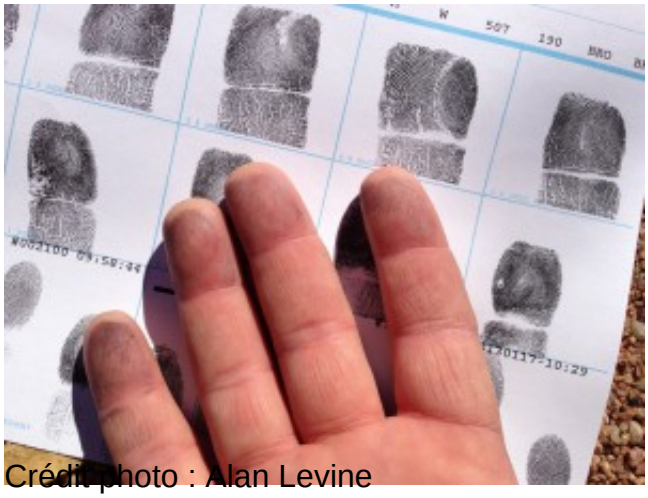
Consultation sur l'identité numérique



Crédit photo : Alan Levine

Je palabrais il y a peu à propos de l'identité numérique. Et PAF, voilà que notre premier ministre nous pond une consultation sur le sujet (site d'origine ici). J'ai donc joyeusement sauté à pied joints dedans. Je dois avouer que j'ai trouvé le document extrêmement pertinent même si on sent très vite poindre le spectre de la centralisation si chère à la France.

Réflexion 1 : Déléguer la gestion de l'identité, y compris régalienne, à une entreprise privée serait une solution qui engendrerait une perte générale de l'identité. Une sorte de privatisation du soi. Outre l'impact sociétal, l'économique serait, quant à lui, probablement très élevé pour la société. Il est cependant nécessaire de trouver un « juste milieu » qui n'en serait probablement pas un.

Réflexion 2 : S'il est indéniable que l'état doit avoir son rôle régalien à jouer, la création d'une N-ème plateforme d'identification n'a que peu de chance d'aboutir, surtout s'il n'ouvre accès, au début, qu'aux services publics. Il est nécessaire que l'action de l'état s'inscrive dans un périmètre plus global dans lequel la sphère privée et les entreprises pourront également intervenir.

Réflexion 3 : Il n'est pas pertinent de chercher à réunir toutes les authentifications, ne serait-ce que parce que certains voudront garder une barrière hermétique entre leurs identités en ligne. Le problème du mot de passe réutilisé à outrance est principalement un problème culturel et d'éducation. Il devrait être abordé à l'école. De nombreux outils existent pour conserver un porte clé de mots de passe à l'abri de toute intervention d'entreprise privée ou d'un quelconque autre tiers.

Réflexion 4 : Les contraintes de séparations strictes des bases de données instaurées en 1978 par la CNIL sont capitales pour assurer les libertés individuelles. Une trop grande centralisation des capacités d'identification doit continuer à être considérée comme néfaste. Cependant, pour certaines administrations bien précises, une simplification pourrait être envisagée par l'usage du numéro le plus répandu et connu de tous : celui de la sécurité sociale.

Réflexion 5 : La carte d'identité numérique repose sur un pari extrêmement risqué à long terme. Celle-ci reposerait, comme le passeport biométrique, sur une base de données centrale qui risquerait une fuite plus ou moins importante à un moment ou à un autre. Quoi de pire, pour protéger des objets, que tous les enfermer au même endroit en comptant uniquement sur la protection de l'endroit ? Chacun doit être libre de choisir où et comment ses données personnelles, y compris celles servant à l'identifier, doivent être conservées et protégées. En ce sens, l'entrepôt personnel est séduisant, mais uniquement s'il n'est pas situé au même endroit que l'entrepôt de l'autre.

Réflexion 6 : la dématérialisation des formulaires est bien souvent vue sous un angle simpliste consistant à mettre à disposition un fichier PDF qui, une fois sur deux, ne peut être rempli en ligne et doit, presque toujours, être imprimé. Elle doit être poussée plus avant en suivant l'exemple de la déclaration IRPP qui ne se base plus sur le principe du formulaire (même si la présentation est volontairement très proche de celle du formulaire papier). Dans cette optique, l'identification à partir d'un entrepot de donnée permettant de pré-remplir, selon le choix de l'utilisateur, les champs les plus traditionnels, semble être la bonne voie.

Réflexion 7 : L'informatique permet, quasiment depuis ses débuts, de définir des rôles et des droits différents pour un même individu. Dans un système informatique, un individu fait partie d'un ou plusieurs groupes ayant un ou plusieurs droits, parfois des droits différents sur des groupes différents. L'application de ce principe à l'identité numérique ne présente pas de difficulté particulière, par exemple sur le cas de l'assuré social pouvant gérer le compte de ses ayants droits mais uniquement à son propre dossier médical.

Réflexion 8, 9 et 10 : l'identification des agents de l'état pourrait reposer sur un socle commun d'identification centralisée par un moyen quelconque (carte à puce, par exemple), mais là encore, centralisation et socle commun signifient compromission potentielle à grande échelle et forte dépendance à un organe unique. En poussant la réflexion plus loin, la problématique est la même dans le monde de l'entreprise et un principe commun réglerait beaucoup de problèmes plutôt que de rechercher des socles communs à chaque famille (état, collectivité, entreprise, particulier…).

Réflexion 11 : là encore, la centralisation est l'ennemi de l'efficacité et de la sécurité. Vouloir à tout prix réduire le nombre de canaux sécurisés est une mauvaise idée. Il faut au contraire encourager diversité et multiplicité. Ce qui n'interdit pas à l'état de recommander quelques principes de base permettant d'assurer une sécurité convenable, sans pour autant agir comme un intermédiaire dans les dialogues M2M ne le concernant pas.

L'ensemble de ces réflexions fait remonter plusieurs axes forts :

- L'état doit continuer d'exercer ses fonctions régaliennes certifiant l'identité dite « réelle » dans les mondes numériques
- D'autres services, dans le monde de l'entreprise et même personnels, doivent pouvoir bénéficier des fruits de cette réflexion
- La simplicité d'utilisation doit être au moins égale à la sécurité réellement mise en oeuvre, sous peine de tuer le dispositif avant sa naissance

- Chacun doit être libre de choisir ce qui peut être fait et par qui en ce qui concerne ses données d'identification
- La sécurité absolue est une chimère

La page 7 du document donne une bonne vue sur l'histoire de l'identité en générale, d'abord gérée de grée à grée puis gérée par l'état pour son propre compte et pour accompagner ce qu'on pourrait regrouper sous le nom de mondialisation. En effet, à l'époque, il était impossible de se référer à un voisin ou à l'ami d'un inconnu pour certifier son identité, qui plus est si ces personnes n'étaient pas présentes.

Comme indiqué à la page suivante, les mondes numériques apportent leur lot de bouleversement. L'un d'entre eux permet à présent de pouvoir s'en référer à n'importe qui, n'importe quand pour n'importe quoi, en s'assurant, relativement simplement et avec une fiabilité bien souvent suffisante, que la personne qui est en face existe réellement.

Les systèmes de certificats numériques et du chiffrement asymétrique permettent depuis longtemps d'échanger de façon sécurisée des messages (protection du contenu du message contre les regards indiscrets ET authentification assurée de l'émetteur). Ils permettent également de bâtir un réseau de confiance, chacune des identités existantes pouvant être certifiée par d'autres.

Ces principes, appliqués sur les réseaux à de très nombreux niveaux, constituent une solution élégante, correspondante à tous les prérequis, pour la gestion de l'identité numérique :

- Acentralisation
- Mission régalienne de l'état
- Simplicité d'utilisation
- Ouverture globale aux entreprises, particuliers et même autres états

Scénario général :

1. Jean Kévin lance son logiciel « mon identité » pour la première fois. Une paire de clé va être générée et le logiciel va proposer à Jean Kevin de protéger sa clé privée par un mot de passe et de la sauvegarder sur une clé USB « au cas où ».
2. Jean Kévin va faire le tour de tous ses amis qui vont signer sa clé, certifiants l'un après l'autre que NON, Jean Kévin n'est pas Jean Michel. L'identité de Jean Kévin en sera renforcée dans le sens où ces sigatures seront toutes publiques.
3. Jean Kévin va ensuite vouloir consulter son dossier médical en ligne. Le site de l'assurance maladie va l'informer que le lien n'a pas pu être fait entre son identité numérique et son compte d'assuré social et va l'inviter à saisir son numéro de sécurité sociale.
4. Après la saisie, le site l'informera que son identité n'est pas reconnue par l'état et qu'il serait de bon ton de la faire certifier.
5. Rendu dans sa préfecture locale avec sa clé publique, Jean Kevin obtiendra la signature de l'état, certifiant qu'il est bien civilement Jean Kevin.

Dès lors, le site de l'assurance maladie lui ouvrira ses portes, mais aussi celui des impôts, et de manière plus générale, tout site administratif qui n'aura pas besoin d'autres informations d'identification que son état civil qui aura été validé par l'état. Pour des questions pratiques, il peut être pertinent de faire en sorte que la globalité de ces fonctionnalités soit embarquée dans une carte à puce, une clé informatique ou tout autre périphérique portable permettant une utilisation en tous lieux et en tous temps.

Libre à chacun de fixer le niveau de confiance requis pour « utiliser l'identité ». Un réseau social en ligne pourra par exemple n'exiger aucune signature de la clé du porteur alors que la validation d'une déclaration d'impôt demandera, à minima, la signature de l'état. Libre à chacun également de créer autant de clés que d'avatars numériques, et de s'en servir à loisir.

Lorsqu'une identité est compromise (perte de la clé privée, par exemple), les signatures peuvent être révoquées par le signataire, rendant la clé inutile (soupçon de fraude par l'état, par exemple), ou bien la clé toute entière peut être révoquée par le porteur (à supposer que la clé de révocation soit disponible et simple d'usage).

Le maniement d'une paire de clés de chiffrement n'est actuellement pas aisé. En attendant la démocratisation de ce genre de principe (tant côté logiciel & technique que côté culture & usage), et pour permettre l'usage par le plus grand nombre, il est possible d'envisager le déport complet de la clé et des informations qu'elle protège sur ce qui était qualifié d'entrepôt personnel de données. Multiplicité et diversité sont donc assurés. Par ailleurs, un tel entrepôt doit être envisagé pour la gestion des clés de révocation, permettant aux personnes de faire révoquer leur clé par un tiers de confiance.

Le principe de fonctionnement sous- jacent étant le même, et même si un tel dépôt géré par l'état aurait, pour des raisons de confiance, tout son sens, d'autres acteurs peuvent fleurir sur ce secteur, à la condition indispensable d'être certifiés et audités régulièrement. Multiplicité et diversité sont ainsi assurés en attendant de pouvoir reproduire, dans les mondes numériques, ce qu'est la CNI aujourd'hui.

Les usages sont ensuite virtuellement illimités :

- certification de son identité lors de ses relations avec l'administration (l'état signe la clé)
- authentification sur le système d'information de l'entreprise (l'employeur signe la clé)
- accès à l'ordinateur familial et/ou déverrouillage d'un trousseau de mots de passe divers pour l'accès au site ne proposant pas l'authentification par certificats (clé autosignée)
- validation de paiement chez un commerçant, en boutique ou sur internet (la banque signe la clé après avoir exigé la signature de l'état)

Mais aussi, avec quelques adaptations du principe de base des clés asymétriques :

- Pouvoir rentrer dans sa maison équipée d'une serrure numérique, et permettre, depuis son bureau, à l'amie de sa fille d'ouvrir la porte quand cette dernière à « oublié sa

clé ». (la clé de l'amie est apprise par la maison, sur demande d'un des deux parents)
- Interdire l'accès à un lieu (privé ou public) à certaines personnes sans avoir à vérifier les cartes d'identité et les comparer à une liste noire et sans stocker l'ensemble des données concernant les personnes acceptées (on se borne à vérifier que la clé présentée par le visiteur contient un nombre de signatures assez satisfaisante pour être considérée comme valide et on vérifie quelle ne se trouve pas sur liste noire). Ou inversement : autoriser l'accès à une liste précise de personnes, à l'entrée d'un concert par exemple (à l'occasion de l'achat d'un billet, la clé de la personne est signée par l'une des clés de l'organisateur du concert)
- Pouvoir prouver qu'on a effectué une action (A vend un objet à B, B confie l'argent à C, C « signe un reçu à B » que A peut consulter, A envoie l'objet via le transporteur D, qui lui « signe un reçu » que C peut consulter, C paie A avec le montant confié par B. Cet exemple n'est d'aucune utilité si on considère que les monnaies acentrées sont l'avenir)
- …

Trois obstacles majeurs se dressent toutefois face à ce principe :

- Il n'est que peu porteur d'emploi dans le sens où il n'y a aucune sécurité d'un système central à assurer. Les seuls acteurs qui pourront gagner de l'argent seront les concepteurs de matériels innovants permettant de gérer son identité et, dans une certaine mesure, les concepteurs de logiciels (pour l'utilisateur et pour les entités qui devront gérer beaucoup de signatures/vérifications)
- L'acentralisation technologique née d'internet est encore vue par beaucoup comme une utopie irréaliste, ce qui freine très largement son développement
- Il nécessite une éducation dès le plus jeune âge à la notion d'identité numérique. Mais ce n'est finalement qu'une nécessité quelle que soit la voie qui sera empruntée.

Education, acentralisation, confiance : voilà mes idées au sujet de l'identité numérique.