

## **SERVUS@TUM: USER-CENTRIC IT SERVICE SUPPORT AND PRIVACY MANAGEMENT**

Silvia Knittl<sup>1</sup> and Wolfgang Hommel<sup>2</sup>

<sup>1</sup> Technische Universität München, Dept. of Computer Science, Boltzmannstr. 3, 85748 Garching, Germany, knittl@tum.de

<sup>2</sup> Leibniz Supercomputing Center, Boltzmannstr. 1, 85748 Garching, Germany, hommel@lrz.de

The Technische Universität München (TUM) has been awarded as one of three German elite universities. Parts of the associated funds and the recently introduced tuition fees are invested in organizational development targeted at better support of students, researchers, and guests, as well as placing them in control of the use of their personal data in the growing number of inter-organizational projects and services. In this article, we first present the concepts and current realization status of our university business process driven recentralization of the IT service support; as many essential parts of TUM's IT infrastructure are handled by the Leibniz Supercomputing Center, which is the common computing center of the higher education institutions in the Munich area, emphasis has been put on cross-organizational processes. Then, we present a user-centric privacy management tool that has been implemented for the Shibboleth middleware and enhances the users' control of their personally identifiable information. A discussion of the synergies enabled by both user-centric approaches concludes.

Previously, service support has been highly decentralized at TUM; for example, depending on service, faculty, and type of customer (e.g., student, staff or guest), different support email addresses had to be used. Users often did not know whom to contact, so incident reports and change requests had to be forwarded, sometimes even multiple times, until the appropriate administrator could respond. Based on an analysis of the former deficiencies, formal support processes based on ITIL were introduced and supported by suitable open source tools; as the Leibniz Supercomputing Center already operated a well-established service desk based on commercial software, organizational integration as well as technical compatibility were major concerns. The ultimate goal is to support this recentralization by a seamless integration into the results of project IntegraTUM, which has been reported about at EUNIS 2006 and focuses on directly involving each user in the management of her personal data via self services [1].

In this context, the inter-organizational exchange of user profiles as enabled e.g. by Shibboleth obviously leads to new requirements concerning privacy management. Shibboleth supports so-called Attribute Release Policies (ARPs), by which one can specify which user attributes (such as name and email address) may be sent to which services. We show that the proprietary ARP language used by Shibboleth has a rather limited expressiveness: it is suitable for simple scenarios, but has several desiderata when it comes to the complex real-world applications. We have built a new ARP engine based on a standards-compliant XACML policy decision point. Now, XACML policies can be used to precisely specify which services may request which user attributes for which purposes under which conditions and obligations. Obligations, for example, include log files of attributes requested by service providers, and thus enhance the users' view of how their personal data is being used by service providers. Several examples of the improvements over Shibboleth's built-in ARP language are given and discussed; the source code of our prototype is available for download from our website.

[1] L. Boursas, W. Hommel: *Efficient Technical and Organizational Measures for Privacy-aware Campus Identity Management and Service Integration*, EUNIS 2006, Tartu, Estonia