Towards a seamless digital Europe: the SSEDIC recommendations on digital identity management

Maurizio Talamo (1), Selvakumar Ramachandran (2), Maria-Laura Barchiesi (2)
Daniela Merella (3) and Christian Schunck (3)

(1) Nestor Lab University of Rome Tor Vergata
(2) University of Rome Tor Vergata
(3) Fondazione Inuit University of Rome Tor Vergata
Via dell'Archiginnasio snc
00133 Rome, Italy
lastname@nestor.uniroma2.it

Abstract: The SSEDIC ("Scoping the Single European Digital Identity Community") thematic network has concluded an intensive 3-year consultation period together with over 200 European and international digital identity management experts and many stakeholder organizations to establish recommendations that address key issues regarding the usability and interoperability of electronic identity management solutions. The resulting recommendations are presented in this paper and should support the European Commission as well as other public and private stakeholders to set priorities for the path towards a Single European Digital Identity Community and the Horizon 2020. The key areas that need to be addressed as a priority are: mobile identity, attribute usage, authentication, and liability.

1 Introduction

Digital identity management plays a fundamental role in securing trust and cooperation in digital and interconnected societies [Axe84, Che05]. The challenges in developing digital means that enable humans to extend their highly developed ability to recognize people and groups in the offline-world into the cyber sphere are significant. Apart from technical also psychological, cultural, legal, ethical, economic, and social issues need to be considered in the process of designing solutions which should be interoperable and convenient to use.

The objective of the SSEDIC thematic network [1] is to provide a platform for all the stakeholders of eID (electronic identity) to work together and collaborate to prepare the agenda for a proposed Single European Digital Identity Community as envisaged by the Digital Agenda (DAE) in its Key Action 16. To achieve this goal the SSEDIC consultation got in contact with as many and diverse stakeholders as possible. SSEDIC met with eID experts from the NSTIC program [Hou11] in Mountain View, Washington and London, SSEDIC

[1] SSEDIC is a EU funded thematic network (ICT PSP Call4), coordinated by Nestor Lab, University of Rome Tor Vergata, Italy. For an overview of the more than 60 SSEDIC partners and associate partners see http://www.eid-ssedic.eu

developed ties to stakeholder organizations in Russia, Turkey and Asia, SSEDIC engaged with international eID experts at ITU in Geneva and ISO/IEC in Rome, and had regular meetings in Western and Eastern Europe. SSEDIC and other European initiatives were presented and discussed at numerous conferences across the European member states as well as in India, Hong-Kong, Dubai, and Moscow. SSEDIC members met with diverse audiences including banking, law, law enforcement as well as representatives from the online entertainment industry and tourism [SSE12c, RZHM14, KRS]. SSEDIC partner organizations represent eID related experience gained in part through EU funded research projects with a total budget of more than 150 million euro [2].

The recommendations in this document are an essential outcome of three years of work by the SSEDIC community [SSE12c]. The process of drafting these recommendations in 2013 involved a short SSEDIC partner survey, a row of monthly meetings and conference calls which lead to an intensive two day meeting in Rome in which the recommendations were prepared. The resulting recommendations were sent to the SSEDIC community in October 2013. All partners were given a two week time window to vet the recommendations and to inform SSEDIC management of any concerns. The recommendations were also presented to a general audience at a workshop at ISSE in Brussels and at the ICT 2013 meeting in Vilnius. The recommendations reported below therefore express the consensus of all SSEDIC partners on how to address key-issues related to digital identity management in order to achieve the ambitious goal of a single European digital identity community.

The key areas that have been identified to be addressed as a priority are: mobile identity, attribute usage, authentication and liability, see figure 1. SSEDIC has summarized the central tasks for these priority areas in the recommendations which are presented in the following sections. SSEDIC strongly believes that these priority areas should be addressed as a matter of urgency and in view of their impact on public-private cooperation, eID governance (including trust frameworks, regulation and privacy), standardization and education.

2 Encouraging Mobile eID eGov Services Adoption

Mobile eID is a key enabler for Banking, eCommerce, eGovernment and eHealth because of ubiquitous nature of mobile technology. It is therefore to be expected that in the future a majority of eCommerce and eGovernment interactions will be done via mobile devices. An increasing number of companies adopts a “mobile first” strategy by designing their products for mobile phones or devices before making correlate designs for traditional desktop and laptop computers. In countries where mobile eID solutions have been introduced for eGovernment (e.g. Austria and Estonia) uptake is fast and citizens show a clear preference for the mobile solutions. Where no national eID systems exist, states may consider to first deploying mobile ID and mobile signatures: a core part of the infrastructure - the end-user devices - are already widely deployed. It might, however, be necessary to negotiate free

[2] The following projects have been considered: ABC4TRUST, eCODEX, epSOS, e-SENS, FutureID, GINI, SEMIRAMIS, SPOCS, STORK, and STORK 2.0

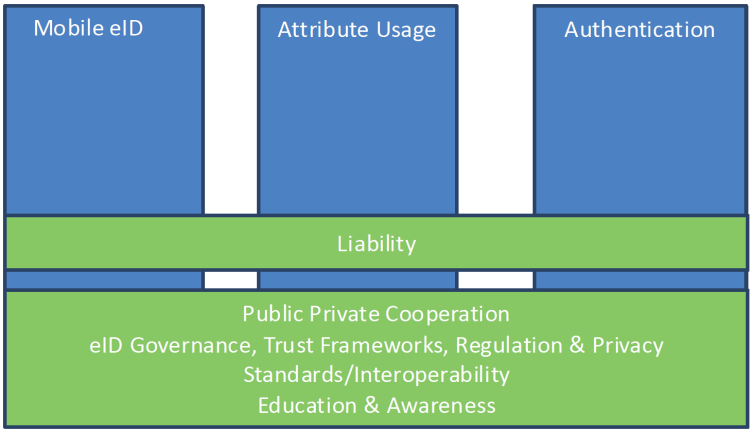

Figure 1: Key focus areas of SSEDIC recommendations

of charge access to certain critical services (similar to emergency calls). This will require close public-private cooperation. To ensure continued uptake and success of mobile eID solutions SSEDIC therefore makes the following recommendations:

2.1 Mobile eID recommendations

1. EC Member States should be encouraged to accept Mobile eIDs, (either server-centric or device based) as being an acceptable and notifiable credential for eGov use.
2. The EC should review Mobile eSignature / Wireless PKI standards relating to eIDs as soon as possible.
3. The EC should invest in research of suitable multi-factor authentication mechanisms using personal mobile devices.
4. The EC should invest in a coordinated approach to education in identity domains such as internet, telecommunications, citizens-eIDs, Travel, Health etc.
5. The EC should stimulate faster mobile eID and mobile signature take-up by rewarding fast adoption.
6. The EC should ensure that all citizens are able to access eGov services via mobile devices regardless of contractual relationship with mobile providers (similar to emergency calls).

3 Harmonizing Attribute Management and Exchange

The management and exchange of certified attribute grows considerably in importance: attribute assurance may in fact become the commercially most important area in digital identity management, with significantly more applications than those focussing on "identification". Attribute management poses several new challenges that have not yet been comprehensively addressed. These challenges include standardization [TBMS14, VPSK12], procedures and assurance measures for linking attributes to existing eIDs [MC12, STO13], managing hierarchies and dependencies in sets of attributes [AFNT04, ACN+02, TV97, TV99], verification of certified attributes, revocation, interoperability including semantic interoperability, privacy, attribute exchange/trade vs. user control and minimum disclosure. Public-private cooperation is highly desirable in the management and exchange of certified attributes.

Both public and private sector play important roles as attribute providers as well as relying parties. Close cooperation is therefore required to obtain user- and privacy friendly solutions across both sectors. Users need to be educated about user control mechanisms and the impact of attribute trade. A sensitive topic is the linking of attributes (including unique identifiers) to eIDs which can - also from the user's perspective - be useful in certain situations and undesirable in others depending on the context.

3.1 Attribute management recommendations

1. Linking: The EC should support the development and evaluation of procedures for linking attributes to eIDs while paying close attention to privacy threats.

2. Harmonization: The EC should initiate or revitalize the decision processes towards a harmonization of attribute semantics (semantic interoperability) and legal value.

3. Standardization: The EC should act on the need for standardization in the attribute management area; organize workshops and projects that bring together stakeholders to initiate standardization. The need for standards should be clearly communicated to policy makers.

4. Privacy: The EC should develop a normative framework to balance the user's right to privacy with the need of online service providers/e-government services to use, process and exchange user attributes. Attention should be paid on how this can be done adequately in an interoperability scenario. Special attention should be paid to attribute trade and reputational/behavioural attributes that are generated through the use of online services (like ratings on ecommerce websites).

5. Verification: The EC should study and evaluate procedures for efficient attribute verification. Appropriate mechanisms (technical and procedural) to ensure accountability and dispute resolution should be developed and implemented.

6. Dialogue: The EC should build on the interest in certified attributes by many e-commerce and industry stakeholders to gain their attention for the goal of creating a European eID ecosystem.

4 Rationalizing the choice of authentication assurance

Currently authentication is achieved by a variety of means. Authentication assurance frameworks are well established and understood (e.g. Stork QAA and NIST) and a number of relevant standards are available or under development [ITU08, ISO11a, ISO11b, ISO11c, ITU13, ISO13, ISO12a, ISO12b, ISO]. Many authentication assurance frameworks focus on traditional two factor authentication, but new data-enabled and probabilistic approaches to authentication are being developed. There are also approaches that allow levelling up an authentication method for example to allow a social networking ID to become higher assurance. The private sector seems open to alternative authentication technologies, especially those which offer reduced deployment and management costs.

At this stage it is unclear how effective these approaches are in reducing the cost of identity management and improving privacy. Further it is difficult to compare and assess such methods when mediating between different trust domains. Future standards therefore should not push a particular solution but should enable interoperability. New approaches to authentication need to support a wide range of uses and contexts and must work for small and large organizations while considering usability and user convenience as key factors [SSE12a].

4.1 Authentication recommendations

1. The EC should promote the establishment of an appropriate, easy-to-use framework for the assessment of authentication technologies including alternative authentication methods (so that they can be exploited where appropriate or discounted where not suitable.)

2. The EC should strongly promote internationally the establishment of an interoperability framework for authentication based on results and experiences like the ones provided by STORK, FutureID and other European projects on electronic identification.

3. The EC should encourage the development of services that are usable by the average citizen and complement this with appropriate education.

5 Liability

The issue of liability is fundamental for the usability of identity information since it plays a critical role in establishing trust. Assessing the assurance of identity information is closely tied to the associated liability. SSEDIC found that the European eIDAS regulation [Com12] as originally proposed was unclear with regard to important aspects regarding liability provisions [SSE12d]. The recommendations below point to some critical issues that must be addressed to create a viable liability framework for digital identity management in the EU. Some of the suggestions have been taken up in part in the position adopted by the European Parliament on April 3, 2014 [Par14]. Others should be considered in the delegated and implementing acts of the regulation.

5.1 Liability recommendations

1. Liability provisions in the eID and Trust Services Regulation need to be revised and updated, taking into account the different roles of identity providers in the Member States, who can be either public or private sector entities. It may therefore be necessary to consider separating the liability of Member States from identity providers, as they may be separate entities.

2. The liability provisions in the eID and Trust Services Regulation need to be reviewed to ensure that they are clear with respect to liability limitations and any possibility of liability caps. Various options are possible, ranging from no liability, unlimited liability to explicitly specifying liability caps in terms of financial amounts (possibly linked to eID quality levels); this topic must be carefully considered. The primary requirement is that liability implications are clear to anyone who relies on the trustworthiness of identities covered by the Regulation.

3. If EC policies on electronic identification intend to cover attribute provision as well (i.e. including in cases where end users will not be personally identifiable on the basis of the provided identity information), then a legal framework needs to be defined that also covers the responsibilities and liabilities of attribute providers. The currently proposed Regulation does not do this.

6 Implementation of recommendations

For the implementation of these recommendations SSEDIC suggests to consider the following aspects.

6.1 Stakeholder involvement

SSEDIC urges the European Commission to involve stakeholders from a wide range of sectors including the internet, telecom, finance, travel, postal services as well as the European Union Member States. In all these areas eID solutions are being developed or are in use which enable transactions in many societal domains like healthcare, finance, work and income, commerce and free movement of EU citizens.

6.2 Local adoption

The adoption of eID solutions for e-government and small businesses at the local level has too often been neglected. Residents have much more frequent interaction with local entities and businesses than with regional or national agencies. However, at the local level sufficient technical competence is not necessarily available, and often expensive changes to back-office procedures are required which do not generate immediate financial pay-offs. Especially municipalities and small businesses often lack the required financial and human resources to broadly implement even national eID solutions. Being prepared to accept credentials issued cross-border is an even tougher challenge and will likely be more expensive than cost saving for many small cities even in the long term.

6.3 International Cooperation and Standardization

European activities should further actively seek to engage with related efforts in other parts of the world like NSTIC/IDESG in the United States and the eID programs in Asia. Participating and obtaining a distinct voice in the world-wide dialogue on eID was found to be essential for the success of the SSEDIC project as well. SSEDIC recommends that representatives of past, ongoing (like STORK, STORK 2.0 and in particular e-SENS), and future EU projects send representatives to standardization organizations to explain and promote their technical results. These representatives should not only explore the relation between results of their projects and existing or evolving standards but also take an active lead in developing new standards and make all the necessary efforts to make a contribution to shape those standards already in discussion.

6.4 The end user

Over the course of the last 3 years, SSEDIC has conducted two large surveys on user attitudes towards eID and use of eIDs [SSE11, SSE12b]. Taking a step back from the results and asking what might be particularly noteworthy characteristics of the respondents to the survey we find that end users are

- Sceptical: expect to see clear benefits from the use of eID technologies
- Convenience seeking: use convenient, readily available tools (also in a professional environment) even if they have experienced or are aware of some associated security issues
- Internationally oriented: engage in cross-border online commerce and banking transactions
- With high expectations: expect their national governments and the EU to take action towards improving the current situation and to ensure cross-border usability of eIDs not only for public but also for private sector applications

These attitudes should be carefully considered when proposing digital identity management solutions to citizens.

7 Conclusion

The SSEDIC recommendations presented in this paper point to required actions in key areas that are essential to provide interoperable and convenient digital identity management solutions in a seamless digital Europe. The SSEDIC network has consciously decided to focus its recommendations on the four key areas shown in figure 1 to give an appropriate weight to its recommendations and the important consensus reached.

However, the SSEDIC thematic network has worked on other areas relevant for digital identity management and produced more than 20 white papers on eID and its use within the EU which contain important background material and further recommendation for specific eID related challenges for example in the areas of criminal justice, dematerialization, education, and business models. For an complete overview we refer the reader to ref. [SSE12c].

The European Union and its Member States are strongly encouraged to act on these recommendations as a high priority in a fast changing world-wide environment. While the eID programs in most European member states are government driven and focus on e-government applications other countries like the United States [Hou11] strive to enable the private sector to provide eID services. The private sector might be able to incorporate technological advances faster and be more sensitive to usability than government lead programs. However, if private sector applications should become the standard, governments run the risk of losing digital sovereignty to private service providers, identity providers and possibly to the governments in which jurisdiction these service providers are based. Other emerging risks include the requirement of mandatory authentication (explicit or implicit) where it is not strictly required leading to attribute aggregation and surveillance. These threats become particularly relevant in context of geo-tagging/tracking and in e-health related areas. The SSEDIC recommendation shall support the EU in recognizing, addressing, and overcoming such challenges.

The EU funded SSEDIC project concluded its work but many challenges as the ones mentioned above remain and require continuing efforts by think-tanks such as SSEDIC. The network SSEDIC created is prospering and will continue to grow as SSEDIC.2020. SSEDIC.2020 will expanding on existing SSEDIC themes, support the implementation of the SSEDIC recommendations, providing advisory and project validation services and promoting international liaison and knowledge sharing.

8 Acknowledgments

The authors would like to thank the entire SSEDIC community for their thoughtful work in drafting the SSEDIC recommendations presented in this paper and in particular Roger Dean, Hugo Kershot, and Jon Shamah as members of the SSEDIC management team and Eric Blot-Lefevre, Hans Graux, Jaap Kuipers, Herbert Leithold, Steve Pannifer, and Heiko Rossnagel for leading work streams and workshops that directly contributed to the development of these recommendations.

References

[ACN+02] Franco Arcieri, Elettra Cappadozzi, Paolo Naggar, Enrico Nardelli, and Maurizio Talamo. Coherence maintainance in cooperative information systems: the Access Key Warehouse approach. *International Journal of Cooperative Information Systems*, 11:175–200, 2002.

[AFNT04] Franco Arcieri, Fabio Fioravanti, Enrico Nardelli, and Maurizio Talamo. A layered IT infrastructure for secure interoperability in Personal Data Registry digital government services. In *Research Issues on Data Engineering: Web Services for e-Commerce and e-Government Applications, 2004. Proceedings. 14th International Workshop on*, pages 95–102. IEEE, 2004.

[Axe84] R. Axelrod. *The evolution of cooperation*. Basic Books, New York, 1984.

[Che05] Ramnath K Chellappa. Consumer's Trust in Electronic Commerce Transaction, Los Angeles, CA, University of Southern California, Marshall School of Business, 2005. 2005.

[Com12] European Commission. Regulation on electronic identification and trust services for electronic transactions in the internal market; available at http://eur-lex.europa.eu, 2012.

[Hou11] The White House. National Strategy for Trusted Identities in Cyberspace; available at http://www.nstic.gov, 2011.

[ISO] ISO/IEC. Information technology - security techniques - a framework for access management. Technical Report ISO/IEC CD 29146:Under Development, International Organization for Standardization, Geneva, Switzerland.

[ISO11a] ISO/IEC. Information technology – security techniques – a framework for identity management – part 1: Terminology and concepts. ISO/IEC 24760-1:2011, International Organization for Standardization, Geneva, Switzerland, 2011.

[ISO11b] ISO/IEC. Information technology – security techniques – a framework for identity management – part 2: Reference architecture and requirements. ISO/IEC 24760-2:2011, International Organization for Standardization, Geneva, Switzerland, 2011.

[ISO11c] ISO/IEC. Information technology – security techniques – a framework for identity management – part 3: Practice. ISO/IEC 24760-3:2011, International Organization for Standardization, Geneva, Switzerland, 2011.

[ISO12a] ISO/IEC. Information technology – security techniques –identity proofing. Technical Report ISO/IEC WD1 29003:2012, International Organization for Standardization, Geneva, Switzerland, 2012.

[ISO12b] ISO/IEC. Information technology - security techniques - requirements for partially anonymous, partially unlinkable authentication. Technical Report ISO/IEC 29191, International Organization for Standardization, Geneva, Switzerland, 2012.

[ISO13] ISO/IEC. Information technology – security techniques – entity authentication assurance framework. Technical Report ISO/IEC 29115:2013, International Organization for Standardization, Geneva, Switzerland, 2013.

[ITU08] ITU. Information technology - open systems interconnection - the directory: Public key and attribute certificate frameworks. Technical Report ITU-T X.509, International Telecommunication Union, Geneva, Switzerland, 2008.

[ITU13] ITU. Framework for discovery of identity management information. Technical Report ITU-T X.1255, International Telecommunication Union, Geneva, Switzerland, 2013.

[KRS] Michael Kubach, Heiko Roßnagel, and Rachelle Sellung. Service providersâ requirements for eID solutions: Empirical evidence from the leisure sector. In *Gesellschaft für Informatik eV (GI), Bonn: Open Identity Summit 2013 : 10.-11.09.2013, Kloster Banz, Germany*, page 69.

[MC12] Talamo M. and Schunck C.H. Re-thinking the Evaluation of eID Credentials to Simplify Interoperability. *European Journal of ePractice*, 14:51–62, 2012.

[Par14] European Parliament. European Parliament legislative resolution of 3 April 2014 on the proposal for a regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market; available at http://www.europarl.europa.eu, 2014.

[RZHM14] Heiko Roßnagel, Jan Zibuschka, Oliver Hinz, and Jan Muntermann. Usersâ willingness to pay for web identity management systems. *European Journal of Information Systems*, 23(1):36–50, 2014.

[SSE11] SSEDIC. SSEDIC eID adoption survey, SSEDIC Deliverable 2.3.1; available at http://www.eid-ssedic.eu/deliverables.html, 2011.

[SSE12a] SSEDIC. Consumer Facing Authentication Assurance, SSEDIC Deliverable 4.2.1; available at http://www.eid-ssedic.eu/deliverables.html, 2012.

[SSE12b] SSEDIC. SSEDIC 2012 eID adoption survey 2.3.2; available at http://www.eid-ssedic.eu/deliverables.html, 2012.

[SSE12c] SSEDIC. SSEDIC recommendations & roadmap, SSEDIC Deliverable 6.3; available at http://www.eid-ssedic.eu/deliverables.html, 2012.

[SSE12d] SSEDIC. A summary swot analysis for eid in europe under the proposed regulation, SSEDIC Deliverable 5.2.1; available at http://www.eid-ssedic.eu/deliverables.html, 2012.

[STO13] STORK2.0. STORK2.0 Deliverable 3.2; available at https://www.eid-stork2.eu/, 2013.

[TBMS14] Maurizio Talamo, Maria Laura Barchiesi, Daniela Merella, and Christian H Schunck. Global convergence in digital identity and attribute management: Emerging needs for standardization. In *Proceedings of the 2014, ITU Kaleidoscope Academic Conference: Living in a converged world-Impossible without standards?, St. Petersburg, Russia,10.1109/Kaleidoscope.2014.68584752014*, pages 15–21. IEEE, 2014.

[TV97] Maurizio Talamo and Paola Vocca. A data structure for lattice representation. *Theoretical Computer Science*, 175(2):373–392, 1997.

[TV99] Maurizio Talamo and Paola Vocca. An efficient data structure for lattice operations. *SIAM journal on computing*, 28(5):1783–1805, 1999.

[VPSK12] F Veseli, P Paillier, J Schallabock, and I Krontiris. D8.4 architecture for standardization v1; available at http://www.ec.europa.eu, ABC4Trust, 2012.