
IDENTITY MANAGEMENT SOLUTIONS IN HETEROGENEOUS LEARNING ENVIRONMENTS

*Stephan Graf, Technische Universität München
Ivan Gergintchev, Technische Universität München
Sabine Rathmayer, Technische Universität München*

Introduction

The successful implementation of eLearning strategies is considered a major goal of German higher education institutions (HEIs). This goal includes an organisational concept of eLearning, as well as eLearning's technical integration into the existing information and communication technology (ICT) infrastructures. In the context of two main research projects, we at Technische Universität München (TUM) have developed user-customizable, technologically enhanced learning environments for different user groups of varying interests, preferences and expertise. Based on this research work in elecTUM (<http://www.tum.de/electum>) and ZePeLin (<http://www.zepelin.org>) we propose suitable identity management solutions corresponding to heterogeneous learning scenarios.

Quite often different campus management systems are deployed for the purpose of digital administration of students, staff, guests and alumni accounts at a single HEI. However, the establishment of a modern integrated IT infrastructure requires a holistic view of personal data used by web applications, such as learning platforms. Therefore most HEIs implement their own central identity information broker by providing tools for profile modelling, authentication and authorization data management, as well as by efficient search interfaces based on directory services.

To ensure eLearning services that serve both TUM and external institutions, we identified various requirements tailored to the needs of specific user groups. One such group consists of intra-university users, such as students and employees. Another group includes all guest users, such as exchange students who, unfortunately, are not registered in the central identity management system but requires seamless access to available IT services. A third group is one of external users who require access to certain IT applications (for example, due to course enrolment). Because these users are not regular university members, they are also not existent in the central directory. Aspects important to all groups are data protection and privacy. To meet user group demands, we analyzed a number of centralized and federated approaches to seamless user management. Here we present three customized solutions and describe their application areas, advantages and disadvantages. We will introduce our solutions in order of increasing level of functional complexity.

The simplest identity management solution for web applications (excluding local user management) is clock-controlled user import. We implemented it in the TUM's central learning management system. For the requirements of our external partners' HEIs we developed an integrated distributed solution, which is within the scope of ZePeLin and based on the Microsoft framework ASP.NET. Because we also aimed at building up a future-oriented, widely spread federated authentication and authorization infrastructure (AAI), we cooperated closely with Germany's National Research and Education Network (DFN) and the Leibniz Supercomputing Centre (LRZ).

Clock-controlled user import

The chosen identity management solution for CLIX, the central TU München learning management system, involved clock-controlled profile import and role assignment as well as user authentication against the directory service (as shown in Figure 1). The user database was imported in two ways: by using CSV files and via a direct data pull over LDAP. The first approach used a program that processes directory data for a nightly build of a file with new or modified personal records. To achieve

better performance results and lesser amount of transferred data, we agreed with the provider of the directory services on a customized scheme of the directory information tree. That scheme takes into account that applications based on a relational database cannot deal with multi-value attributes. Furthermore, we marked modified records with a flag, allowing for minimal, yet precise import over LDAP.

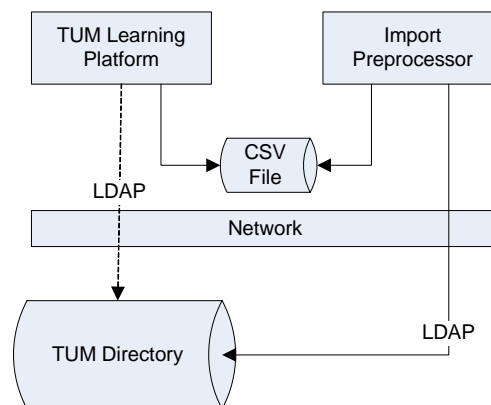


Figure 1: Clock-controlled user import in the TUM environment

Although this approach increases adjustment costs only marginally, it has some severe drawbacks. One of them is this solution's inflexibility caused by the application specific format of the data. Another one is data redundancy due to shadow accounts and privacy issues. A third drawback is risk of data inconsistencies which may occur since data is updated in regular intervals only. The latter risk implies increased administration effort and costs when importing a database of external users is needed.

Integrated distributed identity management

In October 2006, we launched the ZePeLin initiative to provide an organizational model as well as an integrated infrastructure for adaptable, modular, powerful and scalable learning management in Bavaria. Built on top of Microsoft Sharepoint Portal Server (MOSS) 2007, our web platform includes a set of basic portal functionalities plus the flexible integration of additional components for learning management.

Along with ASP.NET 2.0, Microsoft provides a customizable standard implementation of a membership model with basic functions, such as log-on or user lists. That model uses web forms or Web SSO to authenticate users against an identity management system that is not based on Windows or that is external. ASP.NET 2.0 includes a connector (provider) to a local MSSQL database and Active Directory domain. MOSS 2007 adds a connector for directory services from any manufacturer imposing some assumptions in terms of the source data structure, e.g. the existence of explicit domain groups, which cannot always be satisfied. The crucial point, however, is the opportunity to implement an own provider over an open interface to connect to arbitrary data sources. In addition to a membership provider, a role manager may also be registered. MOSS 2007 uses the standard ASP.NET role manager interface to gather group information about the current user. Each ASP.NET role is treated like a domain group by the authorization process.

To allow extranet usage in the hosted environments of the first three customers –the HEI of München, Regensburg und Deggendorf– we implemented our own ASP.NET membership system that achieves high-value integrated identity management. In Figure 2 this implementation is shown as “custom membership provider”. In our solution we dynamically retrieve membership data for a user from the directory service of each HEI on the fly. We also support connections to multiple data stores for the same portal to enable shared courses, in particular those of partner institutions. Secure communication over LDAP SSL and adaptability constitute other main characteristics of this solution. Its disadvantage is server-side dependence on single-vendor software.

The main elements of our membership system are a membership provider and a role manager. The profile connector carries out the authentication against the directory of the HEI education, accesses user profiles and queries the data source with implicit wildcards according to various criteria through the implementation of the abstract `System.Web.Security.MembershipProvider` class of the ASP.NET framework. The only attributes that are required to be saved locally are the account name and the e-mail address. Management of other important ones, such as first name and surname, depends on the user's preference.

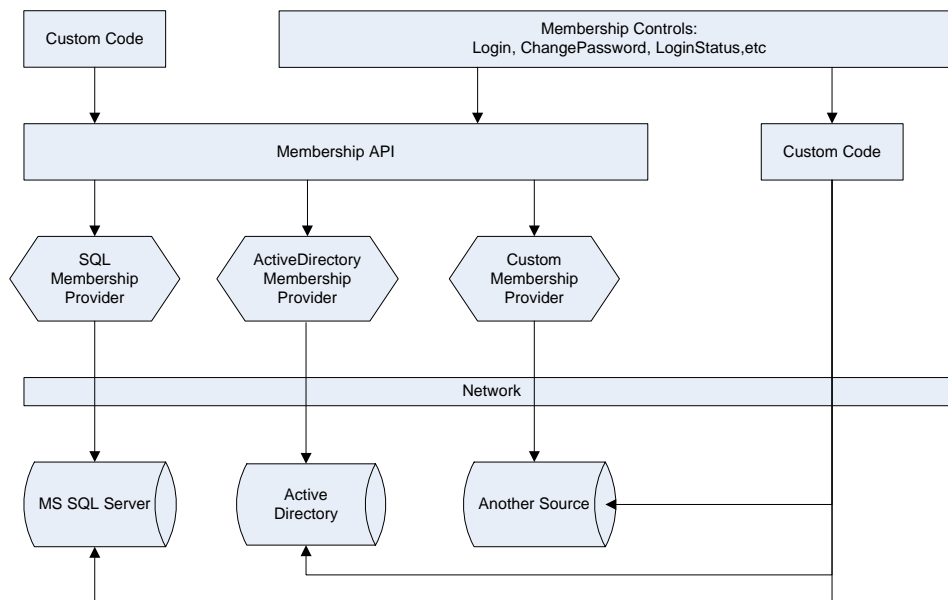


Figure 2: Membership system Architecture from [9]

The essential methods of the membership provider are the following:

```
// checks the credential of a user
Public Boolean ValidateUser (String username, String password)

// MOSS 2007 calls these methods to populate the user picker control
Public MembershipUserCollection FindUsersByEmail(String emailToMatch)
Public MembershipUserCollection FindUsersByName (String usernameToMatch)

// MOSS 2007 calls these methods to resolve user names and to get the user's
display // name
Public MembershipUser GetUser (Object providerUserKey)
Public MembershipUser GetUser (String username)

// MOSS 2007 calls this method to resolve user names in invitations
Public String GetUserNameByEmail (String email)
```

A core component of all three e-learning portals is our role manager which implements the abstract `System.Web.Security.RoleProvider` class. Since the directories of the HEIs include no groups, we derive the desired information by interpreting several user profile attributes and the directory structure. This approach allows us to build easily particular faculty's student groups and the group of all professors. The possible granularity of these groups depends mainly on the quality of the data in the corresponding directory. The following methods are relevant to MOSS 2007:

```
// MOSS 2007 calls this method to check the existence of a domain role
Public Boolean RoleExists (String roleName)

// returns every domain role of an user
Public String() getRolesForUser (String username)

// returns all domain roles
Public String() GetAllRoles ()
```

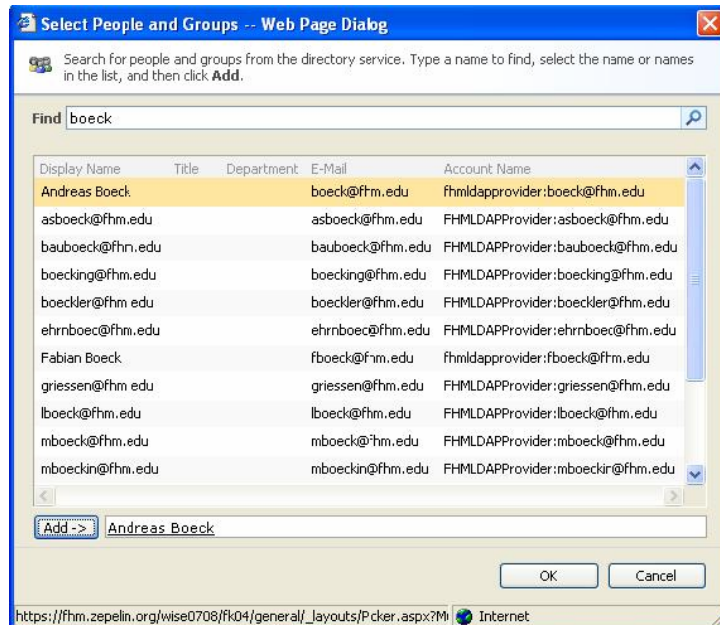


Figure 3: User picker dialogue in MOSS 2007

As mentioned above, data transfer takes place via encrypted SSL channels. Encryption affects performance of the connector directly. So an SSL bind with the directory in Regensburg claims over 500ms compared with about 200ms on an insecure channel. Another operational issue is the strong dependence of the portal's smooth operation on the availability of the remote directory's services. We address this weakness by applying a randomized algorithm for accessing redundant directory machines. In Figure 3 you can see the user picker dialogue which dynamically retrieves the necessary information of a user.

Our ASP.NET solution realizes distribution transparency of personal data for a single web application so it can be applied very successfully on this well defined domain. However, in order to achieve some kind of distribution transparency of personal data for different learning services and different domains a decentralized approach is required.

Authentication and Authorization Infrastructure – Federated Identity Management

Both contexts described above show an efficient solution for the particular scenarios. Due to different kind of limitations of the solutions a powerful and flexible identity management with federated authentication and authorization is needed. With the IntegraTUM [1] project, TUM therefore started to build up a flexible identity management a while back. This management is shown in Figure 4. A central meta-directory is fed by different source systems over an administration satellite. In this process data formats from the different providing systems are adapted and other administrative processes take place. The central meta-directory forms the TUM's consolidated data inventory and thus guarantees a high data quality. As necessary, connected destination systems may be fed in different formats and with a certain selection of attributes. Due to the diverse requirements of the destination systems, data formats will also be converted or the data supply correspondingly reduced.

Through the IntegraTUM identity management, a basis for the creation of an authentication and authorization infrastructure at TUM was formed. This structure enabled the implementation of a unified login for all systems, including the central LMS. Here, students may use the central identifier they receive on enrolment to log on to all connected systems. However, every system requires an individual login. Real value and palpable integration of the systems, however, are mainly achieved by implementing a Single Sign-On (SSO).

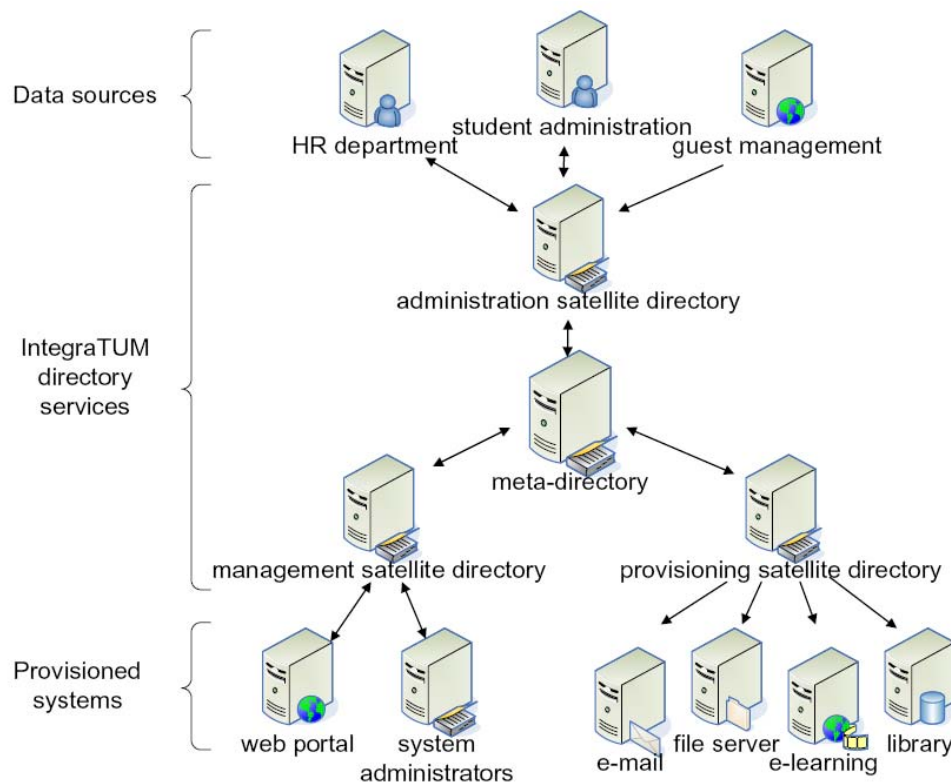


Figure 4: Identity management infrastructure of IntegraTUM (see[3])

For the implementation of a Single Sign-On, various studies have been carried out, analysing, classifying and surveying the application of multiple SSO at TUM ([2, 7], among others). Aspects such as standard conformity, flexibility, costs and integration in the TUM infrastructure were of high importance in this context. Out of this, a suggestion has been developed that has been presented to the TUM's IT technical committee and used as a basis for decision for the university's executive ([6]). Two different scenarios have been considered that were already mentioned at the beginning of the document.

We are talking about the different user groups. This is an essential aspect regarding the usage of an LMS. Internal user groups may be fed over the central identity management and thus have access to the system. This scenario could be covered by the identity management suggestion we presented first – the clock-controlled user import. The central identity management is an important criterion as a basis for an internal SSO. However, the necessary infrastructure for an SSO is missing between systems. Furthermore, we are confronted with various problems regarding guests and external users. In addition, connecting different external identity management systems proves to be quite difficult. These problems could be solved with the help of the second solution. Here, however, everything depended on a corresponding guest management and did not yet form the base for a standardized exchange of user information between the individual HEIs and thus no federated context. Thus, only a third solution was possible for an internal and external SSO in connection with the chances and possibilities of a federated authentication and authorization infrastructure.

Here, Shibboleth was the clear favourite. Thereby, the university's broad executive decided to build up and implement an AAI on the basis of Shibboleth. The solution just presented covers all previous scenarios. External users may receive controlled access to part of the resources, and all internal systems may be seamlessly connected via an SSO.

Shibboleth is a project of the Middleware Architecture Committee for Education (MACE) of the Internet2 initiative. Shibboleth is an open-source product and enables a standard-based internal and organisation-wide web SSO. For secure exchange, version 1.1 of the OASIS SAML standard is used. This also guarantees the compatibility with other web SSO systems. User information may be transferred and systematic decisions may be made for authorization (see [8]). An essential aspect of Shibboleth is the approach of "federated administration" and "access control based on attributes". This, in particular, satisfies the special situation of eLearning systems with an irregular number of users and thus forms a powerful and efficient solution. An in-house identity provider saves the relevant personal data and corresponding information for every user in different attributes. Through these attributes, a user has access to a resource (e.g. affiliation to an institution, membership in a certain group, etc.). The identity provider transfers information, so-called assertions, to a service provider –that is a service a user wants to use–, according to specified rules (attribute release policies). Here, identity information or only individual attributes may be transferred. We are talking about an extremely capable SSO system that meets the high demands of flexible identity managements. Figure 5 shows a graphical overview over the functionality of Shibboleth. TUM's decision for Shibboleth was not only made based on technological aspects, but also considering other projects.

Shibboleth is widely used at universities and libraries. As early as 2002, a preliminary study to build up an AAI was carried out by the SWITCH association in Switzerland. Groundwork for this was the well-established co-operation of different Swiss universities. Several systems were analysed according to certain aspects set beforehand. The main focus in Switzerland lay on the integration of eLearning systems. In the end, Shibboleth was the first choice (see [11]).

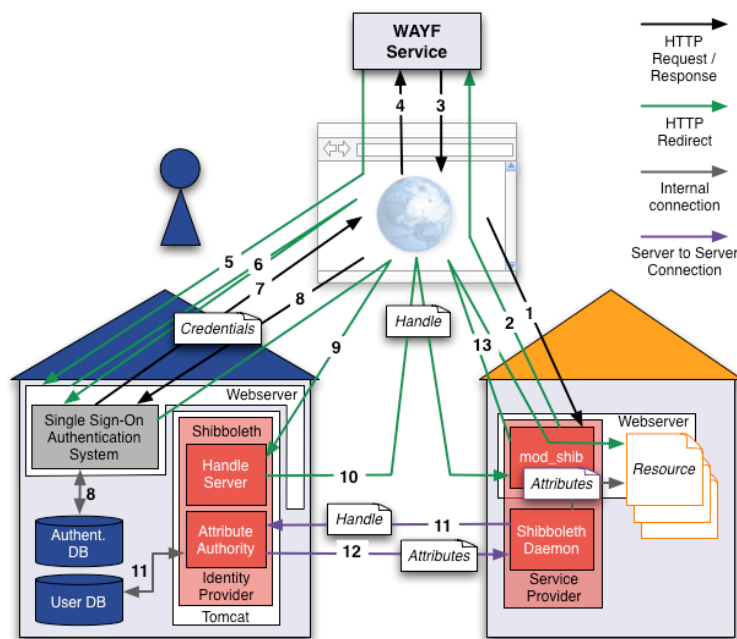


Figure 5: Functionality of Shibboleth (taken from [12])

In Germany, the "Verteilte Authentifizierung, Autorisierung und Rechteverwaltung (AAR)" project (Distributed authentication, authorization and rights management) started in 2005. It focuses on an SSO relating to library services. Thus, the main target lies in the optimization of the access to electronic contents. The technological groundwork is also formed by Shibboleth (see [13]).

Initiated by the AAR project, the DFN (Verein zur Förderung eines Deutschen Forschungsnetzes e. V., Association for the promotion of a German research network) decided in January 2006 to assume the co-ordination of an AAI on a national level. In this context, a new service, the DFN-AAI, was founded which has been in use since October 2007. This is a federation based on Shibboleth. The DFN administers the membership by terms of contract and provides a stable technical operation (see [4]).

So far, we have only explained the functionality and the TUM's decision for the implementation of Shibboleth. We have also mentioned the term AAI several times. In this context in particular, we have inserted Figure 6 for a better understanding. This graphic shows why a federated identity management

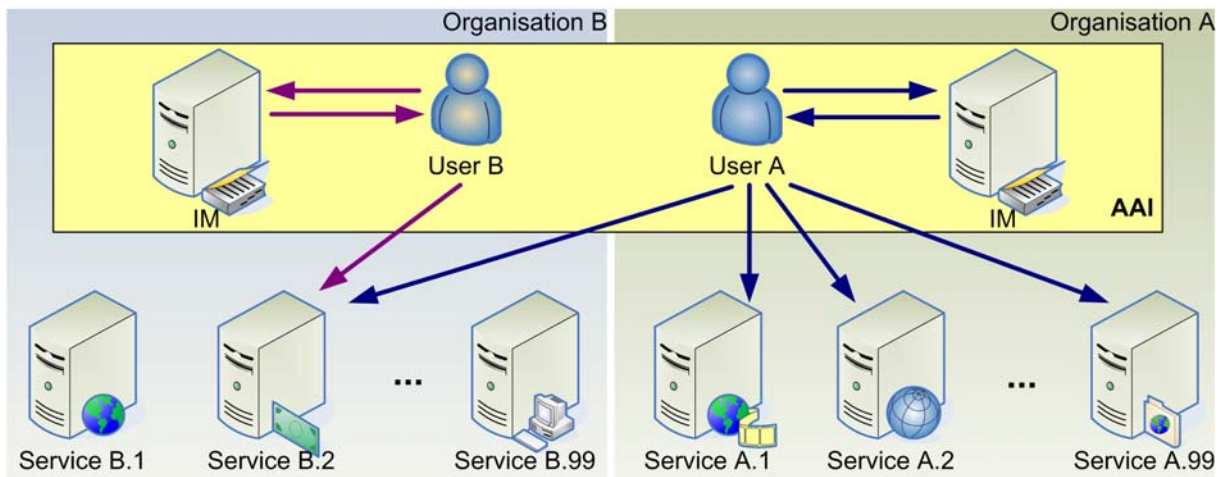


Figure 6: Overview Authentication and Authorisation Infrastructure

system is necessary within a heterogeneous user environment in relation to eLearning. Regarding TUM, one field of application is "Virtuelle Hochschule Bayern" (vhb, virtual Bavarian university). Students of other universities may access TUM courses after registering at vhb. The current process for this is as follows: a student registers at vhb, submits his identification to vhb (normally via mail; some universities, however, have implemented a proprietary online process suggested by vhb, such as TUM) and is then activated as a vhb user. This does not mean, however, that the student now has automatic access to the corresponding lecture at another university. For this purpose, vhb informs the respective lecturer to admit the student to his course (see [14]). The previous process –even in the proprietary version– is neither convenient nor reasonable in the long term. In this context, vhb also wants to join DFN-AAI. As shown in Figure 6, the entire organisational process would thus be considerably easier. Students would not have to register via vhb, but could use vhb as their own service provider which forwards the students directly to the courses of the individual universities. Thereby, a seamless service evolves which replaces complex paper processes and supersedes subsequent work at the individual universities.

Here, however, it is necessary to extend the previous DFN-AAI scheme appropriately. We have submitted the following suggestions: Title, sex, date of birth, place of birth, registration number, course, aspired degree and term. This information is required by universities for issuing certificates and enables a more efficient service in LMS systems for lecturers.

Here, the hitherto collected experiences regarding TUM's central LMS system and the knowledge from ZePeLin as well as the attributes used in both systems have been matched with the suggestions of the DFN-AAI (see [5]) and complemented according to the example of the Swiss SWITCH association (see [10]).

Conclusion

For the TUM's central learning platform a new authentication interface based on the position paper compiled by TUM is currently developed by the manufacturer. At present, the interface is still a prototype but has already been incorporated into the test federation of the DFN-AAI. TUM-specific data can already be transferred, and user may thus access the system. This is an important step to meet the demands of the Bologna process for a higher mobility of students and to position TUM on the global education market in the long term.

The presented identity management solutions are essential for the development of systems for web-based learning and co-operative knowledge management in consideration of the initiatives in the field of education and Web 2.0. All three solutions presented here were or are currently used at TUM since they represent an adapted solution for the respective user scenarios. In principle, the solution we presented last is to be applied at TUM, because it meets the requirements best. It is still important, however, to check the possibilities shown here for changes and accommodate appropriate improvements.

References

1. BODE A. *INTEGRATUM DFG ANTRAG*. 2004 [CITED 06.02.2008]; AVAILABLE FROM: [HTTP://PORTAL.MYTUM.DE/IUK/INTEGRATUM/DOKUMENTE/INDEX_HTML/CIO-TU_MUENCHEN.PDF](http://portal.mytum.de/iuk/integratum/dokumente/index_html/cio-tu_muenchen.pdf).
2. BONITZ R., *EINBINDUNG VON PORTLETS AUS DER ZENTRALEN LERNPLATTFORM CLIX IN DAS PORTAL DER TUM DURCH NUTZUNG VON WEB SERVICES UNTER BERÜCKSICHTIGUNG EINER SINGLE SIGN-ON STRATEGIE*, IN *FAKULTÄT FÜR INFORMATIK*. 2007, TECHNISCHE UNIVERSITÄT MÜNCHEN.
3. BOURSAS L., HOMMEL, W., *EFFICIENT TECHNICAL AND ORGANIZATIONAL MEASURES FOR PRIVACY-AWARE CAMPUS IDENTITY MANAGEMENT AND SERVICE INTEGRATION*, IN *EUNIS*. 2006: ESTONIA.
4. DFN. *DFN-AAI - AUTHENTIFIKATION AUTORISIERUNGS INFRASTRUKTUR*. 2007 [CITED 24.01.2008]; AVAILABLE FROM: [HTTPS://WWW.AAI.DFN.DE/](https://www.aai.dfn.de/).
5. GIETZ P., LIENHARD, J., MAKEDANZ, S., OBERKNAPP, B., PFEIFFENBERGER, H., RAUSCHENBACH, J., RUPPERT, A., SCHROEDER, R. *DFN-AAI TECHNISCHE UND ORGANISATORISCHE VORAUSSETZUNGEN - ATTRIBUTE -*. 2006 [CITED 11.02.2008]; AVAILABLE FROM: [HTTPS://WWW.AAI.DFN.DE/FILEADMIN/DOCUMENTS/VERTRAEGE/ATTRIBUTE.20061130.PDF](https://www.aai.dfn.de/fileadmin/documents/vertraege/attribute.20061130.pdf).
6. GRAF S., HOMMEL, W., *SINGLE SIGN-ON AN DER TUM: KÜHNE VISION, KLARE ENTSCHEIDUNG, NACHHALTIGE REALISIERUNG*. 2007: IT-FACHAUSSCHUSS DER TECHNISCHEN UNIVERSITÄT MÜNCHEN.
7. GRAF S., RATHMAYER, S., *VORSCHLAG ZU „SINGLE SIGN-ON“ – UNTER BERÜCKSICHTIGUNG AKTUELLER ENTWICKLUNGEN –*. 2007, TECHNISCHE UNIVERSITÄT MÜNCHEN, PROJEKT ELECTUM.
8. INTERNET2 M.I. *SHIBBOLETH PROJECT - INTERNET2 MIDDLEWARE*. 2000 [CITED 06.02.2008]; AVAILABLE FROM: [HTTP://SHIBBOLETH.INTERNET2.EDU/](http://shibboleth.internet2.edu/).
9. SCHWICHTENBERG H., *MICROSOFT ASP.NET 2.0 MIT VISUAL C#*. MICROSOFT PRESS DEUTSCHLAND. 2005.
10. SWITCH. *AAI ATTRIBUTE SPECIFICATION*. 2007 [CITED 12.02.2008]; AVAILABLE FROM: [HTTP://WWW.SWITCH.CH/AAI/DOCS/AAI_ATTR_SPECS.PDF](http://www.switch.ch/AAI/DOCS/AAI_ATTR_SPECS.PDF).
11. SWITCH, *AUTHENTICATION AND AUTHORIZATION INFRASTRUCTURE (AAI) PREPARATORY STUDY*. 2002.
12. SWITCH. *SWITCHAAI - EXPERT DEMO*. 2006 [CITED 07.02.2008]; AVAILABLE FROM: [HTTP://WWW.SWITCH.CH/AAI/DEMO/EXPERT.HTML](http://www.switch.ch/AAI/DEMO/EXPERT.HTML).
13. UNIVERSITÄTSBIBLIOTHEK F. *AUTHENTIFIZIERUNG, AUTORISIERUNG UND RECHTEVERWALTUNG (AAR)*. 2005 [CITED 07.02.2008]; AVAILABLE FROM: [HTTP://AAR.VASCODA.DE](http://aar.vascoda.de).
14. VHB. *VIRTUELLE HOCHSCHULE BAYERN*. 2008 [CITED 12.02.2008]; AVAILABLE FROM: [HTTP://WWW.VHB.ORG/](http://www.vhb.org/).

Authors

Dipl.-Inf. (Univ.) Stephan Graf
Technische Universität München
Faculty of Computer Science, I10
Boltzmannstr. 3, 85747 Garching
Stephan.Graf@tum.de

Dipl.-Inf. (Univ.) Ivan Gergintchev
Technische Universität München
Faculty of Computer Science, I10
Boltzmannstr. 3, 85747 Garching
Ivan.Gergintchev@in.tum.de

Dr. rer. nat. Sabine Rathmayer
Technische Universität München
Faculty of Computer Science, I10
Boltzmannstr. 3, 85747 Garching
Sabine.Rathmayer@tum.de