

SSEDIC second year: presenting results relevant to universities

Victoriano Giralt¹

¹Central ICT Services, University of Málaga, Málaga, Spain, victoriano@uma.es

Keywords

eID, electronic identity, Digital Agenda for Europe, SSEDIC, survey, results.

1. ABSTRACT

SSEDIC (Scoping a Single Electronic Identity Community) has entered its third year helping the European Commission (EC) to create a common view of the electronic identity landscape as input for the 2020 Digital Agenda for Europe (DAE). The results from the second year of work have recently been reviewed by the EC and published in the SSEDIC web site (<http://www.eid-ssedic.eu/>). Although there are seven published documents this year, we would like to focus on three of them that are of higher relevance to Universities: results of the second SSEDIC eID survey (which has got a significant level of input from the Higher Education community), the Authentication Standards Paper and, specially, the document on eID in universities. The main aim of the presentation is raising awareness of these materials among the University IT community.

This second year work has used the input from the first year review, presented at last year's EUNIS congress in Vila Real, and its review results will be the stepping stone to the last year of work. We would like to have the views of the University IT community in order to improve SSEDIC knowledge of electronic identity in Higher Education and thus provide a better input to the DAE.

2. SSEDIC eID SURVEY

SSEDIC consulted 1,000 respondents residing mostly in the European countries. Unlike the Year 1 SSEDIC eID expert survey, the Year 2 was designed to reach for a wider public as recommended to the SSEDIC consortium during the first project review. The survey produced valuable insights regarding the different types of eID credentials used by a wider public when proving the electronic identity on the Internet (including the frequency of their use, the way the credentials were obtained, and reasons for not using some types of eID credentials), users opinions on the necessity and goals of eID regulation at European as well as national level, eID federation and privacy issues, cross-border online use of eID, and secured exchange of sensitive documents via Internet. Even though the Y2 survey was aimed at wider public than the Y1 expert survey, the methodology and several parts were maintained or slightly reformulated in order to remain comprehensive also for non-experts. This attitude allowed the comparison of the results of both surveys and thus made the insights even more valuable. In general, the findings of both surveys were consistent and opinions of the general public confirmed the last year's experts' recommendations.

3. AUTHENTICATION STANDARDS

This paper contains interesting information about electronic identity terms that are being heard more and more frequently in University IT environments, such as Levels of Assurance, Registration and Credential issuance, OpenID, OAuth, identity tokens and other *hot* topics. IT can be used as a starting point for those setting up (or updating) an electronic identity infrastructure in their universities.

The document also dedicates some pages to analysing important topics like comparing STORK and NIST views on levels of assurance or the views on eID from the British and Austrian governments.

4. eID IN UNIVERSITIES

This document has been compiled by the four Universities that participate in SSEDIC and tries to give an overview of the current situation with electronic identity and university credentials as well as a glimpse of what the future could bring.

Electronic identity, in Higher Education, has meanings that diverge from the industry ones, mainly due to the length of time electronic services have been available to members of the community and the very diverse ways used to access them. The most accepted meaning is some form of linkage from a real persona to a virtual cyber-self that requires some form of identity proofing at some point in the network and, often but not always, in the physical world. Once this linkage has been established, the person behind the cyber-persona gets identifiers that allow services and other persons to single out the owner and, maybe, some attributes that carry some extra information about the person. The oldest form of such identity could be an e-mail address backed by an account in a university owned multi-user time-sharing system. For a noticeable length of time, such identifiers were considered strong enough, and influenced many a view on how to express identity and relationship to an organisation.

These are the questions that the document tries to answer: What is the current situation? What is the role of eID? What are the **challenges** for the future? Are there **roadblocks** or potential *show stoppers* one should be aware of? What are the major **milestones** for the upcoming years?

5. OTHER DOCUMENTS

The SSEDIC network has produced other documents with diverse relevance to the University IT community but that constitute recommended reading to anyone dealing with any form of identity in the electronic world these days.

These documents are “eID deployment in AT, BE, DE, FI, IS, and SE”, “Distributed Identity Infrastructure: The Target Vision”, “Regulatory findings” and “Business Models for eID”

6. REVIEW RESULTS AND FUTURE WORK

The project results review from the EC experts has been positive and all documents have been accepted for publication. Then, the reviewers recommend actions for the final year that SSEDIC will do its best to follow, with as much input as possible from as a broad community as possible. The main point for year three are: fact-finding and analysis followed by clear recommendations to stakeholders and close watch of the massive rise of device based eID.

7. REFERENCES

Giralt, V., Kerschot, H. & Shamah, J. (2012) SSEDIC: Building a Thematic Network for European eID. EUNIS Congress. Vilareal, Portugal.

NIST Special Publication 800-63-1, Electronic Authentication Guideline, December 2011. Retrieved April 3, 2013, from: <http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf>

STORK Deliverable 2.3, Quality authenticator scheme, March 2009. Retrieved April 3, 2013 from: https://www.eid-stork.eu/dmdocuments/public/D2.3_final_1.pdf

8. AUTHORS' BIOGRAPHIES



V. Giralt is the systems manager for the University of Málaga. Graduated as an MD from University of Málaga in 1986, and became a member of the University IT team in 1987 as a programmer. Has worked as a programmer for the University and systems administrator both for the International University of Andalusia (1990-1995) and the University of Málaga. Chairs the technical committee of the Confia Identity Federation for the Andalusian public universities and the Groningen Declaration Executive Committee. Member of the steering committee of RS3G EUNIS task force, member of the European Committee for Academic Middleware, member of the TERENA EMC2 task force, acting as co-chair during 2012, member of the RedIRIS identity task force, member of the SSEDIC EU expert network on electronic identity.