# Identity Management at the University of Sheffield: a pragmatic approach

David Speake[1], Mark Taylor[2]

[1]CiCS, University of Sheffield, Sheffield S10 2HB,d.speake@shef.ac.uk. [2]CiCS, University of Sheffield, Sheffield S10 2HB,m.taylor@shef.ac.uk

**Keywords**
Identity Management, authentication, account provisioning.

## 1. EXECUTIVE SUMMARY

This paper is intended as a case study of how one large, complex institution dealt with the problem of replacing an ageing account provisioning system and developing an in-house identity management system, in a context in which, like many others in the UK HE sector, we had limited resources to bring the project to completion. The paper outlines how we succeeded in overcoming the problems to produce an effective working system.

### 1.1. Background

The University of Sheffield, which is a member of the prestigious Russell group of research-led Universities, has some 24,000 students and 6,000 staff. Some seven years ago, we identified the need to replace the ageing account provisioning system which was only capable of dealing with Novell accounts. It was clear that, in the near future, we would require a more functionally rich identity management system, capable of automating to a much greater degree the provisioning and management of users and computer accounts. Central to the decision to move forward was the awareness that the number and type of accounts was set on a steep upward curve. However, the main factor determining the approach which we adopted was the limited resources we had at our disposal to carry out the work.

### 1.2. Key Activities

The main aspects of the project implementation which are described in the paper include technical aspects of the development, the technical landscape, choice of technologies and integration with other administrative systems. We discuss the process of selecting a programming environment, and the rationale for in-house development. We also make reference to the 'soft' areas such as project and resource management and highlight a number of issues which may be of interest to a wider audience. We evaluate the successes and failures of the project, and consider the future of the system, now that commercial IDM systems are mature and readily available.

### 1.3. Conclusions

The case study concludes that despite some weaknesses in implementation, the decision to proceed with development of an in-house system was the only practicable one at the time. The decision was also timely because, without the creation of such a system, we would not be able to provision and manage effectively the very large numbers of accounts which we now have to deal with.

## 2. INTRODUCTION

The University of Sheffield, which is a member of the prestigious Russell group of research-led Universities, has some 24,000 students and 6,000 staff. Some seven years ago, CiCS (Corporate Information and Computing Services) identified the need to replace the ageing account provisioning system which was only capable of dealing with Novell and mail accounts. Registration for these accounts was handled in different ways, by different staff, using different levels of automation. There was no one source of student and staff data, nor were there effective mechanisms for ensuring that users' authorisation was appropriate after changes to their circumstances. The existing PC based registration system for access to Novell servers was old, unmaintainable, reliant on an ex-member of staff and no longer able to provide the flexibility necessary in a rapidly changing environment. The existing registration system for OES and other Oracle systems combined user registration with application administration functions, was written in a range of tools (some obsolete 16 bit Windows), was complex to use effectively and was not integrated with other registration systems. It was clear that, in the near future, we would require a more functionally rich identity management system, capable of automating to a much greater degree the provisioning and management of users and computer accounts. Central to the decision to move forward was the awareness that the number and type of accounts was set on a steep upward curve.

This paper is intended as a case study of how one large, complex institution dealt with the problem of developing an in-house identity management system, in a context in which, like many others in the UK HE sector, we had limited resources to bring the project to completion. The context is important for two reasons: firstly because it defined the parameters within which the project had to function, and secondly because our experience could be transferable to other institutions in similar circumstances.

The paper outlines how we succeeded in overcoming the problems to produce an effective working system.

## 3. TECHNICAL ENVIRONMENT

The University operates a large installation of Novell servers which provide file and print services to our population of some 30,000 users. MS Windows is the desktop client for most users, although there is a sizeable population of Mac users, and a somewhat smaller one of Linux machines. Over the lifetime of the project, a number of 'enterprise' applications have been introduced or become more important. These include our portal solution (which has been through two iterations of software platform), our VLE (WebCT Vista), learning management systems, document management system, SAP finance and HR systems, Reporting system and others. All of these systems, whether with a large user base like the portal and the VLE, or smaller populations like the LMS, require user maintenance functions.

## 4. RATIONALE FOR IN-HOUSE DEVELOPMENT

Proposals for the replacement of the existing account provisioning system grew out of the awareness that the existing system could not cope with the increase in computer services and accounts, but we were also aware that we did not know what the future would hold in terms of these services. While IDM systems available at the time could deal with some of the major commercial applications, they did not have the ability to link either with popular open-source systems such as those in use at the University, or with other non-windows based proprietary systems such as our CIS suite (developed by Oracle UK), or our Coda finance system. Integration with our administrative systems, both student and HR, were essential for proper management of users, and this was only possible with an in-house system. We therefore decided that only in-house development would give us the flexibility and future-proofing that we required. The approach also offered us a way of managing the necessary development despite very limited resources.

# 5. PROJECT IMPLEMENTATION

## 5.1. Choice of technologies

The previous system had been developed in Foxpro by a now retired member of staff, and we were concerned that a replacement should be developed using more widely adopted technologies. Having said this, the choice of technology platform was arrived at after several weeks evaluation and testing on all the platforms on which the system would need to operate: we had in-house skills in Oracle forms development and the Perl scripting language appeared to offer the necessary libraries – LDAP, networking, CGI and so on. Python and Java were also considered, but rejected due to OS incompatibilities and reliability issues. The database in use for the CIS systems was and is Oracle, and it was logical to add the extra tables necessary for the IDM to this database.

## 5.2. Project Implementation

The development of the CRIS system was something of a test case for project management techniques within CiCS. Until this point, systems development had either been carried out in the traditional data processing fashion – i.e. analyse, design, code, with separation of duties between functions; or entirely ad-hoc by one person with little reference to either users or methodologies. We decided that, because of the importance of the system and the non-traditional development technologies (perl/TCP/IP) it was essential to control the project formally.

To this end a project group was set up, consisting of members of CiCS with a stake in the outcome of the project, and a project manager appointed. The project management method used was a variant of PRINCE2 for smaller projects. The aim of the project was defined as:

"*To investigate, define and implement a system which will provide a unified method of registration for all current and future CiCS computer systems. This will provide a single point of contact in an accessible format for all CiCS operational staff involved in registration and be related to staff and student information held in other systems. Consideration will be given to the registration of authorisation information as well as authentication.*"

The project team consisted of a Project Sponsor (Deputy Director of CiCS) (p/t 0.01), a Project Manager (.05), two representatives of Customer Support Services (.05) and one technical representatives (1.0). Another technical representative was later drafted in to undertake the work on the Oracle forms front-end.

Detailed analysis and specification work started in the spring of 2001, and was mostly finished by December of that year. The system came to be known as CRIS, partly because it is an acronym for Computer Registration Integrated System, and partly because the old system was known as BOB. The first real programming work started during Autumn of 2001, early versions of the first perl programs were working in November, and by late April of 2002 a very early working version of the crisp system was up and running, which was able to administer CIS and Oracle accounts.

The final modules and the password synchronisation web page were completed during September of 2002 just in time for the deadline of Student registration. Student Registration was a severe test for the new CRIS system, and many bugs and design flaws were discovered and fixed during the registration period. It was only at the next year's registration process that most of the features now existing in CRIS were available, partly because of the lack of resource (only one programmer was available full-time to the project), and partly because the design itself changed as the team learnt more about what was really necessary for an effective implementation and the programmer learnt more about the technical aspects of the environment in which the system was being built. Further improvements to performance (primarily to cope with the rush at registration time) continued to made until two years ago.

Since 2005 activity in this area has moved from being a project to being one element of the normal business of CiCS ("Business as usual"). It is significant that only three years later, at a point where we are beginning to consider whether commercial solutions or indeed person-centric solutions are more apppriate for the future, have we fully realised the importance of the in-house development.

Review of the project itself was a somewhat informal process, with regular meetings of interested parties, but little in the way of gateway reviews or post-implementation review. This informality may in itself have contributed to the 'feature-creep' alluded to later.

## 5.3. Project outputs

The project outputs can be summarised as follows:

- A system design
- Effective testing
- Implemented system fit for purpose

A simple schematic of the system design can be represented by the diagram below:

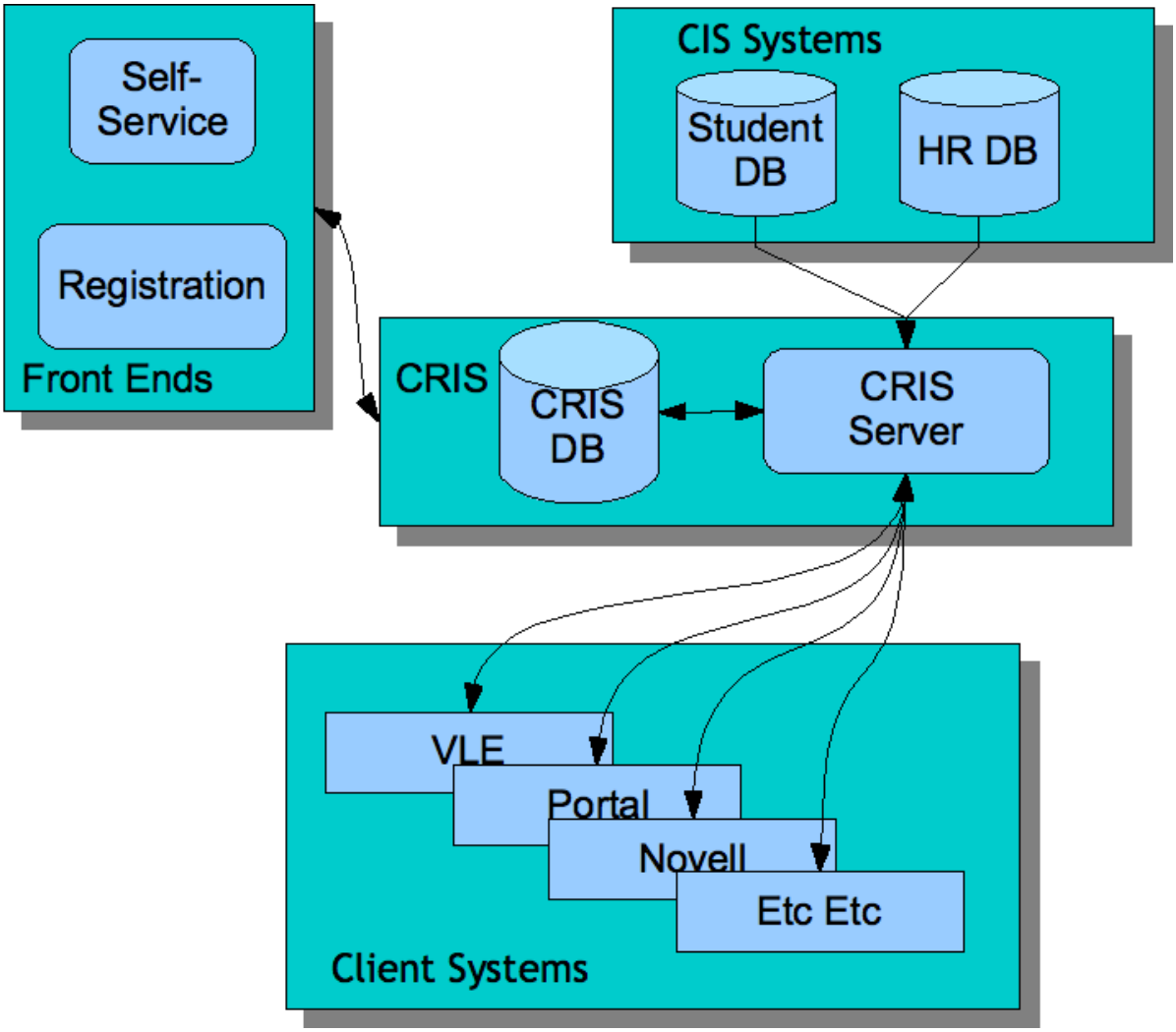


Figure 1

As can be seen, the CRIS server processes are driven from the HR/Student systems, and from the interaction with front-end processes. All communication between processes is over TCP/IP. The functions performed by CRIS are broadly as follows:

- Manual administration of users & computer accounts.
- Semi-automatic bulk creation of computer accounts, driven by lists of users.
- Administration of "loan" computer accounts used for short periods by temporary staff.

- Administration of email aliases.
- Administration of email delivery accounts.
- Administration of filestore allocations.
- Administration of account group memberships.
- Administration of account passwords.
- Synchronisation of passwords across all services, applications, and systems.

The following functions are performed by a web interface for end-users:

- Self-administration of computer accounts by end-users via a web page.
- Self-authorisation of computer accounts by new students via a web page.
- Synchronisation of passwords across all services, applications, and systems.
- Automated password ageing: a function has been designed (but not yet implemented) to perform co-ordinated password ageing across all services and applications, including those which do not themselves natively support password ageing.

The following functions are performed by a overnight batch housekeeping process:

- Automated deletion of computer accounts owned by staff & students who have left the university, driven by SAP & Student Registration system records.
- Automated suspension of computer accounts owned by students who are in debt to the university, driven by Student Registration system records.
- Automated deletion of computer accounts owned by non-contractual staff, driven by "review dates" specified when the users' accounts were initially created.
- Automated suspension of "loan" computer accounts used for short periods by temporary staff.
- Automated Ucard expiry.

## 5.4. Issues arising

The main issues which arose can be subdivided into technical issues arising from the design and build phase, and generic project management issues.

The technical issues included:

- *Burden of maintenance*. Development of an in-house system combined with the complexity of the CRIS system is such that, if the current developer were to move on, CiCS would face considerable difficulties in maintaining the code.
- *Security.* Problems implementing SSL transactions using the available Perl libraries meant that home-grown routines had to be developed. These are almost certainly not as secure as SSL.
- *Audit features*. Although transaction logs of all transactions are kept, there is currently no auditing of the correctness of the accounts – i.e. we don't know with certainty that only current authorised users have active accounts.

The project management issues included:

- *Inadequate resource management*. Because the project was almost entirely internal to CiCS, and members of the project team were outside the traditional development environment, there was a sense that resource was 'free', with the consequence that proper account was not taken of the costs of development.
- *Ever-vanishing finish point*. Inadequacy of resource, and the fact that the project had no budget assigned to it, meant that time scales were bound to slip. However, the slippage was perhaps more than could have been expected even given these factors. This extended timeframe gave rise to a number of problems in itself, such as loss of enthusiasm and commitment, and decreasing clarity about the original aims of the project.

- *Feature creep*. Owing to the extended timeframe for the project there was never a sense that the functionality desired had been achieved, and there were constant demands for new features which were not part of the original specification.
- *Lack of ownership within CiCS.* Although the project Sponsor was the deputy director of CiCS at the time, the project was still essentially invisible – i.e. recognition of its importance to the running of the University was limited, and therefore resource issues were not properly addressed.
- *Matrix Management.* Project Management and Line Management responsibilities were not clearly defined, and colleagues had difficulties in prioritising their day-to-day duties against their project work.

## 5.5. Successes

Despite the issues with the management and implementation of the development identified above, the project was a considerable success, and we are currently in a position to provide the University with the following facilities:

- All computer accounts are now normally created within 2 minutes of a request. Mail accounts take no longer than 30 minutes.
- Ability to have all accounts with synchronised passwords if desired. This is particularly important for single-sign-on access to systems through the University portal, and would not have been practicable without the rapid synchronisation possible through CRIS.
- Streamlining of computer account provisioning at student registration time. All student accounts are now pre-created and activated via self-service screens by the students themselves.
- CRIS allows for the bulk creation of accounts for existing users on newly implemented application systems, removing the burden of manual creation.
- The system is a valuable information resource for front-line support staff, providing a wealth of information about users of our computer systems.
- Over 200,000 accounts are now maintained and controlled by the CRIS system.

# 6. FUTURE DEVELOPMENT

## 6.1. In-house

As has been mentioned previously, a number of improvements to the system can be envisaged. As well as auditability, and automatic password ageing, we have considered the extension of the system to make it capable of dealing with authorisation within systems. This however, would be a major rewrite, and would require significant knowledge of individual application systems. It is not clear that this would be possible or practicable.

More generally we have to consider whether further in-house development is desirable. At the time of system design, only fledgling commercial systems existed. The situation now is very different. Many of the major vendors now sell (or give away) Identity Management systems. These offer, to a greater or lesser extent, the ability to integrate with major ERP systems, with directory services, and with a range of mail services.

## 6.2. Commercial Solutions

- Sun Identity Manager. This offering, which is now free, can provision accounts for a wide range of OS's, applications, and directories. It can be extended by means of custom-built resource adaptors to manage services which are not part of the core offering. It also has authorisation workflow, which means that the process of provisioning accounts for new

members of staff can be automated from from the point where the employee is entered on the HR system. Auditing facilities are also part of the package.

- Novell Identity Manager. This product offers similar functionality to Sun's IM, while relying on a Novell e-directory infrastructure for meta-data maintenance.

## 6.3. Futures

Person-centred identity management is only now beginning to become a reality. CRIS will have difficulties in dealing with a user-centric IM model, as will many commercial solutions.

# 7. CONCLUSIONS

Development of an in-house Identity Management system was the only practicable solution available to the University at the time. Commercial systems were in their infancy, and delay in implementation would have posed serious problems for the roll-out of new applications. While there were difficulties, both in terms of technologies and project management, the end result has been a major success, and it is now recognised that we have a system which will meet our needs at least until the next disruptive change in Identity Management becomes a reality.