Digital Identity Management
The issue of Trust and the role of Trusted Third Parties

Jorge A. Restrepo, November 2018

Having an identity is a foundational human right

From birth to death, each individual human being is unique and at the same time bears equal dignity and rights with their congeners. For this reason, each individual human being needs to be differentiated. This uniqueness is established by law and follows a protocol that starts by registration at birth. Registration at birth is at the same time a right and an obligation. A right to the individual, an obligation to the State. State asserted identity consists of a set of personal data, normally name, date and place of birth, sex and parents. It also consists of some kind of credential that proves the identity. However, there are well documented state malfunctions that fail to provide a 100% coverage of birth registration in over 110 low and middle-income countries in the world[1]. As a result, an estimated 1.1 billion people living on earth possess no legal identity, which is roughly 14 % of all human beings on this planet. This is a serious problem, as having an identity is the foundational human right from which other rights originate. The right to education, health, justice, political participation and so on emanate from having a recognised civil status as a citizen. International governmental organisations, led by the World Bank, follow the state of birth registration and the processing of vital statistics as a means to good governance and provide valuable data on progress to be made[2].

Conclusion: civil identities are provided by a trusted third party that is not always and everywhere worthy of trust: the national state. Nonetheless, the need for a trusted third party that confers authority to the individual identity is universally acknowledged and the national state is the entity considered to be endowed with the right and obligation to do so. The state issues a credential attesting the identity. This credential may take different forms but is increasingly part of a digitalised system.

Modern Identity systems and human rights

The debate about civil identity in modern times has an added complexity due to the technologies available to implement a civil registration programme. The present tendency consists on launching national digital identity programs, in other words, programs that stock sensitive personal information in numeric databases, including – often, the biometrics of the individual, though not all biometric information can reliably be taken from babies[3].

In that respect, a number of practitioners and sponsors of civil identity programs have identified a series of good practices http://id4d.worldbank.org/principles that are supposed to offer guarantees for the individual that their rights will be respected; though the reality is best described by Joseph

[1] The World Bank monitors the state of civil registration world-wide. See https://www.worldbank.org/en/topic/health/brief/global-civil-registration-and-vital-statistics
[2] State of the art studies are conducted permanently by the World Bank, see more information at http://id4d.worldbank.org/country-action
[3] The consensus is that taking the fingerprint of an infant, for the purpose of then later using the information for the basis of an adult ID card is unreliable. This is due to the changing nature of fingerprints. A range of different ages are put forward for when it is best to first take fingerprints for the purpose of ID cards, with the European Union criterion of 12-years-old being the earliest.

Fondation OISTE
World Trade Center II – 29 Rte de Pré-Bois, CH – 1215 Geneva 15
Tel: 022 594 30 00; Fax: 022 594 30 01; e-mail: info@oiste.org
www.oiste.org; www.facebook.com/iosetransactions
Organization in special consultative status with the Economic and Social Council of the United Nations (ECOSOC)
Accredited member of the Non-commercial Users Stakeholders Group (NCSG) and Not-for-Profit Operational Concerns (NPOC) of ICANN

Cannataci, Special Rapporteur on the Right to Privacy to the UN Human Rights Council, when he observes that “*while international human rights law provides us with the basic set of universal, high-level principles and rights, certainly in the case of privacy, it does not currently offer the level of detail which is essential for us to operationalise the right in this fast-changing digital world.*[4]” Advocates for the protection of human rights on the digital sphere distance themselves from the enthusiasm about national biometrical identification systems[5]

Born to the Internet registration: the riddle of a secondary identity

But we are still lacking a solution to a different, equally obnoxious and persistent problem: the absence of a universally recognised, easy to use, interoperable, economic, secure and privacy-respectful solution for the purpose of identifying oneself in cyberspace. That is our focus: the question of a reliable trusted third party in cyberspace, which validates the individual user’s identity.

Today, more than half the world’s population uses the Internet, a technology that enhances communications and data transfers worldwide, where there is an apparent freedom to navigate without revealing one self’s identity. However, in order to establish meaningful communications, it is necessary to exchange some identity data. Knowing who the user is and what service it demands is a necessity: Internet could not function without a flow of personal data. The devil is in the details of how personal data is provided, how it is stored, for what purposes, with what kind of authorisations, with what degree of user control.

Internet service platforms function as information silos where personal data is protected by usernames and passwords. The individual provides some kind of personal information in exchange to accessing services – a lot of them free of charge – where a certain level of trust is required. However, in most cases, there is no requirement that this data mirrors the civil, state-issued identity of the individual.

This is perhaps the Achilles heel of the Internet: the absence of an identity layer. On-line security and digital identity management are completely interlinked. Building trust on-line is a technological challenge. The majority of users are not aware that behind the sign-in schema, there is a *Public Key Infrastructure (PKI)*, a mathematical tool that establishes an exclusive channel of communication between the owner of a Public Key and the owner of a Private Key. Both keys are in the hands of a PKI service provider or some entity in a chain of authority delegation, who hands the Private Key to the individual user as the result of a transaction where the individual users provides a relative assurance with respect to their identity. The information exchanged within this communication channel is protected by a cryptographic root. In other words, cryptography serves as a curtain that protects the communication of two people in a crowded room: one end speaks an incomprehensible language (the Public Key) that only the possessor of a Private Key can decipher. For the rest of the crowd, what happens between those two end points is impenetrable[6].

This is how digital identity management works in Internet. Its validity is enforced through protocols and trust management agreements. The entity that issues the Public Key is named a Certificate Authority (CA) and when the CA “signs” or approves an exchange of information between a Public Key and a

[4] Statement by Joseph Cannataci, Special Rapporteur on the Right to Privacy to the UN Human Rights Council, Geneva, 6th of March, 2018.

[5] For instance, Access Now, see https://www.accessnow.org/digital-identity-programs-what-could-go-wrong-our-contribution-at-unctads-e-commerce-week/

[6] Nevertheless, there are several weak points that are used by hackers to break the security of the system. Very advanced data-processing techniques (quantum computing) will be able to break all PKI coding in the future. See the article “Prime factors” in The Economist, October 20th 2018.

Private Key, the result is analogous to "notarizing" and identity in the physical world. The CA Browser Forum and the Mozilla Foundation provide a list of CAs.

Certificate Authorities which operate cryptographic roots are thus the trusted third parties in cyberspace. But the notion of identity that they validate is very different to the state-issued identity. Certification Authorities cannot be compared to the state as a trusted third party, with the exemption of the issuance of Electronic Signatures, where CAs must check the legal identity of the individual.

Nevertheless, there are vulnerabilities within the CA system. The standard of the Public Key certificates emitted by CAs is known as SSL/TLS X.509. It is those certificates that validate a web-site as secure, identifying it with the letters HTTPS in the navigation bar, hence validating it as a secure site. The problem is that this validation, once is emitted by a CA, is not questioned by other CAs: the system assumes that none of the CAs has been compromised or has questionable integrity in regards to the issuance and signing of X.509 certificates.

An institutional answer to the above is the Web-Trust auditing system: roots of trust bearing the Web-Trust sign have undergone a check of their reliability and integrity. The OISTE WISeKey root publishes an annual audit. Risks are also confined by the limited number of recognized Certification Authorities and the high concentration of certifications originating from just a few of them: more than 99 percent of all SSL certificates originate from only seven of the world's largest providers. Mozilla's root store lists just 65 proprietary holders or trusted root certificates.

Another way to protect the credibility of CAs is by creating standard-making bodies and collaborative ventures such as the CA Security Council (CASC), see https://casecurity.org/casc/ and the CA/Browser Forum: https://cabforum.org/. The latter produced the Extended Validation as a means to guarantee that only CAs which undergo an independent audit, whose juridical status has been checked and verified, will emit Extended Validation certificates.

However, none of the above offers a generic and final solution to the problem of the individual's digital identity in cyberspace. All it does is offering an endless cycle of username and password creation, defying the more robust memory to keep them all under control and piling-up personal data all over the Internet, without guarantees with regard to the level of protection and the ownership of data.

Privacy has become a growing concern. The European Union recently enacted a law on personal data protection – known as the GDPR – that endows the individual user with robust rights over personal data. This law is already influencing legislation on other jurisdictions. However, it remains to be seen whether the problem will be solved legally or by the introduction of new technologies.

Finally, there is a debate concerning the advantages that cyberspace offers to use pseudonyms, create avatars or avoid identification as a means to foster and protect freedom of expression.

Conclusion: Certification Authorities are trusted third parties that offer a reasonable degree of trust, but their authority to legally validate the identity of an individual is limited since there is not a binding link to the civil, state-issued identity of the individual. All the system cares about is that there is a concordance between the Public and the Private Key, not who the user is. However, this is the mechanism commonly employed to create trust on-line with a relative degree of identity involved.

Electronic signatures – a higher degree of digital identity

Using the same PKI technology, with certain upgraded features, some qualified Certification Authorities offer – for a fee – the service of electronically signing on-line. In this case, there is a legally standing link to the civil identity of the individual, which must be guaranteed by the third trusted party, i.e. the qualified Certification Authority.

The validity of an electronic signature is equal to the handwritten signature in the physical world and has to comply with some regulatory frameworks: eIDAS in the European Union; NIST-DSS in the USA; ZertES in Switzerland. The requirements are that: (1) the signatory can be uniquely identified and linked to the signature; (2) the signatory must have sole control of the private key that was used to create the electronic signature; (3) the signature must be capable of identifying if its accompanying data has been tampered with after the message was signed, and (4) In the event that the accompanying data has been changed, the signature must be invalidated.

The United Nations Commission on International Trade Law (UNCITRAL), a standard setting organism, produced the UNCITRAL Model Law on Electronic Signatures (2001), which has been adopted in some 30 jurisdictions. A relatively recent update (2005) establishes a mechanism for functional equivalence between electronic and handwritten signatures at the international level as well as cross-border recognition.

Notwithstanding the value of all the above, the truth is that digital signatures do not provide an answer to the question of how to implement a security layer that will change the sign-in paradigm of username and password. For the lambda Internet user they are costly, complex and useless, since they provide a much higher degree of trust than is required for most day-to-day interactions.

Conclusion: what seems to be missing in Internet is a simple mechanism by which users will avoid the pitfall of providing too much personal information when it is not needed while at the same time establishing communications within an environment where trust is provided and enforced by the information and communication technologies used.

As things stand today, GlobalSign has a point when they state that: "Having formed the backbone of internet security for nearly the past two decades, certificates from publicly trusted CAs remain the most proven, reliable and scalable method to protect internet transactions. CAs continue to work in collaboration with browsers and other parties to enhance the SSL protocol and enable additional functionality that will continue to meet evolving threats and protect all users"[7].

The whole debate about "digital identity management" is misled by the fact that the term "identity" is used to reflect personal data management, not pure identity. The issue that really concerns us all is "personal data management", with privacy, security and ownership being the main topics to be resolved.

New proposals are emerging. According to some "we are at a point in the development of identity that it is possible to develop and deploy technologies that allow individuals to create a self-sovereign basis for their identity independent from civil registration[8]", but this brings us to the false dichotomy of pure identity versus the present challenges of personal data management. What is at stake is not pure identity, what is at stake is personal data management and the link to civil registration has nothing or very little to do with it.

[7] https://www.globalsign.com/en-ph/ssl-information-center/myths-about-cas/

[8] This is the proposition of the Self-Sovereign Identity movement and the SOVRIN Foundation. See Phil Windley's blog http://www.windley.com/archives/2016/04/self-sovereign_identity_and_legal_identity.shtml. The foundation site is https://sovrin.org/