

IDMone makes the difference

1st Hendrik Eggers¹, 2nd Dr. Peter Rygus²

¹Friedrich-Alexander-University Erlangen-Nuremberg, Regional Computing Centre (RRZE), Martensstr. 1, 91058 Erlangen, Germany, Hendrik.Eggers@rrze.uni-erlangen. ²Friedrich-Alexander-University Erlangen-Nuremberg, Regional Computing Centre (RRZE), Martensstr. 1, 91058 Erlangen, Germany, Peter.Rygus@rrze.uni-erlangen.de.

Keywords

identity management, project report, lessons learned, openness.

1. EXECUTIVE SUMMARY

The paper reports on the lessons learned at German identity management project IDMone. To this end, it describes the wrong turns made and the ways to find out. The lessons are: the importance of project management standards, documentation of discussions, the way the project was managed itself, project planning and agile methods, business consulting, how to transform concepts to specifications and openness. These lessons should be more or less applicable to every profoundly changing IT project.

The paper also refers to the special circumstances in Germany - Bavaria - Franconia - Erlangen under which this project was conducted.

1.1. Background

The paper reports on the Erlangen Identity Management project IDMone, whose beginnings were presented at EUNIS 2007 (Eggers, 2007). The project IDMone, which was part of the agreement on objectives between the Free State of Bavaria and the University Erlangen-Nuremberg, has reached its first main target.

1.2. Conclusions

With IDMone, the RRZE started publishing all information and algorithms that could be applicable to more than only the Erlangen-Nuremberg problems on an open source basis. We are looking for partners willing to employ these developments and able to play an active part in further development to benefit all parties. This Openness in publishing and insights makes the difference.

2. History

After the start in 2006, the project was first presented to EUNIS at EUNIS 2007. (Eggers, 2007) Starting point was the agreement on objectives between the Free State of Bavaria and the University Erlangen-Nuremberg in 2006, which lasted until the end of 2008. This agreement defines a project for implementing identity management (IdM) under the aspects of e-government in paragraph 3.8.3. Shortly before, after long discussions with the Regional Computing Centre (RRZE), the university's board had realised the essential role of campus-wide identity management, as opposed to keeping managing users.

A project team was formed and new engineers were hired. As public service wages can't compete with common salaries this took about half a year so project kick-off was on November 7th 2006. In October 2008 the meta directory and a web-interface were launched, meeting the first main project target.

To illustrate the dimension, some facts on the University Erlangen-Nuremberg from 2006:

- 26.000 students, 6.000 employees, 10.000 guests
- second largest university in Bavaria and rank 17 in Germany
- since 1991 self-developed, ldap-based user management at the RRZE
- 16 mission critical systems working with independent user management from the directory named above
- "account view" instead of identity management
- And all the other well known problems growing over time in any IdM solution.

During the course of the project it became clear that the planned coverage could not be reached in the time originally estimated. Setting up a system with completely unknown software took more than six months learning time before it was understood in such a way that concrete conceptualizing could have been started.

After half the time the decision was made that the web-interface delivered with the identity management solution was neither meeting the special needs of Erlangen university, nor was it compliant with Bavarian accessibility regulations. In addition, the effort spent on customizing the application was increasing exponentially. So it was decided to develop a web-application on our own. Open Source and incorporating only the needed features, but doing so in a perfect fit. WAID (web administration for identity management) (Zhelev, Eggers, 2008) was born.

Another big work package was establishing and ensuring data quality. From other German projects, especially our colleagues from North Rhine - Westphalia, we knew that this would take time and effort. But there was no prior publication to reuse, nor a framework to utilise. So Krasimir Zhelev started researching and developed a drools-based solution that solves the Erlangen problems but is also open enough to be adapted to other organisations needs. (Zhelev 2008) He is looking forward to publish the results of his work at the end of 2009.

The project funding ended in December 2008 but fortunately the RRZE took responsibility and brought up a bridging finance plan until the new agreement on objectives is signed.

3. Lessons Learned

As presented at EUNIS 2007 the project was managed using a practical approach to PRINCE2. There is a "closing the project" step in every PRINCE2 project: the developed solution is brought to day-to-day business and project members take a look back, reflecting on what they have learned from mistakes made and successes achieved. The following sub-chapters describe the major lessons learned from project IDMonE.

3.1. Project management standards

The presented tools and techniques (Eggers, 2007, 2006) were key factors for the project's success. Fostering communication while harmonizing the work style of every project member was essential, but has worked only within the project itself. The RRZE as a whole did not benefit from these

standards, as they were only poorly introduced to the rest of the colleagues. The lack of information resulting from this caused many discussions and one-on-one lessons to integrate colleagues into parts of the projects. In the future, tools and standards have to be introduced to everybody through internal training which is already institutionalised for other areas.

3.2. Documenting discussions

Even with project management tools like weekly reporting through blog or having all documents online in a wiki, there was still a lack of documentation regarding the ongoing discussions. Many conceptual questions were discussed in several rounds, with sometimes changing participants. But in between there was no documentation of the discussion's status quo. In parts, flip-charts were representing the different thoughts and positions but no effort was made to bring these to the wiki. Some points and directions in discussions had a reasoning all participants of former discussions were aware of. But every new participant had to be introduced to the reasoning of the discussion group. So what we are still working on is a work policy stating how to document the state of discussion without much effort but in a form that everybody can understand quickly. The documentation of the outcome is not a problem, however. This is summarised in a specification which can be implemented more or less directly.

3.3. Project Management

The project board was very successful in backing the project politically and strategically. But in a way, there was too much involvement in operational decisions because problems were mostly reduced to this layer. The communication between the project partners had the problem that it employed a high level of detail. So the problem occurred that hard decisions - like the parts of the project that were started from scratch and self-developed - were prolonged due to misunderstood respect for the project partner. Project goals were changed without a complete risk analysis while other goals were not sufficiently operationalised. Risk management in the university is still a problem because it needs a complete rethinking from all participants. The problem with the insufficiently operationalised goals is now changed through less strategic goals with a clearly pointed out relationship to the operational goals.

3.4. Project planning / switch to agile methods

Starting with a classical project planning and a work break down structure quickly led to lag. The project plan was always behind and never current. This resulted from a great uncertainty in effort estimation. Tasks thought to be done in hours took days and others which were supposed to last weeks were done in days. For too long, there was the illusion to oversee the whole project duration in one plan and do the planning bit by bit. This changed with the decision to develop the web-interface on our own and make use of agile methods. Small tasks were defined and described in bugzilla - the famous bug-tracking tool that can be misused as task-manager as well - and then implemented. These were aggregated to work packages, that were addressing special problems or features. From this point onwards, the productivity of the team was rising, big steps were made and even colleagues were seeing progress in the project. This along with the insight that the current problems have to be addressed before further plans could be made, created an overall satisfaction with the project.

3.5. Business consulting and a case of schizophrenia

The hardest lesson learned was that commercial business consulting in identity management has no out-of-the-box solutions for German university role problems. The authors don't know if it is unique to Germany but the typical case of a secretary working for the department of biology in the morning and for the department of philosophy in the afternoon - we call this "a case of schizophrenia" - and that these two roles have to be divided strictly has not been solved yet. The same problem occurs with assistants working on funded projects which end with the follow-up project starting two months later. De-provisioning would condemn them to two months without system access. Solutions for these problems have to be developed and implemented with the different commercial products. The

authors are looking forward to an intensive exchange of concepts and solutions within Europe, addressing and solving these problems, not to re-inventing the wheel again and again.

3.6. Concepts to specifications

Due to lack of personnel and to shorten the time spend on writing we tried to skip the detailed concept after the blueprint to save time. But the system architecture became too complex to implement from the requirements right away. Even during the project, after switching to agile methods, the bug-tracking system bugzilla was incorporated more and more to specify tasks and to have a written history on growing specifications. Now, after the project has ended and was handed over to production, a new ruling for development requests was made. The processing is as follows:

1. requirements engineering/blueprint
2. dependency analysis de-pictured in a dependency chart - done by the developers
3. detailed plan of work packages
4. detailed concept for all work package
5. specifications for every task in the current work package - done by the client or by the developers or under moderation of the developers
6. cost/effort estimation
7. prioritisation by head of IT-Advisory board after consulting RRZE board of managers (publication of current tasks of the developers through internal reporting)
8. implementing what was specified
9. Deliveries (feedback, bug fixing) - changes in specification during this time have to be placed via a formal change request
10. handover/acceptance
11. roll-out through client or with support from the developers

Reporting will be done via e-mail if information is confidential else via blog.

3.7. Openness to the max

Transparency is the keyword for one of the major objectives of IDMone. Openness - reports via blog (IDMone Blog - unfortunately in German only) - open source tools like jidgen (jidgen) and jpwgen (jpwgen), aka. j*gen tools, - and scientific research play a major role. The paper "TOWARDS FIRST-AID IDM-TOOLKIT" - presented at this year's EUNIS - describes the j*gen-Tools in detail, so they are omitted here.

Reporting was essential during the progress of the project. Not only to keep all stakeholders in mind and informed, but also to draw attention to this profoundly changing project and even allow "lurkers" a close look on what's going on. Not to forget the colleagues from other organisations keeping an eye on what's done in Erlangen's IDMone. But to be frank a weekly report is very tough. A biweekly report seems more manageable for the project manager as he was not only in charge of managing but also involved in the operational procedures.

The decision to develop a web-interface for identity management - mentioned above - was a big turning point from product loyalty towards use of open source technology. The complete web front-end is open source based and components are about to be published (P&P Blog on software components). We hope to finish the work on it this year so further research results will be available at the end of 2009.

To summarise: this project was a big effort not only in terms of identity management itself but also and perhaps foremost in establishing a culture for managing large projects while changing organisational structures. Some more aspect - primarily environmental conditions - took effect on the success of the project IDMone. These will be discussed in the following chapters.

4. Consequent rethinking

One of the main objectives of the project was to implement a completely new Identity Management System instead of migrating bit by bit. This blank slate approach gave a good amount of freedom, making it possible to get away from an account centric view towards a consequent person based view.

4.1. Meta directory design

This affects the structure of the meta directory most of all. The context representing the university contains several sub-trees. Starting with the person sub-tree wherein the person objects are stored in a flat structure. Flat because a person can be associated with the university in multiple ways. These associations are expressed in affiliation objects within the affiliation sub-tree (flat storage as well). Every affiliation points to an organisational unit within the organisational structure sub-tree. A person object has at least one, up to many affiliations. The organisational units within the organisational structure sub-tree are stored in flat structure as well, to be prepared for relocation of organisational units. Any service provided to a person results from an entitlement. The entitlements are stored in a sub-tree grouped by services. Entitlements can be linked to a person object or an affiliation object. This way, a person can obtain services because he or she is member of the university in general or resulting from a specific membership to an organisational unit. This allows to implement "once per person" services - mostly free - and customized services to the special needs of specific organisational units.

The relationship between a person and its affiliations and a person and its (direct) entitlements are ensured by dn-based, two-way links. So every person object contains links to the related affiliations and entitlements and every affiliation or entitlement has a link to its owning person. This ensures integrity of the meta directory and will be expanded to almost all objects and their relationships.

The provisioning of the target systems is only based on the entitlements. So every service has its own entitlement object which allows the connector to provide the system with the data needed to offer services to an authorized user.

Within the web-front-end WAID the person logs in with an account generated as he or she joined the university. This user name stays constant throughout the persons life cycle within the university. Through the web-front-end a person could access information on his or her current affiliation(s) and entitlements. This is the first step to establish a single user name and a single login. Special user names are still generated to use specific services.

4.2. Centralism versus Federalism

The second objective was a centralized meta-directory instead of an intra-organisational campus federation. Unlike Munich (Hommel et. al. 2008) and Karlsruhe (Schell et. al., 2008), who prefer loosely coupled systems in a trusted environment, at IDMone - alike Salford (Kerr, Carassik, 2007) - the arguments pro and contra a central system where balanced.

Pro's:

- The RRZE has the motto to be "THE IT service provider" of the Erlangen-Nuremberg University.
This central role is de-facto in day-to-day business. All important server systems are hosted at the RRZE or at subsidiaries. Although all central IT systems are operated by the RRZE, some faculties or departments are running individual systems. Due to German data protection law, however, these systems, as long as they are operating with personal information, whether of students, employees or guests, have to be approved by the data protection commissioner who focuses on secure operations in a secure environment. And this can currently only be ensured while cooperating with the RRZE. To keep this central role as central identity management system is a key factor.
- A single system can be protected and secured more efficiently and effortlessly in comparison to many de-centralized systems. To reduce effort in system administration it is necessary to reduce the total number of systems as well.

Con's:

- A central identity management system is a single point of failure, as long as no counter measurements are taken to reduce this dependency. To fight this, all systems providing services to the customer have local user management. These are currently transformed to be provisioned by the identity management system. Only those attributes regarding a person needed by the target system to offer the service in a desired way are provisioned. This economy of data is one of the main principles in German, and, since recently, also in European data protection law. The identity management system talks to this target system while no target system is able to initiate communication with the IdM. This one way communication minimizes the chance for attacks on incoming connections to the identity management system.
- Only one organisation “owns” the information and is responsible for protection, security and quality.
As said above, the RRZE is THE central IT provider. During more than 40 years it has proven its quality and reliability. There is of course criticism from time to time but over all the university trusts its computing centre.

The system is implemented in a centralized way, but through the local user databases every system is independent in cases of system failure of the identity management system. Only changes are not recognized by the de-central systems. And the central web-application for identity management (short: WAID) is offering an interface which must be used by administrators in the computing centre as well as delegated administrators. Currently this is the only real single point of failure, because if the web-application crashes or loses contact to the meta directory, only the IdM super administrator is able to operate.

5. Preparing cost and activity accounting

One of the major objectives was to foster cost and activity accounting. Although the RRZE introduced cost and activity accounting in 1999, Bavaria will introduce cost and activity accounting for all public bodies in 2010, which brings some changes to be implemented. Cost units and accounts have been harmonised throughout the whole university. This put pressure on the RRZE as all existing services had to be summed up under these categories. To see clearly which services are still used and which ones could be suspended, transformed or put together with another project a service portfolio for the RRZE was started. This project is currently running and will not end before the mid of 2010. But the results of the project are essential for the implementation of affiliation based service packages with auto-approval or delegated approval of service requests. This means that in the future, members of the university will get services based on which affiliations they have, i.e. which organisational unit within the university they are members of. That way every organisational unit might have their own service package to offer to their members. Service requests beyond these packages have to be approved by the responsible manager of the requester. To measure the cost of these service packages and their utilisation for the proper fit to the customer a detailed log is needed storing information on who is using which service provided by what resource. Once per year the accounting will get the information about what services have been used. Currently the question of where the cost of offering a specific service or the cost for using the accounted service will be tracked is still open.

Nevertheless the RRZE is looking forward to more transparency regarding how essential to university life the provided services are and how high the costs emerging from offering these services are. No doubt this will help make clear the central role stated above and the necessity of having an IT service provider. The economies of scale in procurement and service providing are already well known within Erlangen and the Free State. Bring on the next “budget war” - we are prepared.

6. Outlook

Much work left to do.

In the next agreement on objectives between Free State and university in 2013, IT matters will again be included. We are looking forward to get a renewed sponsoring to continue the project. Otherwise there will be less personnel and less speed, but we will keep working on IdM! The new project - working title “IDMtwo” - will have the main objective of propagating the benefits of IdM to the

university. More and more systems will be connected to the IdM via provisioning. We're looking forward to spreading the word via web-based single sign on which is interesting for most locally service providers. It raises the attraction of web based applications enormously.

One big challenge is a concept for de-provisioning as described above. In scientific reality, it is normal that a funding for one project ends and the next funding starts two month later but the employed scientist - with an intermediate funding from elsewhere - wants to keep on working without changing permissions or being de-provisioned from single systems because of their lost affiliation to the officially ended project. We are confident to solve this problem but would be happy for any input on this.

We also hope to publish some WAID related components or WAID itself as open source. Currently we are looking for partners who are interested to use major parts of this web-application and are willing to participate in further development.

So perhaps there might be a chance to talk at EUNIS 2009 ff. on concepts for identity management and work together on a product independent framework to solve several problems which are specific to universities and therefore will be not addressed by commercial products.

7. REFERENCES

- Eggers, H. (2006). Identity management in 18 months - an example process. EUNIS 2006, Tartu.
- Eggers, H. (2007). Six months more - about another ambiguous identity management project. EUNIS 2007, Grenoble, <http://www.eunis.org/events/congresses/eunis2007/CD/pdf/papers/p97.pdf> (last visit 03.02.2009).
- Hommel, W. (2006). Efficient technical and organizational measures for privacy-aware campus identity management and service integration. EUNIS 2006, Tartu.
- Hommel, W. ;Knittl, S.;Pluta, D. (2008). Strategy and Tools for Identity Management and its Process Integration in the Munich Scientific Network. EUNIS 2008, Aarhus, <http://eunis.dk/papers/p1.pdf> (last visited 30.05.2009).
- IDMone Blog. <http://www.blogs.uni-erlangen.de/IDM/> (last visited 25.05.2009).
- jidgen. <http://jidgen.berlios.de/> (last visit 03.02.2009).
- jpwgen. <http://jpwgen.berlios.de/> (last visit 03.02.2009).
- Kerr, D.; Carassik, M. (2007). Creating capability for associate support through Identity Management, EUNIS 2007, Grenoble, <http://www.eunis.org/events/congresses/eunis2007/CD/pdf/papers/p176.pdf> (last visit 03.02.2009).
- P&P Blog on software components. <http://www.blogs.uni-erlangen.de/PP/topics/PPSA/> (last visited 25.05.2009).
- Schell, F.; Höllrigl, T.; Hartenstein, H. (2008). Federated and Service-Oriented Identity Management at a University. EUNIS 2008, Aarhus, <http://eunis.dk/papers/p89.pdf> (last visited 30.05.2009).
- Zhelev, K. (2008). Data Linkage in IDM Systems. http://www.rze.uni-erlangen.de/forschung/abgeschlossene-projekte/20080220_BRZL_AK_MetaDir_Data_Linkage_in_IDM_Systems-public.pdf (last visited 30.05.2009), BRZL AK MetaDir, Bamberg, 20.02.2008
- Zhelev, K.; Eggers, H. (2008). WAID 1.0. <http://www.blogs.uni-erlangen.de/IDM/stories/2554/> (last visited 25.05.2009).