus large qui voit les tiers de confiance progressivement faciliter

l'accès à l'ensemble de leurs services et moderniser leurs échanges et relations avec leurs clients.

Construire la chaîne de la confiance

Avec la dématérialisation des flux d'échanges, les entreprises ont besoin d'un cadre de sécurité qui va bien au-delà de la seule signature électronique, et qui englobe notamment des services d'horodatage et de conservation. Aux difficultés purement techniques s'ajoute en outre un frein d'ordre statutaire : à qui puis-je faire confiance pour garantir, auprès de tiers, la validité de mes échanges numériques ?

L'un des principaux enjeux du monde numérique est donc de créer et d'organiser la chaîne et le marché de la confiance, en lui permettant de trouver son équilibre économique.

Ainsi La Poste a d'abord fait ses premiers pas en créant avec Sagem la première autorité française de certification des échanges électroniques, Certinomis.

Grâce à cette expertise technique reconnue, La Poste a pu développer progressivement l'ensemble des services nécessaires au monde des échanges numériques, et notamment un "Cachet électronique de La Poste faisant foi".

Elle offre ainsi aux entreprises l'accès à ses services de preuve électronique, ainsi qu'au cachet électronique, en proposant des interfaces standard, y compris en marque blanche, que La Poste a rendues publiques à cet effet.

Enfin, ayant construit un environnement conforme aux fondements de "l'Internet de confiance", La Poste peut délivrer aujourd'hui des applications représentant ses services et

procédures métiers, comme la lettre recommandée électronique, transposant dans le monde numérique leur valeur juridique.

Cet effort de longue haleine lui permet d'actualiser ainsi les valeurs traditionnelles de confiance de La Poste, en lui permettant de devenir rapidement l'un des futurs tiers garants de référence des échanges formels. Gageons ainsi que bien d'autres tiers de confiance emboîteront le pas de la dématérialisation et que les entreprises sauront s'emparer des nouvelles facilités d'échanges électroniques, certifiés et sécurisés au plan juridique. ■

Du marché de la sécurité au marché de la confiance

Youval Eched et Olivier Argaut (95),
Service de Cachet électronique, DDNS, La Poste

Le développement du commerce électronique repose sur le principe que les échanges électroniques ont une validité équivalente à celle des échanges "physiques".

Suite à la directive européenne du 12 décembre 1999, les pouvoirs publics ont donc créé les conditions juridiques nécessaires, avec les décrets sur la signature électronique¹.

LE MARCHÉ de la preuve électronique, comme celui de l'e-business reste cependant un marché relativement jeune. De nouveaux acteurs (spécialistes de la sécurité, start-up etc.) cherchent encore à s'y positionner, appuyant leur marketing sur leur image technologique et faisant référence aux concepts de la sécurité informatique.

Or, la sécurité n'est pas aisément associable à une image valorisante puisqu'il s'agit, par essence, d'une stratégie défensive de prévention de l'agression.

Elle sera souvent perçue comme un coût, plutôt que comme une perspective de profit. C'est donc un domaine difficile à "marqueter" au-delà du cercle des seuls techniciens.

Les acteurs émergents, dont les discours mélangent les aspects technologiques de la sécurité et les caractéristiques

¹ - Un autre moyen acceptable juridiquement est la convention de preuve telle qu'elle se pratique par exemple pour les échanges EDI. Ceci suppose que les relations d'affaires sont établies sur une longue période. Il ne répond donc pas à toutes les configurations du commerce électronique.

téristiques fonctionnelles de la preuve électronique, entretiennent en outre cette confusion. Ils espèrent ainsi se positionner face à d'autres acteurs ayant fait leurs preuves dans l'économie classique.

Cette confusion peut d'autant plus facilement être entretenue que les standards technologiques mis en œuvre définissent parfois des aspects fonctionnels, par exemple la gestion des clés.

Il convient pourtant d'en appeler, ici, à des principes fondamentaux : les exigences de qualité du marché de la confiance sont liées à la capacité des acteurs à respecter des engagements à très long terme (trente ans, voire davantage pour certaines obligations légales).

Toute confusion contribue dès lors à gêner le décollage du marché de la preuve électronique, et par conséquent, à limiter la croissance des échanges électroniques au sens large.

Créer "l'Internet de confiance", c'est offrir un message de confiance basé sur une approche claire et compréhensible des différents métiers. Et ce message se situe à l'opposé d'une approche technologique de la sécurité.

Ce qui n'empêche pas, bien évidemment, une rigueur totale sur un strict plan technique. Il est à ce titre particulièrement éclairant que l'Afnor ait enfin entrepris de normaliser la preuve électronique comme organe de base du marché de la confiance. Il est en effet clair qu'une standardisation des formats et des usages de preuve, à l'instar de ce qui se fit hier dans l'échange de données électronique (EDI), est de nature à pérenniser les investissements des entreprises dans la dématérialisation des échanges.

Ces travaux ont pour objet d'aider l'ensemble des professionnels – opérateurs d'infrastructures de sécurité, autorités de confiance, tiers de confiance et utilisateurs – à structurer et organiser le marché au-delà des aspects technologiques avec l'optimum de transparence et de règles de jeu connues et construites par tous.



Organisation du marché de la confiance

Après Télé-TVA et Télé-IR pour la DGI, le développement de la lettre recommandée électronique par La Poste permet aujourd'hui un premier retour d'expérience du marché naissant de la confiance.

La modélisation proposée ci-après a pour objet d'analyser l'organisation du marché de la confiance, de comprendre comment la totalité de ses composantes intervient dans un service public de confiance comme la

lettre recommandée électronique de La Poste et de conclure, enfin, sur les conditions qui faciliteraient la viabilité économique du marché de la confiance.

Principes fondateurs de la création d'un Internet de confiance

La confiance est un capital qui résulte de trois composantes : le statut, l'autorité² et la compétence. Elle est offerte sur le marché par des acteurs qui ont légitimité à fournir les usages



et procédures liés à l'exercice de la confiance. Ce sont les tiers de confiance statutaires.

Les tiers de confiance se dotent des moyens de preuve nécessaires (les "compétences") à leurs engagements et responsabilités de tiers garant en s'appuyant sur la "chaîne de la confiance" (voir schéma).

À l'instar de ce qui existe dans l'économie physique, un tiers garant sera reconnu comme tiers de confiance dans le monde électronique si et seulement s'il répond aux conditions cumulatives suivantes :

- il devra disposer statutairement de procédures qui font foi légalement ;
- il devra démontrer sa compétence, c'est-à-dire la capacité à offrir ce service quel qu'en soit le support ;
- enfin, son autorité devra être reconnue et consacrée par l'usage, seul moyen pour ce tiers d'être durablement accepté comme référent sur la procédure pour laquelle il entend faire foi.

De fait, il y a encore relativement peu d'acteurs en mesure aujourd'hui de satisfaire à ces trois exigences. Des alliances sont donc probables à court terme, avec l'objectif pour certains d'entre eux de compléter leur dispositif de services de tiers de confiance, en s'appuyant, par exemple, sur des prestataires ou opérateurs capables de délivrer la "compétence" dans les canaux électroniques.

Rôle de chacun des acteurs dans la chaîne de la confiance

L'ensemble des acteurs présentés ci-dessous sont liés dans une chaîne contractuelle continue au sein de laquelle chaque acteur est pleinement responsable du niveau de service qu'il représente dans la chaîne.

L'utilisateur final contracte pour un service de confiance global (par exemple une téléprocédure) auprès du tiers de confiance ayant délégation pour l'exercice de cette procédure.

1^{er} niveau : les équipementiers

Les équipementiers fournissent le matériel technique nécessaire à la mise en œuvre des infrastructures de confiance.

2^e niveau : les opérateurs d'infrastructures de confiance

Les opérateurs mettent en œuvre et exploitent les infrastructures de confiance. Ils sont garants de la continuité et de la qualité technique du service offert (listes de révocation des certificats, archivages éventuels des certificats, etc.). Ils fabriquent aussi les produits dont les tiers certificateurs ont besoin.

3^e niveau : les tiers certificateurs

Les tiers certificateurs constituent le back-office des services de confiance : il s'agit d'autorités de certification, d'archivage, d'enregistrement ou encore d'horodatage. Ils prennent donc la responsabilité de la bonne fin de la procédure pour laquelle ils sont établis en autorité, en conformité avec "l'état de l'art" du domaine d'expertise considéré.

Les autorités de certification sont, par exemple, responsables des procédures de délivrance de certificats. Elles doivent être ainsi en mesure d'effectuer des contrôles correspondant aux garanties offertes (contrôle d'identité en face à face par exemple). Elles se portent garantes de l'identité des porteurs de certificats et de la validité des certificats utilisés, en conformité avec la politique de certification qui les engage.

4^e niveau : les tiers de confiance

Les tiers de confiance sont, de par leur statut, leur autorité et leur compétence à même de proposer des services de confiance ("faisant foi") qui utilisent les infrastructures et certificats délivrés par les tiers certificateurs. Ils peuvent s'appuyer sur une ou plusieurs autorités qu'ils agréent, afin d'assurer un usage valide et contrôlé de la signature électronique pour leurs besoins applicatifs, garantissant ainsi la validité et l'identification du signataire de téléprocédures.

Premiers retours d'expérience...

Créer un langage unique

Une démarche est actuellement en cours auprès de l'ensemble des acteurs de l'Internet de confiance pour clari-

fier le marché et standardiser la chaîne de la confiance, sur la seule base de procédures de contrôles et d'un vocabulaire unique.

La construction de la chaîne de la confiance ne pourra en effet aboutir si les acteurs ne se dotent pas d'un schéma de contrôle totalement fiable – un référentiel – qui atteste de la qualité des prestataires présents sur le marché. Ce référentiel doit être unique, et présenter bien évidemment une parfaite neutralité vis-à-vis des tiers à certifier. En effet, c'est bien ce référentiel, et les règles qui le composent, qui constitueront le fondement des régulations et garanties de l'Internet de confiance.

L'existence même de ce référentiel unique pourrait être le prix à payer pour que s'installe la confiance en un monde dématérialisé.

Alléger la charge financière reposant sur les tiers certificateurs

Si la création d'un référentiel unique est à l'évidence une condition nécessaire, elle ne suffit pas pour autant à faire du marché de la confiance un marché fluide et profitable, au strict plan économique.

En effet, à la lecture du schéma d'organisation du marché présenté ci-dessus, le lecteur aura compris que les autorités de certification, en tant que back-office ont des difficultés importantes d'accès au marché.

Or, ces "tiers certificateurs"³ doivent non seulement faire face à leurs charges d'opérateur sous-traitant mais également assumer le niveau de responsabilité induit par les textes de lois. Ceux-ci engagent en effet leur responsabilité au regard de la sécurité des transactions pour lesquelles des certificats ont été fournis. Cette responsabilité implique donc des risques financiers importants.

Les pratiques commerciales traditionnelles veulent que la responsabilité d'un service ou d'un produit incombent à son fournisseur. Si celui-ci sous-traite une partie de la réalisation du produit ou du service fourni, il en reste néanmoins entièrement respon-

sable. Pour assurer cette responsabilité, il doit définir et contrôler les niveaux nécessaires et suffisants des prestations qu'il choisit de sous-traiter, afin d'offrir le niveau de qualité attendu au regard de sa prestation finale. Il est dès lors possible de se retourner contre un sous-traitant responsable d'une défaillance qui aurait mis en cause sa responsabilité. Ces pratiques permettent une adaptation des niveaux de prestations et une maîtrise des risques par chaque maillon de la chaîne de valeur.

Dans le cas des tiers certificateurs, il importe probablement de pondérer plus précisément l'étendue de cette responsabilité par rapport à celle des tiers de confiance, afin d'alléger des charges financières trop importantes, liées aux produits d'assurance nécessairement contractés. Des différences d'interprétation de la Directive européenne de décembre 1999 ayant, sur cette question, créé une situation pour le moins disparate entre les États membres, il s'agira là aussi de poser les fondations d'un langage commun.

Les tiers de confiance doivent créer les applications permettant l'usage de la signature électronique

Lieu d'échange privilégié des flux d'affaires, dans un Internet professionnalisé et régulé, le marché de la confiance ou l'Internet de confiance constituent un marché extrêmement prometteur.

Dans ce contexte, la signature électronique et les technologies d'infrastructures à clés publiques (dites PKI) ne constituent dans ce marché qu'un attribut de sécurisation de la preuve électronique.


Les dispositifs des tiers certificateurs ont donc vocation à être intégrés dans les services légitimes des tiers de confiance qui, seuls, leur donnent sens auprès des usagers et clients. En effet, seuls ces services sont capables de générer les usages suffisamment nombreux et fréquents pour pouvoir établir un modèle économique stable et pérenne.

À ce titre, il convient de construire sans délais une économie où les usages dématérialisés proposés par les tiers de confiance viennent s'inscrire comme **le véritable front-office des services de confiance**, dans des conditions permettant le financement des centres de coûts et back-office que constituent les tiers certificateurs.

Il appartient désormais aux tiers de confiance de proposer aux entreprises ces services utiles, reconnus juridiquement, qui engendreront le confort et les économies attendus dans le traitement dématérialisé des contrats, des actes ou encore des relations avec l'administration. Gageons que nous ne manquerons pas ce rendez-vous historique de la modernisation des échanges qu'est l'émergence de l'Internet de confiance et de l'écrit électronique "authentique". ■

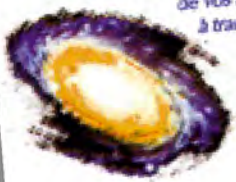
2 - La marque, de ce point de vue, est une représentation de l'autorité.

3 - Ou PSCE.



PARTENARIATS


Nous développons
et nous gérons
les partenariats
de vos activités
à transférer.



ABD

**LANCEMENT
D'ACTIVITES**


Nous valorisons
et nous gérons
vos activités
à transférer.



ABD

**FORCE COMMERCIALE
SUPPLÉMENTAIRE**

Nous valorisons
et vendons vos
compétences
industrielles.



ABD

Ensemble, créons de la valeur économique et sociale.

Votre contact: Hervé MOAL (X78)
147, avenue Charles de Gaulle - 92200 Neuilly sur Seine
Tél. : + 33 (0) 1 46 24 24 36 - Fax: + 33 (0) 1 46 37 19 78
<http://www.abdweb.com>