Digital Identity[1]

Paulo Esteves Veríssimo
pjv@di.fc.ul.pt

José Gomes Almeida
jose.gomes.almeida@apdsi.pt

Pedro Antunes
paa@di.fc.ul.pt

Rogério Bravo
rbravo@mail.telepac.pt

José Pina Miranda
jose.miranda@multicert.com

Pedro Verdelho
pedro.verdelho@gmail.com

André Zúquete
avz@det.ua.pt

Digital Identity (or DI) is perhaps one of the most passionate issues of our days. There is not a single citizen, institution, legal entity, which will not be impacted by it, when unavoidably, the activity of society moves on, prevailingly, to the cyberspace field.
In a near future not having digital identity will be, to a great extent, the same as not having an identity card nowadays.
In its essence, digital identity is based on information on physical and legal persons, which is collected, organised and updated in computer systems.
The certification and checking of digital identity of an individual is based on the so-called digital signature, resulting from the application of a cryptographic feature to an arbitrary text (which is signed), and that feature is only possible to implement, in theory, by the owner of the signature (the individual), holder of what is called a private key.

The elegance of the process is that the signature checking can be done by anyone who has the so-called public key.
Therefore, we have, for instance, the improvement of the robustness of a signature and an interesting democratization of the notary public duty with a remarkable precision.
But on the other hand, in the case of identity theft, the problem becomes much more serious, since it is virtually impossible to distinguish between a signature done by the individual and the one done by an impostor.

In addition, the definition, creation and management processes of digital identities in a society go beyond, to a large extent, this simple technological process, and in our society, migration to Digital Identity moves forward, conspicuously, in default of the understanding, acceptance and participation of the stakeholders, the citizens and the organizations.
Part of the problem has to do with the potential alienation of the various public powers, from public administration to judicial power and the deep social implications involved by digital migration.
A Digital Identity project is not a mere technological project.

[1] The disclosed opinions are the exclusive responsibility of the authors, and do not necessarily reflect the positions of APDSI or any other entities mentioned in the text.

The digital identity belongs to the universe usually referred to as «information society», is multifaceted, and some of the problems which have emerged in the identity "digitalization" process result from narrow perceptions of that reality. In other words, they result from approaching DI only from a technocratic, or commercial, or political or even police/security perspective.
If this approach is to be kept, the DI vision will never succeed.

About the security and technocratic aspects, one may argue, as it has often been heard and read, that «everything or almost everything can be justified when it comes to guarantee our safety» against the most diverse threats, or even that the most important thing is «the efficiency and effectiveness of the administrative, financial and commercial processes».

In fact, these are hasty and somewhat naïve visions of the reality, based on the presupposition that the citizen has a static and passive attitude regarding the information society and the measures imposed by it.

Quoting [1]: «... the citizens are getting more and more suspicious about the information and communication services and infrastructures ...» or «... the experience of the common citizen is dominated by the public awareness about computers' failures, unsuccessful big software projects, malicious programs (virus, *spam*, spies)

There is no other reason for this attitude rather than the security problems perceived by the users, which are far from being solved and which lead to the deterioration of the *trust* felt about the systems.
The non perception of these dynamics by the stakeholders may lead to situations of difficult return as far as the information society is concerned.

Quoting again [1]: «... if a society based on ICT is not capable of generating trust in the services, that is, trust based on justified and reliable arguments, then, those services, which will be no matter what, available due to the market's pressure: shall be regarded with mistrust by the users; shall be managed by restricted groups of "experts", increasing the digital apartheid; they may be ill managed, leading to cyber-crime, e-fraud, cyber-terrorism or sabotage...».

It is not difficult to see the serious problems which may arise in a near future: with Digital Identity systems which are apparently interesting from the technological point of view but not suitably protected by certifiable and auditable safety property; with the lack of a more than necessary modernization of the law on computer crime, or the general adequacy of laws related to identity and identification; with the lack of follow up of means, predominantly of technological nature, which guarantee the effectiveness of police forces and courts in the digital field.
Nowadays, any citizen is the supreme holder of his identification document, his signature, and the privacy rights on the latter and associated data which the Portuguese Constitution grants him.
Consequently, the most serious problem will be taking on technical, political and legal solutions which do not guarantee the ownership and the control of the stakeholder's Digital Identity by themselves.

Digital Identity is upstream various other critical processes, such as: electronic vote; control of accesses (including crossing borders); e-commerce; processes' digitalization in public administration and health.

At this moment, for the policy makers, the debate on identity management shall be actively connected to the official identification documents, such as the Citizen's Charter and the new Portuguese Electronic Passport.
At the same time, for the providers of services and goods, the discussion focuses on the selection of technologies to certify citizens and businesses.
However, the debate on identity management should be placed in such a way as to simultaneously face a set of problems: the wishes of the citizens, related to the protection of liberties, privacy and other prerogatives; the national security concerns, related, for instance, with crossing of borders and the authentication of operations; and the functional efficiency of the public "whole" connected to the *reengineering of Public Administration focusing on the citizen*.

These problems were looked into with some detail in a recent study [2], which examines the several aspects and lists the possible risks, highlighting the main ones: theft, forgery or loss of identity; violation of privacy and the control over personal data; syndrome of the single number; speed and automation of frauds; reliability of frauds.
In the same study some strategic guidelines are proposed regarding the action of the public powers, both in fields directly connected with the State and in those which should indirectly set out the action and behaviour, rights and duties of the other stakeholders (citizens, organizations, companies).

Let us look, in some more detail, into some of these issues, in a perspective of governance.

The high skills of the currently available technological systems make the access, unsuitable transmission, handling and dissimulation, theft and even blackmail on information extremely easy.
Questions about privacy protection, security of assets and well-balanced practices to make information available are being raised.

The governments need to consider several aspects which are, sometimes, difficult to harmonize such as: implementing specific services for the citizen's convenience reasons, but which may reduce their privacy and safety; implementing processes and systems intended for the identification of terrorists and other criminals but which may raise a moral doubt; to adopt interoperability solutions with systems of several sources by means of open solutions, which will, at the same time, have an impact on the social contract between the citizens and the state.

As information systems are being integrated, further developed and modern technological solutions are being adopted, usually with the purpose of increasing the citizen's benefits and/or for the users of some specific businesses, portals and other access points emerge on the Web.
This type of services is normally characterized by a high fluidity and volatility, as they can appear, change and disappear from one moment to the other.

That evolution intensifies the need of improving the management of identities, that is, the way authentication of individuals is carried out, preventing the unsuitable establishment and/or excessive fluidity of the identity.

The policies regarding (technical and not technical) systems for the operation in the scope of Public Administration and in the field of management of digital identities should compulsorily be sensitive to the existing backgrounds: legal, economic and social.
In the case of Public Administration, we may consider that "management of digital

identities" is based on systems combining technology, procedures, action practices, laws and policies which:

i. Put in frame and support the common needs for identification in transactions involving state, governmental and private entities.

ii. Enable reducing governance costs and to improve the quality of the services provided by public entities.

iii. Safeguard resorting to sanctionary mechanisms.

iv. Enable preserving or improving privacy, liberties related to the citizen's identity and the protection of information on people and organizations.

However, it should be noticed that these systems tend to adapt themselves to the new technological solutions in a much slower way than the evolution of the former. One of the images of the control theory is that the response of the system is sub-buffered. However, these adaptation periods of the systems to the new solutions create many possibilities for the occurrence of not foreseen legal, economic or social failures.

In Portugal, the risk management and change management regarding the new technologies is still a bit diffuse, and it is not obvious that factors and trends will be more relevant and will have an impact on medium and long run decisions (of national scope).

Currently there is a natural and usual pressure from the private sector on the governance in order to foster the adoption of certain digital identity's management solutions, without previously taking precautions regarding risk factors and the planning and change management processes, especially as far as the effective protection of the citizens' privacy is concerned.

In this context, we will point out an advisory report recently produced by National Committee for Data Protection [3], regarding the Citizen's Charter, which enables to predict the occurrence of digital interaction modes with the public domain which may deprive the citizen of protection, as to his privacy and more.

The citizens should have a clear perception of the benefits of migrating to DI. In other words, the citizens will gain a solid trust in Digital Identity, in so far as the latter is built based on trustworthy processes and systems.
Without that, it will be like an imposed faith, which will become undermined with the first adversity.

This can only be rationally achieved if the computer processes and systems of Digital Identity are introduced to society with such transparency and simplicity that enables the former to organize itself in order to understand and assess them in an independent way, and/or do the same with the studies necessarily produced by the "owners" of these DI systems (public administration, financial system, other companies).

It is convenient to stress that, as far as the aspects of security and technologies of the most recent symbols of DI are concerned in our country --- Citizen's Charter and Portuguese Electronic Passport --- there are some reasons for concern, pointed out by various sources [2-4].
It is incumbent on the State and the society to avoid that major problems arise from that, because once the trust on the system is broken, it will be difficult to go back to the mentioned symbols. Going over on what has been said at the beginning of this

short text, only the search for the simultaneous balance among the various pillars (society, laws, police forces and courts, safety and technology) can assure solutions which may be efficient for the State, accepted by the citizens, preserve their rights and guarantees and which can also improve certain aspects of social life.

Bibliography

[1] – SecurIST Advisory Board. Recommendations for a Security and Dependability Research Framework, Issue 2.0, June 2006. EC FP6, Information Society Technologies.
http://www.securitytaskforce.org/dmdocuments/SecurIST_AB_Recommendations%20Issue_V2_0.pdf.

[2] – **APDSI**, A Identidade Digital, Actividade nº 1045, Lisboa, February 2007.
http://www.apdsi.pt/getfile.php?id_file=571

[3] – **Comissão Nacional de Protecção de Dados (CNPD)**, Parecer nº 37/2006, sobre o Cartão do Cidadão.(advisosry report no. 37/2006 on Citizen's Charter)
http://www.cnpd.pt/

[4] – **FIDIS European Network of Excellence.** Budapest declaration on ICAO Passports. Budapest, Setembro de 2006.
http://www.fidis.net/fileadmin/fidis/press/budapest_declaration_on_MRTD.en.20061106.pdf

Note

This text was previously published in number 139 (September 2007) of Revista Interface Administração Pública (public administration interface magazine) and is reproduced here with the agreement of the respective Board of Directors.

Lisbon, 2007.10.19