ELECTRONIC IDENTITY MANAGEMENT INFRASTRUCTURE FOR TRUSTWORTHY SERVICES IN E- GOVERNMENT AND E-COMMERCE

Alberto Polzonetti, Damiano Falcioni, Fausto Marcantoni
School of Science and Technology
University of Camerino (Italy)
Name.surname@unicam.it

Abstract - *A number of potential initiatives are being considered including the creation of a international electronic identity management infrastructure for trustworthy services in e- government and e-commerce. A lot of work has been done in recent years in the field of electronic identity management, including through a series of research programs and pilot projects. While each of these projects contributes new elements to the field of electronic identity management, it is also clear that the results will need to be developed further, refined and integrated. This paper would open the discussion on the need for a "multi-faceted electronic Identification (eID) system for all citizens", as a key enabler for trustworthy interactions between public authorities, businesses, citizens, and within the large spectrum of social networks and communities. This concept, which is also referred to as an ubiquitous eID infrastructure for digital life, is envisaged to offer a wide range of functionalities, including the provision of multiple identity instances, from government- accredited to commercially accepted, and ranging from near-anonymity to strong and unambiguous identification. Furthermore, the system should be user-controlled and privacy- protective, providing the basis for accountability and innovative applications in an open and competitive market.*

Keywords: *Electronic Identity Management, e-government, e-commerce*

1 Introduction

International eIDM ambitions are thus high, and it is not yet fully clear how existing initiatives and projects can be integrated into a common vision, or what framework would be needed from a technical, infrastructural, organizational and legal.

There is a need for discussions and consultations to determine exactly what can be expected from a eIDM infrastructure, what the approach and goals should be, and which steps need to be taken next to realize this vision.

The actual debate stresses the need for all states to increase its performance when it comes to the use of innovative ICT solutions, especially in the public sector. In a European context, for example, this emphasis on appropriate public policy is justified, due to the public sector's larger stake in GDP than in other regions of the world. To increase the use of innovative ICT solutions, three interlinked lines of action are proposed :

- Improving the quality and coherence of our investment efforts, as there is currently too much fragmentation which dilutes the efficiency of our investments;
- Raising investment in research and innovation, including through public procurements;
- Stimulating the demand for R&D, by opening up new markets for R&D to respond to real needs and challenges.

A set of measures for the public sector to achieve these goals will be proposed, including large scale actions that go from research to actual procurement and deployment, to ensure that R&D investments have a real impact in practice. This can build on existing building blocks that have already been used in Europe, such as Large Scale Pilots, Public-Private Partnerships and pre-commercial procurement of R&D. One of these areas in which this approach will be applied is the deployment of innovative eID solutions.

2 Needs And Objectives

After these introductory remarks and considerations, in this chapter we speak about on the needs and objectives of a eIDM system: what is it that we expect of something termed a "ubiquitous eIDM system for digital life"? What will the expected/desired impact be, and how far do we want to go?

After the development of basic internet services, service paradigms have moved on to web 2.0 services and are now shifting towards a cloud computing model. In this model, eID is often seen as one element of web services that needs to be able to integrate smoothly with other services. If this is to work in practice, a great deal of flexibility will be expected of the underlying eID infrastructure.

One of the first elements of debate in the community was the basic question of what constitutes an eID. This seems to be a very basic question, and a lot of research has been done on this point, but different perspectives can be taken, which will have a very significant impact on how a eIDM infrastructure should be created. Key questions and goals are:

i. The scope and meaning of 'identity' (at least for the purposes of a eIDM infrastructure) needs to be made clear. Intuitively we tend to think of identity in terms of physical people. From an e-government and business perspective, legal entities are equally important however; and it is even possible to consider the broader nothing of an identity of things/objects. The scope and definition of eID changes when we try to outline what we want to identify, and this is particularly important when examining semantics. Currently, exchanging electronic identity information is very complicated simply due to the lack of common semantics (e.g. even the simple notion of a name is interpreted differently from country to country).

ii. Related to this is the question of management of identities: who creates eIDs, and how are these managed? In reality, end users rely on a multitude of "partial identities" to represent or authenticate themselves in specific contexts, and it is unclear how this can be supported in a European eIDM infrastructure, or to what extent it should be. In order to address this question, it needs to be clear who registers and verifies attributes (if at all), and on what conditions these can be exchanged or re-used, or simply confirmed. Relying on market mechanisms to choose an economically optimal solution may not provide desirable results from a data protection perspective.

iii. Thirdly, an advanced identity management system needs to be able to manage links between entities. Simple examples include linking parent A to child B, or linking manager C to company D. Mandate management and role management is the main example of this. There is a lot of work still left to be done on this point: tools need to be created that allow users of a European model system to verify and manage such links.

iv. A fourth crucial element is the reliability of identity information, either in terms of being generally reputable (considered trustworthy) or in terms of real guarantees (accountability in case of problems). The role of the public and private sector was discussed in this regard as an interesting example: 'official identities' or 'formal identities' are often issued or managed by the public sector, but this doesn't necessarily mean that identification services provided by the private sector are less trustworthy or less usable in practice. From the end user's perspective, functionality is more important driver than clear guarantees in relation to the trustworthiness of identity information, as can be seen in the increasing importance of reputation based identification (e.g. in social networks, which are largely based on establishing trustworthiness via peer-to-peer appreciation). From the service provider's perspective, trustworthiness – especially in terms of accountability and liability – is much more important, and reputation as such may not hold sufficient appeal from this perspective. It has already been made clear in the past that future eIDM infrastructure in Europe should be multi-level, i.e. permitting varying levels of security/reliability. This is one of the key gaps that still needs to be filled.

v. Functionally, it would be important to uncouple the provision of electronic identification or authentication services from specific applications. An 'invisible eID infrastructure' is key to creating an open eID model that could be taken up in commercial and public sector applications. In that respect European governance has the benefit of being conceptually based on a roughly "federated" model. A web of services is a model that plugs into this same concept of thinking: application independence (service-independence) of the eID infrastructure is important.

vi. There is also the question on whether a European legal framework, or at least European guidelines for regulations, is needed. This issue was raised in relation to a number of points, including the multi-level reliability issue addressed above: some participants felt that governments needed to set up the rules and regulations to issue/manage tokens/eIDs, preferably based on European guidelines. Currently, national legal barriers impede some approaches that are being explored at the European level; examples include the German ban against the intervention of intermediaries in the relationship with the public sector (including e-government services), which impedes the use of proxy based identification models; and the ban on using permanent unique identifiers for generic purposes in Germany and Hungary, which means that any European approach cannot require the prior existence of such identifiers. Guidance is necessary on what the consequences of European initiatives will be, and how we can operate within the limits of

applicable laws, given the lack of direct European regulatory competence to harmonize eID regulations.

vii. Finally, the privacy and security aspect should take a central role. The point was made and discussed that private industry (on-line service providers, financial services, mobile communications, …) does not have much of a problem in getting the identity information that they want and as reliable as they need it to be. But there is a significant problem from the opposite perspective: how do you empower users to enforce their rights and manage their data? This should be addressed in a European eIDM infrastructure as well, and this should be done soon; security and privacy protection cannot be taken up as an afterthought. Innovative systems exist in current research, but the infrastructure must be set up to implement this.

Collectively, the considerations above contain a good summary of what can be expected or should at least be considered as the needs of a eIDM infrastructure (in no particular order):

- Clear definition of scope: what is the concept of identity that we want to address at a European level?
- Management of identity: which entities need to be involved in managing an identity, and what is their function?
- Management of relationships: how do entities whose identities are managed relate?
- Trustworthiness of identity: how can you trust the identity, especially in terms of accountability and liability?
- Identity provisioning in applications and services: how do you use identity in an application?
- Clear legal framework: how to regulate the use and management of identity?
- Privacy protection and secure identity management: how do you integrate users' rights into the infrastructure?

3 IMPLEMENTATION

Having discussed the needs in relation to eIDM infrastructure, this chapter examined how an infrastructure meeting these requirements could be implemented, taking into account the diverging and demanding needs in relation to such issues as identity re-use, tiered reliability and trust, private sector support, privacy-by-design and enforcement of applicable rules.

The first aspect extensively discussed in this regard was the strong role that innovative technologies could play in developing this infrastructure. Regardless of the preferred technology, any electronic identity management system is inherently dependent on the use of a secret in some form over another. There are already advanced identity management models in place that allow you to spread a secret robustly over many locations, and that allow you to limit the disclosure of identity information (such as e.g. IBM's Idemix or Microsoft's U- Prove). This allows you to increase security and reliability and improve data protection enforcement. Such PETs need to be developed and deployed further, and it needs to be examined in particular how take-up of such advanced models can be encouraged. The development of a business case around such models is crucial in this regard, as will be further discussed below. Finally, any approach taken at the European level needs to be sufficiently flexible to take up newer approaches to identity management that might emerge or increase in popularity, including e.g. identification based on biometric encryption (through local verification of biometric information) or mobile identification.

As a complement to the technological tools deployed, the architecture as a whole also needs to be designed to meet the objectives above. The role of validation services and proxy services was mentioned in this respect, as solutions that were currently being tested in STORK and PEPPOL, and that were also being examined by private sector partners. These approaches are appealing, as the main issue to be resolved here is to determine reliability/authentication levels; other issues could then be handled by federating (i.e. managing them at the national level). However, other participants in the meeting rightly indicated that such solutions would need to implement strict safeguards to address privacy and security issues: it should be ensured that such solutions cannot become a single point of failure, and that they do not retain information on identity use; otherwise, they constitute a significant privacy threat. Other approaches should therefore also be considered.

Both with regard to technology and infrastructure, the importance of working with industry partners was generally recognized to be crucial. Public-private partnerships and systematic coordination with industry was seen as a key way of ensuring that any model adopted at the European level would also see substantial take-up in reality. It is necessary however to consider the different stakeholders, and particularly the different interests between eIDM users and eIDM vendors. Without a proper link to industry however, European initiatives risk remaining at the theoretical or pilot level, or seeing limited practical use. The integration of harmonized eID middleware implementations in existing operating systems distributed by major vendors was given as an example to be looked at. By harmonizing protocols, the integration and use of existing and new eID solutions could be facilitated to a significant extent.

However, measures to achieve the desired outcomes should not be focused exclusively on the technological and infrastructural aspects, but also on legal issues. There was some doubt whether European regulation was a useful (or even possible) route forward, given the fact that identity

management is generally regarded as a national competence, but it was considered that guidance and support could be provided once an appropriate paradigm for an eIDM infrastructure was established.

In addition to the technical, infrastructural and legal challenges, perhaps one of the most challenging issues is creating a model that has sufficient appeal to end users and service providers, i.e. ensuring that the eIDM platform has real business appeal. To do so, we need to make sure that our own goals and expectations as described above match those of the stakeholders. For instance, while data protection issues and user control are societal needs that must be protected to safeguard our European values, end users' perceptions seem be driven more by short term convenience. There may be a need to reflect on future needs and values in the discussion between experts and end users in this respect.

Naturally, we need to make sure that there is a real business model that makes sense to stakeholders. The example of banks was discussed on this point: even banks that could use a generic eID token (like a government issued eID card) are generally reluctant to do so, even if it would be more secure than their own existing solutions. At least part of the reason is that having their own solutions gives them full and exclusive control over the business model, and that their own tokens act as an advertising medium in a way that generic eIDM tokens would likely not be able to offer. Can this be addressed appropriately? This concern however would be completely different for small innovative service companies.

Globally, while there was a strong consensus on the importance of each of the aforementioned issues (technology, infrastructure, legal framework, business case), it was also felt that some additional research would be required to offer satisfactory answers that would allow the creation of a coherent and suitable European eIDM framework. The question was raised on whether an 'eIDM research roadmap' was needed, and if so, what it would look like. This is a complicated issue, due to the need to continuously take into account the changing eID landscape in each of the countries involved and in the eID industry. A flexible approach would thus be needed, with a strong emphasis on maintaining open communications with industry representatives.

Despite this complexity, if we want to go from research to implementation as envisaged by the planned Communication, we need to make sure that our knowledge of the eIDM landscape is complete, and research on a number of key issues still seems needed. Principally, the conceptual model behind the functionality that we are looking for is not clear: how can specific roles and responsibilities be defined and organized in a general eIDM framework, and how can the advanced technological options commented above be integrated into this framework? Secondly, the economics behind eIDM are not well understood, or more accurately: it is unclear how the objectives that we have envisaged above can be implemented in a way that is attractive for end users and service providers alike. Broadly painted, many service providers with an extensive customer base and the required infrastructure want cheap access to as much info as they can use, and end users are more interested in convenience than in security; at any rate, it seems unlikely that end users would be willing to pay a premium for security. It would be interesting to see if there are cases currently available that are supported by the market (as opposed to government mandate or subsidies), or what encouragement measures are being applied effectively to improve the economic appeal of electronic identities.

Apart from the concepts and economics, the issue of accountability was presented as an area of discussion. Electronic identity management is needed to support accountability, by giving the service provider a way to reliably link certain actions to certain users. Currently, this operates mostly within closed contexts: service providers can rely on electronic identities either because they issue or manage them themselves, or because they have a clear contractual relationship with the issuer of the credentials. Open eID infrastructures that are not limited to a closed group of service providers see much less uptake, and the issue of accountability plays an important impeding role here. This becomes even more clear when discussing whether private sector issued eIDs should be usable in a public sector context. While there is no objection to this in principle, there is still a substantial lack of trust and a real need for sufficient accountability guarantees.

In addition, as was also noted above, even if accountability from the end user is sufficiently guaranteed to the service provider, the inverse relationship (accountability of the service provider to the end user) is not yet guaranteed in practice; this is an aspect where further research or possibly regulatory guidance might be needed, including in terms of implementing real privacy-by-design solutions, to ensure that our envisaged European eIDM approach is sufficiently focused on the end users' interests as well. In the same respect, the questions of usability and accessibility were raised: solutions need to be inclusive to all users. While a lot of research has already been done in this domain, there is a clear need to link this research to real results.

Globally, there was a consensus that new research would be needed to coordinate existing knowledge and know-how (which is already available to a significant extent in Europe) into a coherent vision. A comprehensive approach would be needed to form a coherent picture of how existing solutions and newer innovative approaches could be integrated into an eIDM infrastructure that supports the needs and objectives defined above. The issues of accountability, economics and inclusiveness were identified as key problems to be addressed in this research. Further efforts could then focus on creating the necessary components in a second stage.

It is thus clear that future research will be instrumental in shaping the approach taken towards creating the envisaged ubiquitous eIDM infrastructure. Specific tools are to steer

this research or to bring it to fruition, including through pilot implementations or actual deployment.

A number of interesting possibilities for moving forward were none the less discussed, including:

Identification and dissemination of best practices in eIDM initiatives, as is currently already being explored (e.g. through the eID Observatory);

Collecting and disseminating clear overviews of the art in eIDM solutions, as a way of encouraging take-up of advanced solutions by currently less advanced market players and as a way of permitting frontrunners to explore innovative solutions more easily;

Focusing on standardization efforts (e.g. standardization of interfaces) to reduce the complexity of the problems we are facing;

Identifying and exploring innovative eIDM approaches, to determine which approaches are already being tested/implemented that could meet some of the requirements above.

These approaches are appealing, as they would allow progress to be made irrespective of the final outcome to be chosen. However, it is clear that a coherent model for a eIDM infrastructure would need to be determined before the outcomes from these approaches can be leveraged fully, and that the full societal context needs to be considered, including the need for inbuilt privacy protection and security.

4 Socio-Economic Impact

In this section we discuss the socio-economic impact of creating a eIDM infrastructure, including in terms of financial gains and general benefits to all stakeholders.

From a macro-economic perspective, one of the first interesting aspects of this debate focused on export possibilities. The European approach to identity is rather particular, and reflects our cultural attitudes towards identity, data protection and privacy. The discussions above (including on technical, infrastructural and legal needs) reflected this: there is a desire to ensure that our eIDM infrastructure matches our cultural perceptions on these issues. While this European approach may not be universally welcome, it does open interesting avenues for exploitation. Some regions (including e.g. in Asia) have shown some interest in European personal data paradigms, and we should thus not overlook the possibility that the eIDM solutions developed in Europe could prove to be valued exports. Thus, from a macro- economic perspective, there appears to be a real potential for validation.

However, the micro-economic perspective must also be considered, and it was clear that on this point the socio-economic impact depends on whose interests you're considering (service providers, end users, or solution vendors). The return on investment therefore also depends on whose perspective you take, and one of the key complexities to be overcome is the need to make sure that there is a fair distribution of benefit; otherwise, the solution will not be taken up. This is linked to the business model question raised earlier: who is profiting from the infrastructure, and who is paying for it? These two aspects need to be sufficiently linked.

You might want to consider an authentication process as an example of a business model. Such a model is not necessarily a best practice (or legally permissible in countries that require CSPs to offer free verification services), but it does illustrate the point: without a real business model that matches cost with benefit, uptake will suffer. The Norwegian and Swedish public sector, for examples the public sector acknowledged that they wanted end users to take up eIDM, and that taking up part of the bill as a government was an acceptable cost of public policy. In contrast, in the UK initiatives relying on the users' willingness to pay for authentication certificates failed. This was acknowledged to be a key question: how do you model pricing and benefits to optimize uptake?

In that respect, it is clear that underlying costs that affect the price tag must also be acknowledged and accounted for. Liability is a key component of cost: during the discussions, Nordic approaches emphasizing trust were contrasted with other European approaches emphasizing accountability. While both approaches can function within their respective markets, interconnecting them will be quite complicated, due to the need to bridge this difference in perception of accountability requirements. Similarly, there is often a price to be paid for simplicity and accessibility: username/password systems may be easy and seem cheap, but when support costs for forgotten passwords are factored in, the picture may change. These elements also play a role if you want to accurately gauge costs and benefits.

5 Conclusion

It seems that there was a good consensus on the objectives for a eIDM approached as commented in the first section above, and on the need for additional research on a number of issues, including on accountability, economics and inclusiveness. These should permit the creation of a coherent concept for a ubiquitous European eIDM infrastructure, suitable for adoption by public and private sector service providers, and adjusted to the needs and expectations of the end users. The creation of an appealing business model that links costs to benefits will be crucial to ensure real take-up, keeping into account that both costs and benefits will have clearly visible and less apparent implicit components.

These issues will not be solved in the short term, and further reflection and refining of the positions above will still be needed to arrive to a clearer picture of Europe's post-i2010 objectives and strategies in the field of electronic identity management.

Please use the styles contained in this document for: Title, Abstract, Keywords, Heading 1, Heading 2, Body Text, Equations, References, Figures, and Captions.

Do not add any page numbers and do not use footers and headers (it is ok to have footnotes).

6 References

[1.] BOTTERMAN, M., GRAUX, H. and MITRAKAS, A., "A Roadmap for a pan-European eIDM Framework by 2010", http://europa.eu.int/information_society/activities/egovernment_research/doc/ eidm_roadmap_paper.pdf (accessed November 2011)

[2.] DUMORTIER, J. and GRAUX, H., Legal Study on Legal and Administrative Practices Regarding the Validity and Mutual Recognition of Electronic Documents. November 2006. Draft Final Report. Tender No. ENTR/04/67. 111 pp., http://ec.europa.eu/enterprise/ict/policy/legal/index.htm (accessed November 2011)

[3.] ENISA "Privacy and Security Risks when Authenticating on the Internet with European eID Cards", November 2009, http://www.enisa.europa.eu/activities/identity-and-trust/eid/eid-online-banking, Accessed November 2011)

[4.] EU research & innovation strategy for digital technologies, http://ec.europa.eu/information_society /newsroom/cf/ document.cfm? action=display&doc_id=597 (accessed January 2011)]

[5.] Eurosmart," European Citizen Card: One Pillar of Interoperable eID Success", October 2008, https://www.eid-stork.eu/dmdocuments/public/ecc-position-paper-final.pdf (accessed November 2011)

[6.] Leitold H.and Posch R. and Rannenberg K. and Krontiris J., "eID Interoperability (chapter 12) book title: Handbook of eID Security: Concepts, Practical Experiences, Technologies",{2010},pages = {167 - 186}, publisher = {Walter Fumy, Manfred Paeschke}

[7.] Reinhard Posch,"Trust, Security and Identify Managament: The Austrian Viewpoint",Conference on Trust and Identity Management,year = {2007},pages = {12 - 21}