The relational identity

Is our current system highly reliable when it comes to checking a person's identity? In light of current events it seems to be not the most secure or effective, which is alarming considering the impact this has on public safety and in cost to the community.

Although France appears to be in control of the situation, the French borderer and air police intercepts over ten thousand fake documents per year, proving that this remains a major issue. For instance over two million of fake driving license are being used as ID and it seems all too easy for oneself to obtain fraudulent papers. This fall into four main categories:

- Falsification (the fraudster uses a genuine document and changes an element, for example the photo or vital records), this is most common kind of fraud;
- counterfeiting (identical reproduction) ;
- the stealing of printed documents before they reach the administration;
- Identity fraud (using an authentic stolen or lost document, or issued on the basis of false supporting documents).

Most of the time only a simple scanner is needed to forge perfect identity documents, and complete kits including the driving license, health insurance card and residency card can be provided by traffickers to migrants.

One could think that Biometric documents are the answer but they can also fall into the 4th category described above.

Now concerning identity checks, these also are unreliable. Here are some examples to illustrate this matter:

- In France, when entering a court of justice, carrying with you a black gown or showing from afar a lawyer's card, authentic or not, is a sufficient proofs for grads and you shall not be forced to go through security gates
- Receptionists in office buildings or any national administrations are not in the slightest trained to recognize fake documents, even a national identity card.
- And in reality even in a highly protected ministry can the security prevent access to someone if their resemblance with the ID's photo is uncertain? Not really. This raises another important default in this system: in a valid ID the holders picture is often out of date. A 24 year old often doesn't resemble his picture taken when he was 15 in black and white on this ID, so how can we be sure that it is really him?

For the community this is a major issue. Documentary fraud enable all kind of abuse such as obtaining loans thanks to false pay slips, identity thievery, driving without having passed the license or without insurance, car thievery, receiving undue benefits, entering homes of vulnerable people, as well as being necessary for terrorist and organized crime.

It's time to change method. The solution proposed here is called "relational identity" and is based on the testimonies of people who know the document holder and can vouch for him.

Nowadays internet makes this possible. I will hereby show you how this solution can greatly decrease fraud especially the risks related to organized crime and terrorism while respecting fundamental rights in a better way than the sovereign organizations have so far.

For instance it is common knowledge that a large number of data are kept safe in secure servers around the world, and it is possible to prevent from transferring personal data from one database to another without the authorization of the relevant person.

The concept of relational identity is based on the four following rules.

1. The evidence-based identity

   A person's identity is guaranteed by numerous third parties: states, communities, businesses, but especially friends and family members.

   These third parties may also have to produce a certificate of good repute in order to certify that to their knowledge, the person in question has no connection with mafia or terrorist groups.

2. The identity scoring

   An identity is rated based on the number and the quality of testimonies, by a scale developed by an independent jury composed of qualified persons. This may be adapted over the years.

3. The choice by all individuals of the trusted third parties in charge of keeping their identity elements.

   The elements of a person's identity are stored in the cloud, with trusted third parties chosen by the holder and to certain elements by the sovereign authorities (e.g. vital records).

   Once proved that the elements of a database cannot be transferred to another one, we could imagine numerous and diverse elements being stored: vital, addresses, web links, phone numbers, but also diplomas, certificates, bank statements, health information, etc.

   A person may keep personal information in different trusted third parties' databases, depending on their nature. Here are some examples:

   - ✓ vital records, internet addresses, telephone numbers, etc.
   - ✓ health record
   - ✓ contracts of employment, payroll and employment certificates
   - ✓ diplomas
   - ✓ financial and banking information
   - ✓ list of insured properties
   - ✓ etc.

   Trusted third party may then verify the information provided by the holder, and vouch for their accuracy. For example the one chosen in charge of the vital records will verify the authenticity of identity documents provided.

The holder may also choose a partner called "Registrar" in charge of linking the main login user (a nickname or vital elements) with the trusted third parties. It is the Registrar that provides the ID cards with the key enabling the holder to access the ID system.

4. The control of the disclosure of the holder's identity items

   Individuals have one key or a few allowing them to access their identification elements and to enable occasional or permanent access to a third party in order to prove their identity and/or their qualities.

How it works

In practice this would work as follow: to prove their identity or quality, a person would present his or her card which would be read by a free universal identification smartphone application allowing the border police for example to verify if it is indeed the original card.

They would then see on the screen a picture or a short video of the holder, the rating of his identity, as well as other elements necessary. With the same application, protected by a PIN, the card holder will see these requests and allows access to them or not.

If the card is stolen or lost, the card holder may deactivate it immediately via Internet. He then needs the assistance of several of its relations - designated in advance by him - to put another in service. These friends will be questioned via Internet to verify that the holder has warned them of his change the card.

The holder may have multiple cards corresponding to different identity information. For example a card which would only record all his medical details would enable any doctor, with the holder's permission, to have a full picture of his medical background without further research.

Another application could be professional cards: it would automatically show the holder's picture and confirm his function: policeman, fireman, or a registered nurse etc.

Fake documents would then become impossible to make, simply because identity documents would no longer exist. The card is only a key giving access to elements of identity that are stored on secure servers.

The security of this system relies on the integrity of servers and on the certification of the information.

- The integrity of servers on which identity information is stored.

  Some may be managed by states, others by private operators selected by the holder.

- The certification of the information

  All information, depending on its nature, may or should be accompanied by a certification. A degree or certificate must for example be certified by its issuer or by an independent certification authority.

All the technologies necessary to put in place this new system are already available:

- the secure cloud

- cards that are impossible to copy and may be authenticated by smartphone,
- smartphones and applications enabling the secure authentication of cards, including the new version of the IPM application of the World Customs Organization.

So there should be no delay in the creation of this project.

The entities necessary for performing of the main functions also exist:

- the digital service providers likely to play the role of "Registrars", retaining the list of trusted third party retained by each card holder and providing the appropriate link after authentication of a card,
- the trusted third parties,
- the certification companies,
- and above all individuals wishing to receive a free digital ID card.

The financing of this operation is largely insured by a contribution to digital service providers ensuring the functioning, by trusted third parties, by certification companies and by anyone wishing to benefit from the new methods of identity verification and of trustable information acquisition from card holders, or of other information necessary for their activity.

Finally, the relational aspect of the organization, which gives value to all identities, also includes means for the police to trace the mafia and terrorist networks.

9 December 2015