Identity in eHealth - from the reality of physical identification to digital identification

Abstract

Maria João Magalhães Pereira Campos

MESTRADO EM
INFORMÁTICA MÉDICA
2º CICLO DE ESTUDOS

Orientadores:

Luís Filipe Antunes, PhD

Manuel Eduardo Correia, PhD

Oct|2011 17 October 2011

Abstract

Many heterogeneous and highly specialized software applications for eHealth have been implemented and deployed by diverse health organizations, such as public and private hospitals and health care centers. The rational management of these eHealth assets together with their efficient and interoperable integration represents today a major hitherto unresolved challenge for the health sector at a global level. One of the present implications is the serious interoperability issues that arise by the lack of widely accepted standards for the homogeneous integration of the diverse identity and authentication mechanisms used by the eHealth applications ecosystem. Unfortunately this has not yet been a major infrastructure concern for the eHealth context and thus constitutes a major road block for the realization of these applications full integration potential.

It is a common occurrence that only at the time when an application is put into production there is an awareness about the sudden difficulty of integrating and conciliating the new application identity management and users profiles with what has already been done for the rest of the applications currently in production at the site. This situation is aggravated when the application leaves the local domain to be deployed at the regional or even national level, where, without a well-planned digital identification infrastructure, the applications integration difficulties can be orders of magnitude more severe.

In this work we propose a new high level model for the secure identity provisioning of eHealth applications. The critical infrastructure standard components required for such an infrastructure, together with the Portuguese eID smart-card, allow us to delineate a novel and highly flexible infrastructure for secure identity management and authentication services for eHealth.

The secure privacy oriented identity infrastructure we propose fits well within the specific needs of highly diverse eHealth applications, precisely because it provides a strong foundation, upon which more reliable, secure, trustworthy and real interoperable eHealth applications can be built and deployed.

The relationship between digital technologies, identification, and trust is complex. Some communities have preserved trust in reputation-based ID systems as digital proxies developed. In others, digital technologies have come to substitute for it.Â Identity in a digital age. From baby footprints to digital footprints. Present-day ID systems are epitomized by the inked footprints found on many birth certificates.Â In reality, identification has always been messy and probabilistic; digital tools let us estimate the risk of mistaken identity more precisely and better optimize systems to encourage trust. ID systems of the future could lead to more avenues for inclusion, more tailored civic representation, and more efficiency for institutions that rely on ID. A 2015 report from Accenture defined the four keys of digital trust as security, privacy, benefit/value and accountability. In other words, technology users â€“ whether they are citizens or students â€“ have to believe that a digital form of ID is not only safe, but also provides more perceived value than a physical format. But the tenants of digital trust go far beyond IDs; they extend to other areas of our life including control over our data and online history.Â Their goal is to build up the profile of digital identification before making a play into the public sector of hospitals, airports and other universities. â€œIf that cultural tipping point is there we could be onto something big â€“ hopefully weâ€™re just on time,â€ Murphy says. Digital identity capabilities from Trust Stamp are now being integrated with Mastercardâ€™s Wellness Pass solution, which it will launch in cooperation with Gavi in West Africa.Â A biometric digital identity platform that â€œevolves just as you evolveâ€ is set to be introduced in â€œlow-income, remote communitiesâ€ in West Africa thanks to a public-private partnership between the Bill Gates-backed GAVI vaccine alliance, MasterCard and the AI-powered â€œidentity authenticationâ€ company, Trust Stamp. We have been warning you night and day since March that this was coming, now itâ€™s here, the first iteration of Bill Gates fever dream masterpiece of a vaccine tied to digital identification.Â Welcome to Phase 1, in just a little under 4 months from the date we told you it was â€˜coming soonâ€™. Digital identification across platforms brings opportunities for individuals and businesses but requires security and data protection measures to be in place to foster trust. Trust is key This paper addresses a number of issues that arise from building digital identities based on foundation-al or functional identification systems. These include the need for a legal, data protection framework, security, privacy and consent, interoperability, and the importance of standards.