Identité numérique

Crédit photo : dallesmeets

Comment s'assurer à la fois que je suis qui je dis être et que je ne dis pas, à côté, que je suis un autre ? Exprimé autrement, comment assurer l'unicité et la certification de l'identité des habitants des mondes numériques ?

Dans l'autre monde, à votre naissance, vos parents vous donnent un (ou plusieurs) prénom(s) et l'associent à leur propre nom. L'administration couple ensuite ces deux informations à vos date et lieu de naissance. Ce quadriptique certifié par l'administration est censé remplir ce rôle. Dans la vraie vie, chacun sait que ça ne marche que si vous êtes de bonne foi et que l'agent administratif chargé de votre dossier a fait attention. En bref, même si ce n'est pas trivial, se créer une seconde identité est parfaitement faisable.

Et ça pose plein de soucis, pas seulement parce que des terroristes se baladent avec un faux passeport ou parce que les bien pensants ne comprennent pas que l'anonymat de Maitre Eolas, ce sont justement ses nom & prénom(s) civils.

Heureusement, l'informatique va aider ! Sisi. Il suffit de mettre une carte à puce dans une carte d'identité et la coupler à une base de donnée centrale qui sera infaillible. Sisi. Puisqu'on vous le dit. Si on sait pas le faire avec un bout de carton enfermé dans du plastique, ajouter du silicium dedans va nécessairement régler le problème.

Dans mon monde, ce que je suis est majoritairement dicté par l'autre. Nous nous définissons par nos relations avec autrui. Pour ma famille, mes clients et quelques autres, soit quelques 2 ou 300 personnes, je suis, par convention sociale, Bruno. Pour vous, lecteurs de ce blog qui ne me connaissent pas outre mesure, je suis Bruno à tendance Turblog. Pour les gens des univers du réseau j'ai (presque) toujours été Spyou.

Trois identités, si on regarde bien, donc. Mais ces trois identités renvoient inévitablement à moi. Sans aucune équivoque possible. De nombreuses personnes peuvent en témoigner et de nombreuses passerelles existent, permettant, si on se donne la peine de chercher 12 secondes

et demi, de faire le lien.

Et ces trois identités existent parce qu'il y a au moins une personne qui peut attester que je suis connu sous chacun de ces noms.

Revenons-en au silicium dans la carte d'identité. Que va-t-il nous apporter de concret ? Pas grand chose si ce n'est une facilité numérique de vérifier les informations inscrites physiquement sur la carte par le truchement d'une base de donnée déportée et supposée infaillible. Sauf que si le formulaire administratif qui a servi à la renseigner était bidonné, elle sera tout autant bidonnée. Le risque de fuite de données de la base centrale, c'est le cadeau bonux. Moralité, de quoi gagner un temps infinitésimal au prix d'un risque qui semble hypothétique mais qui, comme les accident nucléaires, sera gravissime quand il arrivera. Et il arrivera.

Alors comment résoudre ce problème lié à la centralisation ? En reprenant la base de ce qu'est l'identité : je suis qui je suis parce que l'autre dit que je le suis. Et si beaucoup de ces autres le disent, mon identité n'en est que renforcée. Et si une personne dit que je ne suis pas cette personne, doute il peut y avoir.

Et sacrée chance, l'informatique d'aujourd'hui nous offre déjà les outils pour la certification de pair à pair. C'est même utilisé depuis la nuit des temps pour s'échanger des emails de façon sécurisée :

- Je me crée une clé personnelle à laquelle j'associe mon adresse email et ce que je considère être mon identité
- Je vais voir Tatie Martine et je lui demande de certifier que je suis bien qui je suis. Techniquement, elle va utiliser sa propre clé pour signer la mienne
- Tout un chacun peut savoir que Tatie Martine a proclamé que j'étais bien qui je dis être
- Si vous avez confiance en Tatie Martine, cela peut vous suffire pour avoir la certitude que je suis bien qui je prétends être.
- Plus des gens vont certifier que je suis moi, plus mes propres certifications pourraient avoir du poids, un peu comme le principe du pagerank de google.

  C'est bien joli, mais ça ne fonctionnera jamais en vrai, et puis moi, je suis un asocial qui ne connaît personne, je suis donc exclu de ce système.

Oui mais non. L'état peut avantageusement participer au système. On peut par exemple imaginer que chacun signe la clé de monsieur le Maire pour asseoir la légitimité de son identité numérique et que ces mêmes maires signent la clé de l'état qui, à son tour, signera la clé de qui souhaitera être certifié « old school » avec vérification de l'acte de naissance et compagnie.

Quant à l'adoption du principe par la majorité des populations, il manque uniquement l'outil pratique et sexy associé à l'usage que tout le monde attend. Un porte clé qu'on peut passer devant l'écran de son smartphone pour se connecter sur twitter ?

> Bon, ok, admettons que ça fonctionne à grande échelle et pas que pour le mail mais mettons… Pour voter pour le prochain président. Qu'est-ce qui m'empêche de créer un réseau commun de certification de fausses identités avec 200 petits cons comme moi, le tout au nez et à la barbe de l'état, pour voter X fois avec X identités ?

C'est une chouette idée, ça ! Un bon cas concret d'usage de la chose. Dans l'absolu, rien n'empêche, comme n'importe quelle élection, de tenter de tricher. Mais si vous faites ça avec 200 personnes, ça se saura, et le premier qui brisera la fausse chaîne de confiance fera tomber tout le château de cartes. Et puis peut- être qu'il faudra imposer la signature de l'état pour avoir le droit de voter aux élections nationales, ce qui nous remettrait dans l'exacte situation actuelle concernant les faussaires.

Exacte situation, pas tout à fait, car s'il est aujourd'hui possible de créer un faux passeport et de bananer l'état, il est beaucoup plus difficile de se construire une fausse vie sociale dans laquelle j'aurais de vrais gens prêts à témoigner publiquement que je suis Franck L. sans que personne n'ouvre sa gueule pour dire que non, je ne suis pas Franck L. mais Bruno.

En bref, pas quelque chose de 100% infaillible non plus, mais quelque chose d'utilisable par n'importe qui, qui n'est pas centralisé et qui offre des tas de perspectives, par exemple :

- une boutique pourrait proposer un prix réduit automatiquement aux personnes recommandées par des clients préexistants sans avoir à gérer des bons de réduction ou des codes cadeaux
- je pourrais entrer au bureau, au datacenter ou chez moi avec ma clé numérique sans aucun besoin d'un dispositif central, simplement parce que les serrures pourront vérifier la chaîne de confiance qui correspond à la clé que je porte sur moi (et probablement la clé elle-même) sans besoin d'une base centralisée
- on pourrait même prévoir des signatures de différents types, l'un de ces types serait le vote, permettant de signer la clé d'un candidat à la présidence, et l'élu serait celui qui a obtenu le plus de signature-vote. Un soupçon de théorie mathématique illustrée dans les bitcoins/zerocoins permettra même d'assurer l'unicité et l'anonymat du vote.

Mais j'ai peur que les lobbys de l'identité numérique conseillent à nos énarques d'adopter leur solution centralisée. Ce serait tout de même idiot de se tirer une balle dans le pied du porte monnaie. Et puis tous ces trucs informatiques de hippies, ça fait un peu peur.

Après tout, dans leur monde, leur petit confort semble passer souvent avant l'intérêt collectif.