Publication des Annales des mines avec le concours du Conseil général de l'industrie, de l'énergie et des technologies et de l'École nationale des mines de Paris

N°65 • BIMESTRIEL
JANVIER 2012

La Gazette

DE LA SOCIÉTÉ ET DES TECHNIQUES

« Se défier du ton d'assurance qu'il est si facile de prendre et si dangereux d'écouter »

Charles Coquebert
Journal des mines n°1
Vendémiaire An III (1794)

La signature numérique : Quand les pauvres innovent avant les riches

La signature numérique pourrait être la clé de la protection des identités en ligne. L'adoption de cette technique, proche de celle des cartes à puces, conduirait à des progrès significatifs dans les échanges entre entreprises comme dans la maîtrise et la protection des identités virtuelles. Cependant en France, il y a eu durant les 20 dernières années de nombreuses tentatives de mettre en place un tel système, mais aucune n'a été couronnée de succès. Les expériences similaires menées aux États-Unis et au Royaume-Uni ayant aussi fait long feu, on pourrait croire que cette innovation d'usage ne relève que d'une utopie. Mais en étudiant, dans le cadre d'un mémoire de troisième année du Corps des Mines, les cas de l'Inde et du Portugal, on s'aperçoit qu'il n'en est rien, et que bien au contraire, la signature électronique apporte à ceux qui l'utilisent une grande simplification et sécurisation de la vie administrative. Faut-il être pauvre pour innover ?

Un besoin de la société du numérique

Les dernières décennies ont vu l'explosion des échanges via Internet, si bien que la connaissance mondiale, c'est à dire la quantité d'information stockée par l'ensemble de l'humanité, est passée de 3 milliards de Gigaoctets en 2000 à 24 milliards de Gigaoctets en 2003[1].

Or ces échanges contiennent de plus en plus d'informations personnelles, dont le contrôle échappe de façon croissante aux personnes concernées. Un exemple très célèbre sur Internet est celui de la vidéo du Star Wars Kid. Dans cette séquence de quelques minutes, apparaît un adolescent canadien en train d'imiter un personnage de la célèbre série *Star Wars*. Il y danse avec un ramasse-balles représentant son sabre laser. Cette vidéo a été réalisée en novembre 2002 au studio d'enregistrement du lycée de l'adolescent, et y a été laissée. Ayant été retrouvée l'année suivante, elle a été mise en ligne et est devenue une des vidéos les plus célèbres d'Internet. On estime qu'elle a été regardée 900 millions de fois en 2006[2]. Le jeune homme qui n'osait plus sortir de chez lui a dû quitter son lycée, et sa famille a intenté un procès contre ses camarades de classe pour harcèlement moral.

Par ailleurs, la vie privée des citoyens n'est pas la seule à être mise en difficulté par l'importance croissante des réseaux de communication. Ainsi, les organisations sont de plus en plus vulnérables aux attaques informatiques. Les pirates tirent profit d'informations bancaires récupérées en usurpant l'identité de citoyens, ou en piratant les bases de données commerciales de certaines sociétés. Les attaques, plus nombreuses sur les serveurs des gouvernements ou des grandes entreprises, font craindre l'espionnage politique et industriel. La possibilité de créer de réels dommages à des installations critiques a été illustrée par l'attaque de l'équipement d'enrichissement d'uranium iranien du complexe de Natanz, qui a été mis hors d'usage pendant plusieurs mois par le virus StuxNet[3]. Ce virus, ciblant les logiciels de contrôle des équipements d'enrichissement, était capable de perturber le fonctionnement de ces derniers afin de les endommager, tout en continuant de fournir au système de surveillance logiciel des informations falsifiées qui lui laissaient croire au fonctionnement

normal de l'installation. Ce virus a réussi à se propager parce que les documents échangés ne sont pas forcément authentifiés, ce qui autorise l'échange de documents malveillants.

Dans ce contexte, la question de l'authentification numérique est devenue de plus en plus importante au cours de ces dernières décennies, pour protéger la vie privée et défendre les installations critiques.

Aujourd'hui, le mode d'authentification numérique le plus courant en France est l'utilisation d'un simple mot de passe, dont la fiabilité n'est plus aujourd'hui suffisante. En effet, grâce au déploiement des réseaux sociaux, les pirates disposent d'une grande quantité d'informations sur les personnes, qu'ils peuvent utiliser pour usurper une identité afin de récupérer des informations sensibles, ou simplement d'essayer de deviner ces mots de passe.

Or, les moyens techniques pour fournir une identification forte se sont développés et standardisés ces dernières décennies. Il s'agit le plus souvent de l'intégration d'un certificat et d'un composant électronique sûr. Le certificat électronique fondé sur la cryptographie à clef publique fournit un moyen de s'identifier (donner son nom par exemple) et de s'authentifier (prouver que l'on est bien la personne qui porte ce nom). Le composant sûr, de type puce électronique, permet de garantir sa sécurité et son intégrité, et peut être intégré à une variété de supports – carte à puce, clef USB ou téléphone portable par exemple. Ainsi, l'identification et l'authentification utilisent plusieurs facteurs : il faut utiliser quelque chose que l'on sait (son code PIN), mais également quelque chose que l'on possède (un certificat sur une puce électronique). Dans certains cas, on doit également prouver qui l'on est – par exemple lorsque le certificat contient des données biométriques comme une empreinte digitale. L'utilisation de plusieurs facteurs rend l'authentification beaucoup plus sûre que la simple utilisation d'un mot de passe. Les certificats d'identité électroniques permettent donc de s'authentifier et de signer des documents en utilisant la même technologie. C'est pourquoi nous parlerons indifféremment dans la suite de cette note de « certificat d'identité électronique » ou de « signature numérique ».

Cette technologie de la signature numérique a également l'avantage pour les entreprises de permettre de grandes améliorations en termes de dématérialisation. Selon une personne en charge de systèmes d'information à la Bred, la plupart des entreprises commencent à maîtriser la dématérialisation au sein de leur propre organisation, mais le défi qui s'ouvre à elles, dans un contexte de forte sous-traitance, est de gagner en productivité dans leurs échanges avec les différents intervenants externes. Il est aisé de concevoir qu'une grande banque pourrait réaliser d'importantes économies grâce à l'utilisation de la signature numérique pour dématérialiser les contrats et les factures. Cependant, de telles économies ne sont pas réservées aux banques : tout type de métier peut en profiter.

Lafarge Bétons France par exemple pourrait réaliser une économie de l'ordre de 1 million d'hommes x heures par an [4] sur le processus de prise de commande si l'usage de la signature numérique était bien développé parmi ses clients.

Ainsi, la signature numérique rendrait non seulement plus sûrs les échanges virtuels mais améliorerait également la productivité des entreprises.

Les pionniers en France : un enthousiasme éphémère

Du fait des avantages supposés de la signature numérique, de nombreuses entreprises ont essayé de proposer des solutions dans les années 1990.

Par exemple, la Bred Banque Populaire a créé une entité appelée *Click and Trust* chargée d'offrir des solutions de signature numérique, mais les résultats de cette initiative ont été très modestes. Cela peut s'expliquer par le manque de lisibilité des offres de signature numérique, les différentes banques et institutions n'ayant pas réussi à coopérer. Finalement, les seules initiatives qui ont réussi sont celles mises en place dans une situation de quasi monopole, par exemple dans le cadre des relations entre les hypermarchés et leurs sous-traitants.

Étant donné l'échec relatif des initiatives privées, les administrations françaises et européennes ont essayé à leur tour de proposer des solutions d'identité numérique. Au début des années 2000, les institutions françaises et européennes ont mis un grand entrain à construire un cadre juridique permettant la naissance de l'identité numérique. Ainsi, en 1999 est parue la directive européenne CE 99/93 sur la signature numérique, qui a été transposée en droit français en 2000 via la loi 2000-230, qui a été précisée par le Décret 2001-272 de 2001. Puis sont parus entre 2002 et 2004 des textes définissant des procédures de certification de la signature numérique au niveau français et européen [4].

« Pour que la signature numérique devienne une réussite, il faudra qu'elle dépasse le problème de la poule et de l'œuf : les usages peinent à se développer tant qu'il n'y a pas de solution simple et efficace de signature. Et cette solution tarde à apparaître à cause du manque d'implication des potentiels bénéficiaires. »

Ces textes ont permis de définir au niveau européen le concept de « signature numérique » et de « signature numérique avancée ». Cette dernière définition donne à la signature numérique une équivalence juridique avec la signature sur papier sous certaines conditions de fiabilité. Par ailleurs, la directive européenne de 1999 a défini le concept de SSCD (*Secure Signature Creation Devices*) ou dispositifs sécurisés de création de signature, qui donne une valeur juridique à des outils comme des cartes à puce permettant de créer des signatures sécurisées.

La loi française est même allée plus loin en définissant le concept de « signature présumée fiable », qui permet sous certaines conditions techniques et organisationnelles d'inverser la charge de la preuve. Ainsi, en 2004, tout le contexte juridique est en place pour permettre le déploiement de cette innovation tant attendue.

Or, à l'instar de ce qui s'est passé pour les entreprises privées, l'enthousiasme des débuts peine à déboucher sur une solution qui simplifierait la vie des citoyens. En France, aucun prestataire n'a proposé avant 2010 [5] de solution grand public permettant de signer de façon présumée fiable !

Une fois le cadre juridique en place, l'Administration française a souhaité mettre à profit la signature numérique pour simplifier

ses relations avec les citoyens. C'est ainsi que le projet ADELE (ADministration ELEctronique) a été lancé. Il a été doté d'une administration spécifique et d'un budget de 1,8 milliards d'euros répartis sur la période 2004-2007.

Ce projet, qui avait initialement pour but de transformer l'Administration française via un portefeuille de mesures s'appuyant sur l'identité électronique des citoyens, n'a pu être mené complètement à bien. En 2007, il ne générait plus autant d'enthousiasme et d'attention qu'en 2004. L'échec est toutefois relatif puisque cet effort a quand même apporté des mesures comme la télé-déclaration des impôts : en 2008, 50,15% des particuliers français ont déclaré leurs impôts de manière dématérialisée. Cependant, l'apparition d'un guichet unique dématérialisé de l'Administration n'a pas eu lieu, et le certificat électronique introduit pour le paiement des impôts a été retiré depuis.

Nous voyons donc qu'au niveau juridique comme au niveau du projet de modernisation de l'Administration, la signature numérique a commencé par fédérer beaucoup d'enthousiasmes, pour finir par ne plus intéresser grand monde quelques années après. Elle a connu en France trois obstacles principaux :

- la multiplicité des initiatives :

Cela a conduit à un défaut de lisibilité et, par conséquent, à une impossibilité de gérer la communication entre les différents services d'identité.

- des services auto-suffisants :

En France les différents services de l'Administration ne souffrent pas d'un manque de moyens qui les oblige à mettre leurs ressources en commun et à créer ainsi une structure plus efficace : chaque service peut continuer à fonctionner de manière indépendante. C'est ainsi que le projet ADELE s'est arrêté à la dématérialisation des impôts, faute de pouvoir mettre en place une clé unique d'accès aux services de l'Administration.

- la peur de la surveillance :

Enfin, il n'y a pas de plébiscite de la part de la population qui redoute que l'Administration ait un accès centralisé à toutes les démarches effectuées par les citoyens, surtout si la signature numérique est couplée à des moyens de biométrie (si les empreintes digitales servaient d'authentification à la signature). Cette thèse est reprise par de nombreux activistes d'Internet.

Ainsi, après plusieurs tentatives et plusieurs vagues d'enthousiasme, la France n'a toujours pas de moyen simple de gestion de la citoyenneté en ligne.

Cet échec n'est cependant pas exceptionnel : de grands pays comme les États-Unis ou le Royaume-Uni n'ont pas non plus de dispositif cohérent de signature numérique.

Les succès de la signature numérique en Inde et au Portugal

La signature numérique ne serait-elle donc qu'une belle idée dont les freins à la mise en place sont trop importants ?

En fait, si l'on regarde par delà nos frontières, elle est un succès mondial, comme nous allons le voir avec les exemples de l'Inde et du Portugal.

Le décollage économique de l'Inde, qui a généré en 2007 un PIB par habitant de 950 $, laisse à la traîne des millions de personnes. Ainsi, les études de tendance de croissance montrent qu'en 2015 28,5% de la population indienne vivra probablement encore avec moins de 1 UD$ par jour[6]. Pour ces millions d'Indiens, l'accès aux services administratifs et financiers modernes est très difficile : prêts bancaires, livrets d'épargne, assurances, etc. Or, 60 000 villes de plus de 2 000 habitants n'ont aucun établissement bancaire[7].

En 2009, sur la quasi-totalité du territoire indien, moins de 30 % de la population a accès à des services bancaires. Cette injustice est d'autant plus criante que c'est le plus souvent pour les personnes les plus pauvres qu'emprunter ou envoyer de l'argent à sa famille coûte le plus cher. Or, pour que les plus pauvres puissent avoir accès à des services bancaires de qualité, il suffirait que l'ensemble de la population indienne puisse avoir un moyen fiable de s'authentifier sur Internet, ces services étant faciles à dématérialiser.

L'exemple des services bancaires n'est pas isolé : l'accès à de nombreux services tels que le vote, les prêts à la consommation ou le permis de conduire nécessite d'avoir de nombreux papiers d'identité. Ce marché de l'identité organisé en silos est particulièrement défavorable aux plus pauvres qui bien souvent ne détiennent aucun document administratif et ne disposent pas de l'argent nécessaire pour en obtenir.

C'est dans ce contexte que le gouvernement indien a décidé en février 2009 de lancer une opération de grande ampleur pour donner à chaque citoyen une carte à puce contenant un numéro d'identification unique, stocké dans une grande base de données centralisée au niveau du pays. Cette opération a été lancée avec le plus grand optimisme : le nom du projet est « AADHAR », ce qui signifie « support » ou « fondation » en hindi. Cette carte, qui est actuellement distribuée à grande échelle, servira à la fois de carte bancaire, de carte d'identité, de carte de vote et de permis de conduire : elle sera en quelque sorte la carte intégrée du citoyen. Ce projet, qui a bénéficié d'un budget de 669 millions de dollars en 2010, a pour objectif d'équiper 600 millions d'individus en 4 ans. Comme l'a dit Nandan Nilekani, directeur de UIDAI

(Unique Identification Authority of India – autorité indienne en charge du deploiement de la carte d'identité électronique) : « *This isn't just about giving every Indian a number, it's about giving them an identity and an acknowledgement of their existence by the state. That has huge social benefits*[8] ».

Aujourd'hui, malgré des craintes sur la protection des données personnelles, 100 millions de personnes sont équipées de la carte d'identité électronique et la liste d'attente est de plusieurs dizaines de jours[9].

Cette urgence de permettre un accès simplifié et économique des citoyens aux administrations n'apparaît pas seulement dans les pays émergents comme l'Inde. Ainsi le Portugal, confronté à de sévères restrictions budgétaires, a également mis en place un système permettant d'améliorer le service rendu par l'Administration aux citoyens tout en maîtrisant mieux ses dépenses et en réalisant des économies de fonctionnement. Aujourd'hui, l'Administration de ce pays utilise une simple carte dotée d'une signature numérique pour gérer la carte d'identité, les impôts, le vote, la sécurité sociale et l'assurance maladie. Par ailleurs, comme en 2007 seuls 35 % des Portugais avaient accès à Internet depuis chez eux, des « supermarchés du citoyen » ont été mis en place, qui permettent notamment de se connecter aux services de l'Administration via un automate similaire à un distributeur de billets.

On voit donc que la signature numérique, qui a été jusqu'à présent très difficile à mettre en place par les administrations les plus riches, a été largement déployée dans d'autres pays, notamment quand ils devaient faire face à un manque de moyens d'authentification, s'il y avait une crise budgétaire à relever, ou si l'Administration était face à une population peu contestataire.

On peut classer ainsi les pays qui ont mis en place des solutions de signature numérique :

	Pays à fortes ressources	Pays à faibles ressources
Pays où l'administration dispose d'une grande confiance de sa population		Inde, Estonie, Malaisie, Portugal
Pays où l'administration dispose d'une faible confiance de sa population	Belgique, Allemagne, Emirats Arabes Unis, Italie, Suisse, Autriche, Suède, Finlande	Iran, Pakistan, Maroc, Turquie

Il est particulièrement frappant de constater que les pays qui étaient a priori dans la situation la plus favorable sont en fait ceux qui ont le moins recouru à cette innovation.

Quel avenir en France ?

En France, il semble que le besoin de signature numérique soit moins pressant. Cependant, l'augmentation des cas de piratage posera inévitablement de graves problèmes de sécurité individuels et nationaux (par exemple le risque de piratage d'un réseau de distribution d'électricité, d'un hôpital, etc.) si une technologie d'authentification sûre n'est pas largement diffusée. Or, contrairement à la fin des années 1990, les citoyens sont aujourd'hui beaucoup plus familiarisés aux technologies de la communication et sont devenus plus sensibles aux questions de vie privée. C'est dans ce cadre que les autorités françaises étudient actuellement deux projets de signature numérique : une carte d'identité dotée d'une puce permettant de gérer une signature numérique, et un label certifié par un organe d'État (IdéNum) d'offre de signature numérique. À ce stade, il semble que les deux projets ne seront pas compatibles.

Ces deux démarches, qui ont été lancées officiellement lors de la conférence de presse du 31 mai 2011 du Ministre chargé de l'Industrie, de l'Energie et de l'Economie numérique montrent la volonté de la France de proposer un tel service, malgré une certaine indécision sur la démarche à adopter.

En effet, pour que la signature numérique devienne une réussite, il faudra qu'elle dépasse le « problème de la poule et de l'œuf », qui fait que les usages peinent à se développer tant qu'il n'y a pas de solution simple et efficace de signature. Et cette solution tarde à apparaître à cause du manque d'implication des bénéficiaires potentiels.

Cette indécision nous amène à nous demander si cette solution ne se développera en France qu'à la suite d'une crise majeure : par exemple, un fort besoin d'économies au sein de l'Administration ou une attaque très sérieuse sur des systèmes peu sécurisés...

Matthieu Mangion, ingénieur des mines

NOTE

[1] Barrot, Jacques, 28 novembre 2001, *Rapport d'information déposé en application de l'article 146 du Règlement par la Commission des Finances, de l'économie générale et du plan (1) sur la formation professionnelle en Suède*, Paris, Assemblée Nationale, 33 pages. http://www.assemblee-nationale.fr/legislatures/11/pdf/rap-info/i3420.pdf

[2] Solove, Dan, 24 Octobre 2007, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*, Yale, Yale University Press, 256 pages

[3] Malware Aimed at Iran Hit Five Sites, Report Says, *New-York Times*, http://www.nytimes.com/2011/02/13/science/13stuxnet.html

[4] *La signature numérique : Quand les richesses n'apportent pas le bonheur*, mémoire de Matthieu Mangion et Maël Primet, septembre 2011, publication École des mines

[5] Communiques-presse-online.com, 06-12-2010, « Morpho et Dictao présentent la première solution de signature électronique présumée fiable par empreinte digitale », *communiques-presse-online.com*, http://www.communiques-presse-online.com/informatique-réseaux-télécoms-c6/morpho-et-dictao-presentent-la-premire-solution-de-signature-electronique-presumee-fiable-par-empreinte-digitale-au-salon-cartes-et-identification-2010-a4728.html

[6] Boillot, Jean-Joseph, mars 2004, « Économie Indienne perspectives 2020-2050 », *Mission Économique Asie du Sud*, 32 pages, http://www.cepii.fr/francgraph/communications/pdf/2004/050304Inde.pdf

[7] Unique Identification Authority of India, Avril 2010, *From Exclusion to Inclusion with Micropayments*, http://www.uidai.gov.in/UID_PDF/Front_Page_Articles/Strategy/Exclusion_to_Inclusion_with_Micropayments.pdf

[8] Gemalto, Automne 2010, « Ancient and modern », *The Review*, 38 pages, http://www.gemalto.com/brochures/download/review_nov10/index.htm#1

[9] Daily News and Analysis, 30/09/2011, « UIDAI paints a rosy picture on first anniversary of Aadhaar project », http://www.dnaindia.com/bangalore/report_uidai-paints-a-rosy-picture-on-first-anniversary-of-aadhaar-project_1593426

La *Gazette de la Société et des Techniques* a pour ambition de faire connaître des travaux qui peuvent éclairer l'opinion, sans prendre parti dans les débats politiques et sans être l'expression d'un point de vue officiel. Elle est diffusée par abonnements gratuits. Vous pouvez en demander des exemplaires ou suggérer des noms de personnes que vous estimez bon d'abonner.

Vous pouvez consulter tous les numéros sur le web à l'adresse :
http://www.annales.org/gazette.html

RENSEIGNEMENTS ADMINISTRATIFS
Dépôt légal janvier 2012

La Gazette de la Société et des techniques
est éditée par les *Annales des mines*,
120, rue de Bercy - télédoc 797 - 75012 Paris
http://www.annales.org/gazette.html
Tél. : 01 42 79 40 84
Fax : 01 43 21 56 84 - mél : michel.berry@ensmp.fr
N° ISSN 1621-2231.
Directeur de la publication : Pierre Couveinhes
Rédacteur en chef : Michel Berry
Illustrations : Véronique Deiss
Réalisation : PAO - SG - SEP 2 C
Impression : France repro

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE DES FINANCES ET DE L'INDUSTRIE