DOI: 10.7250/eunis.2013.044

University Information Systems and the need for strong authentication and authorisation

Paúl Santapau[1], Vicente Andreu Navarro[2], José Gumbau[3] and Andrés Marzal[4]

[1]Technology Innovation Specialist, santapau@uji.es.
[2]Senior Technology Innovation Specialist, andreuv@uji.es.
[3]Head of Office for Planning and Technology Forecast, gumbau@sg.uji.es.
[4]Vicerector of Campus, Infrastructures and New Technologies, Universitat Jaume I, Spain, Andres.Marzal@uji.es.

Keywords
Authentication, Authorisation, STORK, STORK2.0, ISO 27000.

1. ABSTRACT

Corporate academic Information Systems have faced, in the last years, a growing need for meeting high demanding standards for interoperability, transparency, open access, enhancement of learning and research IT infrastructures and applications, cross-border data exchange, etc. All these aspects of IT allow adding an unquestionable value to university information systems. They are not any more internal and isolated systems managed by a few computer experts and used by a limited number of people in the academic community, but open and accessible tools that a wide variety of users may access.

2. AUTHENTICATION AND AUTHORISATION AT UNIVERSITIES

But this added value is not for free. A rising concern in security of information systems has spread not only among IT specialists but also between the governing bodies of universities, and what is maybe more relevant, among users. Data protection legislation, national rules on IT, standards such as ISO 27000 and others have become frequent discussion topics during high-level management meetings. Security begins to be regarded more as a crucial strategic asset than as a purely technical issue. And a particular aspect of security, identity management, has gained relevance when dealing with open IT academic environments. Proper identity management contributes to guarantee confidentiality (by allowing only concrete people to access the information), integrity (by guaranteeing that data cannot be arbitrarily modified), authenticity of data (by providing reliable proof of the origins of the information) and traceability.

In Spain, only a small group of Universities has considered the possibility of developing Information Security Management Systems based on the ISO/IEC 27000 standards family, but all public universities are currently concerned about the implementation of the security measures defined in the ENS (the National Security Scheme that all public bodies must accomplish in order to guarantee the security of their data and IT infrastructures) and all the academic institutions are obliged to comply with, in terms of IT security, the national legislation on personal data protection. All these frameworks consider, to some extent, the need for the implementation of strong authentication and authorisation mechanisms.

In order to illustrate the above mentioned need and the way used by some universities for approaching a solution for the challenge that it poses, this article will describe the mechanisms designed and implemented for facilitating strong authentication and authorisation in the university services and will analyse them from two different perspectives:

- Technical complexity.
- Legal background.

The initiatives covered in the article focus, from the point of view of University Jaume I, in real-live collaborative solutions such as national identity federations (RedIRIS SIR) or cross-border pan-European projects (STORK), and will describe also the requirements of the services in terms of authentication, linking them to different levels of reliability based on standards (QAA level in STORK, future ISO 29115 standard or NIST 800-63).

3. CROSSBORDER INITIATIVES FOR AUTHENTICATION AND AUTHORISATION

Finally, the article describes a solution beyond authentication for the trusted exchange of identity attributes, and describes how this problem will be tackled in STORK2.0.

To illustrate that solution, we provide Figure 1 in which a classification of attributes has been established based on a three-layer scheme. The first basic layer would represent the attributes that a given user needs to identify him uniquely; these attributes are Name, Address, Date of Birth, etc. The second layer would include more advanced attributes that the user could use to validate things, that is, answering questions like: Do you have a degree in mathematics? Are you enabled for food handling? Can you drive in a given country? Even the level of a given language could be requested within the context of this scheme.

Finally, the third layer or group of attributes would represent those attributes that are related to a specific business sector like, for example, the academic life in which someone can challenge a user to provide his position as a professor in a given university, if a given subject has been passed with a good grade. This last layer could be extended to every single business sector in which user properties could be classified and provided.

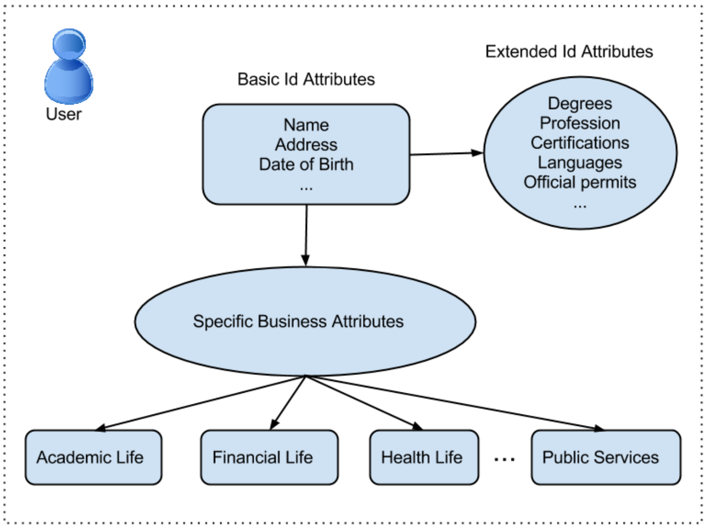

Figure 1. Advanced attribute exchange schema.

Secure idenTity acrOss boRders linKed (STORK) was a project co-funded by the European Commission as a part of its Competitiveness and Innovation Programme (CIP) in order to address, in a cross-border scenario, the identity management problem. STORK project came to its end in 2011 and given the success and the possibilities it exposed to the European Commission, a new proposal to continue and extend its objectives was proposed. This proposal is STORK2.0 that extends the objectives of STORK by adding extended attributes for authorization purposes.

STORK 2.0 goes even beyond and proposes the implementation of solutions for four scenarios in which business specific attributes are required:

- eLearning & Academic Qualifications
- eBanking
- Public Services for Business
- eHealth

For each one of these pilots, a set of attributes would be identified and established to be transferred within the common infrastructure following the aforementioned schema.

4. REFERENCES

Andreu, V. Kolbitsch, J. Ribeiro, C. Oreglia, M. Mahlapuu, L. (2009). STORK D6.3.1 Student mobility – Functional Specification. Retrieved May 17, 2013, from: https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=969

DOI: 10.7250/eunis.2013.044

Hulsebosch, B. Lenzini, G. and Eertink, H. (2009). STORK D2.3 - Quality authenticator scheme. Retrieved May 17, 2013, from: https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=577

RedIRIS (2013). RedIRIS - Spanish Academic and Research Network, Retrieved May 17, 2013, from: http://www.rediris.es/index.php.en

RedIRIS (2012). RedIRIS SIR - The RedIRIS Identity Service. Retrieved May 17, 2013, from: http://www.rediris.es/sir/index.html.en

5. AUTHORS' BIOGRAPHIES

Paúl Santapau works as a Technology Innovation Specialist at the Office for Planning and Technology Forecast of the Universitat Jaume I. He specifically works for the Technology Innovation Lab (TecLab). He has contributed to notable projects like Clauer, CryptoApplet, jXAdES, the adoption of an Information Security Management System (ISMS) and the European Large Scale Projects STORK and STORK2.0. He holds a CISSP certification from ISC2.

His main interests are Software Development, Information Security, Network Security and Project Management.

Vicent Andreu works as a Senior Technology Innovation Specialist at the Office for Planning and Technology Forecast of the Universitat Jaume I. He graduated in computer science from Universidad Politécnica de Valencia and obtained MSc in Knowledge and Information Society at Universitat Oberta de Catalunya. He was the coordinator of the Student Mobility Pilot in STORK project and currently he is working on Security Management, Data Protection and coordinates the eLearning and Academic Qualifications pilot within the context of the European Large Scale Project STORK2.0.

His main interests are ISMS, Risk Management, Data Protection and Privacy, eAdministration and Technology Surveillance.

Jose Pascual Gumbau Mezquita is the manager of the Office for Planning and Technology Forecast of the Universitat Jaume I and the Technology Innovation Lab (TecLab). He is an associate professor of the Computer Science and Artificial Intelligence department. He holds a CISA certification from ISACA and coordinates the IT Governance group of the Spanish Universities in the context of the TIC sector of the Board of Spanish Rectors.

His main interests are System Design, Innovation, Management and Project Methodologies, Information Systems Audit and IT Governance.

Andrés Marzal Varó graduated in Computer Science and Doctor on Computer Science from Universitat Politécnica de Valencia. He became a titular lecturer at Universitat Jaume I (UJI) in 1996. He has coordinated several projects related with Information Systems in UJI. The most notable are: the degree information system (LLEU) and the promotion of the Open Knowledge. He has been researching for more than 18 years and teaching for more than 15. He has published more than 60 publications in journals, books and international congresses and has lead several research projects. He has taken part in several committees within the university bodies. He has also been awarded with the I prize for the Teaching Excellence by the Social Council of UJI.