



## JISC Final Report

Project Information			
<b>Project Identifier</b>	<i>To be completed by JISC</i>		
<b>Project Title</b>	Logins4Life		
<b>Project Hashtag</b>	#login4life		
<b>Start Date</b>	1 <sup>st</sup> January, 2010	<b>End Date</b>	31 <sup>st</sup> March, 2011
<b>Lead Institution</b>	University of Kent		
<b>Project Director</b>	John Sotillo		
<b>Project Manager</b>	Matthew Slowe		
<b>Contact email</b>	<a href="mailto:M.Slowe@kent.ac.uk">M.Slowe@kent.ac.uk</a>		
<b>Partner Institutions</b>	n/a		
<b>Project Web URL</b>	<a href="http://www.kent.ac.uk/is/projects/loginsforlife/">http://www.kent.ac.uk/is/projects/loginsforlife/</a>		
<b>Programme Name</b>	<i>Access and Identity Management Programme</i>		
<b>Programme Manager</b>	Chris Brown		

Document Information			
<b>Author(s)</b>	Matthew Slowe		
<b>Project Role(s)</b>	Project Manager		
<b>Date</b>	31 <sup>st</sup> March, 2011	<b>Filename</b>	L4L-JISC-FinalReport.docx
<b>URL</b>	<a href="http://www.kent.ac.uk/is/projects/loginsforlife/downloads/L4L-JISC-FinalReport.docx">http://www.kent.ac.uk/is/projects/loginsforlife/downloads/L4L-JISC-FinalReport.docx</a>		
<b>Access</b>	This report is for general dissemination		

Document History		
Version	Date	Comments
0.1	2011-03-14	Initial draft
0.2	2011-03-24	Revisions and additions
0.3	2011-03-30	Final revisions
0.4a	2011-04-28	Final draft for JISC review

## Table of Contents

<b>1</b>	<b>ACKNOWLEDGEMENTS</b> .....	<b>2</b>
<b>2</b>	<b>PROJECT SUMMARY</b> .....	<b>3</b>
<b>3</b>	<b>MAIN BODY OF REPORT</b> .....	<b>3</b>
3.1	PROJECT OUTPUTS AND OUTCOMES .....	3
3.2	HOW DID YOU GO ABOUT ACHIEVING YOUR OUTPUTS/OUTCOMES? .....	3
3.3	WHAT DID YOU LEARN? .....	4
3.4	IMMEDIATE IMPACT .....	6
3.5	FUTURE IMPACT .....	7
<b>4</b>	<b>CONCLUSIONS</b> .....	<b>7</b>
<b>5</b>	<b>RECOMMENDATIONS</b> .....	<b>8</b>
5.1	RECOMMENDATIONS FOR ACCOUNT LINKING SERVICE .....	9
5.2	LIMITATIONS OF CURRENT ARCHITECTURE .....	10
5.3	DEFICIENCIES IN CURRENT PROTOCOLS .....	10
<b>6</b>	<b>IMPLICATIONS FOR THE FUTURE</b> .....	<b>10</b>
<b>7</b>	<b>REFERENCES</b> .....	<b>11</b>
<b>8</b>	<b>APPENDICES</b> .....	<b>12</b>

## 1 Acknowledgements

The Logins for Life project was jointly funded by The JISC under their Access and Identity Management programme and the University of Kent. The project built on existing projects such as the Shintau<sup>1</sup> project [funded by JISC, which studied attribute aggregation and built the Account Linking Service], the PERMIS<sup>2</sup> project [funded by the EC ISIS programme, which built the first role based access control (RBAC) policy decision point (PDP)].

The project team is grateful for the assistance of a huge number of colleagues, students, alumni, ex-staff and associates from the University of Kent and other Higher Education organisations who agreed to be interviewed or who contributed in other ways to our research. In particular the Partnership Development Office who ran focus groups in local schools for us which allowed us to expand the age groups contributing to our research and Anne Maruma who helped with survey design and analysis.

### Project Team

- John Sotillo (Chair), J.Sotillo@kent.ac.uk
- David Chadwick (Technical Lead), D.W.Chadwick@kent.ac.uk
- Matthew Slowe (Project Manager), M.Slowe@kent.ac.uk
- Peter Riley, P.W.Riley@kent.ac.uk
- Bonnie Ferguson, B.Ferguson@kent.ac.uk
- George Inman, G.Inman@kent.ac.uk
- Md Sadek Ferdous, M.S.Fersous@kent.ac.uk
- Kristy Siu, kwss2@kentforlife.net
- Leo Lyons, L.Lyons@kent.ac.uk

<sup>1</sup> Shintau Project <http://sec.cs.kent.ac.uk/shintau/>

<sup>2</sup> Permis project <http://www.permis.org/>

## 2 Project Summary

The University of Kent Logins for Life project, a JISC funded collaboration between the Information Services Directorate and the School of Computing addresses the needs of a University to engage with users throughout their lives. Historically, on-line services and identities have been provided by Higher Education, in most cases, only for the period during which study is taking place. The project attempted to foster a much longer online relationship with its users by permitting and facilitating the amalgamation of a user's existing online identities into the University's information systems whilst maintaining security both for the user and for the organisation. This process allows prospective students to engage with the University without the need to create yet another username and password and minimises administration for the University. Social networking applications are ubiquitous nowadays and federated access management protocols such as OpenID and UK Access Management Federation are also becoming much better known and their credentials accepted by many online services. The project explored how these technologies could be harnessed to develop policies and procedures for enrolling new users, for migrating them to fully enrolled members of the university and supporting them beyond their physical presence on campus.

The project also researched other online services that the University might provide to enhance the online experience at all stages of a person's involvement with the organisation and explored the difficulties associated with managing accounts for those members of the University who have multiple roles and therefore are required to maintain more than one digital identity. Investigation of current practices throughout the field of Higher education and from some sectors of the commercial world helped to ensure our recommendations drew on best practice.

## 3 Main Body of Report

### 3.1 Project Outputs and Outcomes

Output / Outcome Type <i>(e.g. report, publication, software, knowledge built)</i>	Brief Description and URLs (where applicable)
Demonstration system for trialling with users.	<a href="https://persistence.kent.ac.uk/logins4life">https://persistence.kent.ac.uk/logins4life</a> Should this demo service move, it will be linked to from the project homepage ( <a href="http://www.kent.ac.uk/id/projects/loginsforlife/">http://www.kent.ac.uk/id/projects/loginsforlife/</a> )
Demonstration results.	Results obtained from performance and stress testing and usability results from trialling with users. (see <a href="http://www.kent.ac.uk/is/projects/loginsforlife/downloads/L4L-Architecture.pdf">http://www.kent.ac.uk/is/projects/loginsforlife/downloads/L4L-Architecture.pdf</a> )
Project Web Site(s)	<a href="http://www.kent.ac.uk/is/projects/loginsforlife/">http://www.kent.ac.uk/is/projects/loginsforlife/</a> <a href="http://blogs.kent.ac.uk/logins4life/">http://blogs.kent.ac.uk/logins4life/</a>
Recommendations to JISC and Kent for Logins for Life policies and procedures	This is the main body of work for presentation to the University of Kent (see <a href="http://www.kent.ac.uk/is/projects/loginsforlife/downloads/L4L.pdf">http://www.kent.ac.uk/is/projects/loginsforlife/downloads/L4L.pdf</a> )
Recommendations to JISC and Kent for software architectures	This is the academic paper which came out of the technical portion of the project which describes the "Account Linking Service". (see <a href="http://www.kent.ac.uk/is/projects/loginsforlife/downloads/L4L-Architecture.pdf">http://www.kent.ac.uk/is/projects/loginsforlife/downloads/L4L-Architecture.pdf</a> )
Roadmap for deployment at Kent	This is a high level overview of the steps involved in rolling out the policy changes described in the Recommendations document (see <a href="http://www.kent.ac.uk/is/projects/loginsforlife/downloads/L4L-Roadmap.pdf">http://www.kent.ac.uk/is/projects/loginsforlife/downloads/L4L-Roadmap.pdf</a> )

### 3.2 How did you go about achieving your outputs/outcomes?

We identified a need to engage earlier and for longer, with those who came into contact with the University's on-line systems and services. In other words we wanted to begin a digital relationship with

those who might work or study at the University in the period before they were actually members of the university and we also wanted to carry on that relationship beyond the time when those users were no longer physically on campus. We also wanted to look at how we dealt with our on-line users currently and examine whether there were ways we could improve and simplify access to data and services whilst maintaining an appropriate level of security.

Our aims and objectives were:

- to simplify the registration process at the Kent website, in particular by allowing the use the digital identities that most users would already possess on arrival at the website,
- to look at how we could make it easier for users to access low level protected resources, again using existing identities as well as the Kent IT account
- to examine how the University handled users with multiple roles

Broadly the project had two strands:

- researching ways we might improve the experiences of staff, students, ex-members and prospective members of the university when using the website; and
- designing a technical solution to allow users to register and subsequently authenticate and authorise with the account credentials of third party applications;

Both these areas of investigation and development were informed by an examination of best practice at other HEIs and in the commercial world. Stakeholders were interviewed individually or in small groups, asked to complete online surveys and questioned in specially convened focus groups. Throughout the project stakeholders were kept informed via internal reports, workshops, seminars and blogs and encouraged to feedback and comment on our proposals and progress.

### **3.3 What did you learn?**

We were able to evaluate much of our research in terms of figures and percentages eg. how many of our current users use social networking applications, access University systems using mobile devices etc. Other areas of research were less easy to quantify because the information gathering was more 'conversational'. However, analysis<sup>3</sup> of the interviews allowed us to assess whether our proposals were received positively, neutrally or negatively, the extent and seriousness of manager's concerns about changes to security and etc.

We researched current best practice by reading research papers, blogs and text books and by conversations, face to face, by telephone and email with colleagues in other HEIs. Many online resources gave links to other resources and led to conversations with others pursuing similar goals. From the early stages of the research it became apparent that, in addition to the proposals to develop an account linking service we should explore how social networking sites could be harnessed to fulfil our objectives in other ways. The rise of social networking sites in recent years is well documented and although some express fears that individual sites may exhibit rapid expansion followed by equally rapid decline it seems unlikely that social networking, per se is going to disappear or become less popular.

We carried out user testing of the account linking tool developed by Professor David Chadwick's team in the School of Computing. The user trials were designed to determine the ease of use of the system, and the level of understanding an external, novice user would achieve from using the system for the first time. Users were asked to perform the following four tasks:

- download a University of Kent postgraduate application form,
- use Moodle to determine which lecture was in week 6 of a specific module,
- download a paper from the ACM digital library, and
- access the Student Data System. User

---

<sup>3</sup> <http://www.kent.ac.uk/is/projects/loginsforlife/downloads/L4Life-stakeholders-report.pdf>

Users were asked to “think aloud” whilst performing the tasks. This allowed the observer to record the user’s thought processes for later analysis so as to discover where any usability problems might lie.

Assumptions we initially made about the attitudes to the changes we were proposing, within different user groups, did not always prove to be the case. Initial discussions among the Information Services staff on the project team concluded that it would be reasonable to expect that proposals which widened and extended access to the university’s systems might be perceived as a threat to security and that therefore managers and other members of staff might be resistant. In particular team members felt that proposals to incorporate the use of social networking sites with University’s systems, in any way, no matter how low the actual risk to security, would not be a direction many stakeholders would agree with. In fact, as we interviewed this group and admittedly with one or two definite exceptions, we found responses were very positive. Conversely amongst the students we surveyed and spoke to there was some reluctance to embrace the idea that social networking applications had a place within higher education. Whilst many welcomed the ideas there were more negative comments than we had anticipated, even allowing for the fact that our question was by necessity rather broad and only examined the overall principle of ‘linking’ social networking accounts to Kent IT accounts. Some respondents were emphatically against any sort of integration with social networking tools. We were also surprised to learn that among some school groups there was a reluctance to trust the university’s assurances about confidentiality.

However, when the users actually performed the trials with the pilot system, they did not exhibit any reluctance to using their own Facebook, Twitter or other accounts to login to university resources, and the comments that were recorded were all very positive. In fact one user spontaneously linked all his various accounts together in the system, without being asked to do so. We learned from this that the project’s proposals should be accompanied by accessible and concise explanations of the benefits and limitations of linking accounts with emphasis on the user-centric nature of the service, the minimal security risks, and including guidelines for safe usage.

The number of responses from the student group to our online surveys was much larger than we had expected (having expected no more than 50, we got 255) especially from the existing (as opposed to new intake) students considering we had carried out the survey during the summer recess. We did not offer any sort of incentive for completing the survey. We were also pleased at the number of free text comments provided by those surveyed.

It became plain as we started to research the way students and others used information technology in their everyday lives that Facebook was much more ubiquitous than we had realised. Less than 3% of the 2010 intake of students said that they did not use Facebook. Approximately 35% of students who completed the survey said that they spent more than 5 hours a week using Facebook. We didn’t ask students how often they accessed Facebook but research from various internet sources claim that up to 25% of users under 35 years old checked their accounts at least six times a day. This contrasted with the 20% of Kent students who claimed they never used the student portal and even a small number (3%) who said they never checked their University email.

In contrast to this we had perhaps overestimated the use and even awareness of OpenID. Amongst both staff and students there was very little knowledge of OpenID and even less said they were using it. This was somewhat surprising as the OpenID Foundation and the Mozilla organisation were suggesting that the penetration of OpenID was now considerable, with over 1 billion OpenID accounts issued and over 50,000 web sites being accessible using this protocol [10]. (It should be noted however that Google uses OpenID to allow its users to be authenticated by third parties, and therefore many users may have OpenIDs without realising it.) There were some students who mentioned OpenID in the free text comments of the on-line survey. OpenID was originally a preferred choice of the project for authentication as it was seen to be ‘brand neutral’. It is apparent that considerable effort would be needed to publicise OpenID and to persuade users to obtain or activate an OpenID account and start using it (as opposed to using it in the background with their Google account). On the other hand, we have seen that very few people coming to the University do not have a Facebook account and many of our users will be logged into Facebook a great deal and can therefore be authenticated to the website transparently. Despite a degree of reluctance from stakeholders to ‘get into bed’ with Facebook it became apparent that to ignore the popularity and distribution of this application would not be serving the community well.

At the start of the project we felt there would be a good deal of support for merging into one account all the accounts of members of the university who currently have multiple roles and therefore multiple accounts. We could then use different attributes to control access to resources needed for the various roles. It became apparent that there was little agreement in how this could be achieved – there were several ways to approach this technically but each approach seemed to polarise opinion as to whether it was advisable to take that approach or not. Additionally as interviews with stakeholders progressed it became clearer that there was little support for amalgamation of roles into one account. There were objections on the grounds of security – a compromised account of this type could potentially expose a great deal of confidential data and/or make vulnerable multiple systems. There were also concerns that roles could become blurred and some support for the fact that retaining single role accounts - which would necessitate log off/log on to switch between roles - served as a reminder of the different dependencies and responsibilities attached to each role. It was also the view of many managers that the problem did not affect a large number of people at the university and where it did the level of disruption experienced and its toll on productivity was not high. After a great deal of discussion the team concluded that they would recommend maintaining the status quo with a commitment to reviewing the extent of the problem in the future.

### **3.4 Immediate Impact**

The Logins for Life project makes recommendations to Kent and the wider JISC community but as yet these recommendations have not been implemented so we can only offer conjecture on the impact.

We anticipate that there will be an increase in the number of prospective students registering with the University of Kent website and as a result there will be increased opportunities for contact with these potential members of the university by admissions staff.

If existing students adopt the linking of social networking accounts to their Kent IT accounts we would anticipate a reduction in the number of password recovery requests made of the IT service desk. Although difficult to quantify, if current students are provided with easier methods of accessing their timetables and library information one could expect a reduction in absences or late attendance for lectures and perhaps a reduction in library fines and less frustration for students with reservations on books.

Although it was not one of the objectives of the project to examine in detail the broader use of social networking sites as 'official' communication conduits for the University it was something which our own research and other resources found was often mentioned as being 'desirable' and useful to many students and other users. This is perhaps not a great departure from current practice as many HEIs have Facebook pages and Twitter feeds. Evidence suggests<sup>4</sup> that communications via social networking tools, for many students, are more likely to be read in a timely manner than those sent by University email, which could have many implications especially where ad hoc and urgent messages are concerned. This is not to suggest that the University would abandon 'official' channels of communication.

Providing a well-designed and technologically up-to-date web experience enhances the reputation of the University as a key player in Higher Education.

Dissemination and discussions and workshops concerning the proposals of the project do seem to have lessened initial resistance to the amalgamation of social networking and academic resources though there are still justified concerns that the University does not compromise security in its efforts to improve the user experience.

The wider community could expect to see similar benefits if the recommendations and tools, which have come out of the Logins for Life project, are adopted. The Account Linking tool developed by the

---

<sup>4</sup> <http://www.kent.ac.uk/is/projects/loginsforlife/downloads/L4L-online-survey-analysis.pdf>  
<http://nmc.itdevworks.com/index.php/2009/08/facebook-usage-how-often-do-different-types-of-users-access-facebook/>

School of Computing is open source and has been made available to other institutions and anyone else interested in using it.

### **3.5 Future Impact**

It is the opinion of the project team that HEIs need to offer users of their websites and on-line services a high quality experience which is at least equivalent to that experienced at leading commercial and social networking sites. It is difficult to assess the negative effect that failure to take these measures might have but it seems likely that institutions with good reputations will attract more prospective students and that the quality of students studying at an institution will remain high.

Increasingly it is seen as a central aim of governments and those working in Higher Education to reach out to sections of society who historically had not been so well represented on under-graduate courses. This does not mean HEIs need to 'dumb down' the process of engaging with prospective students but rather that the diverse technologies and devices used by this wider community should be seen as part of the portfolio of communication tools that are employed to attract, inform and engage with our users.

The decision to facilitate registration and authentication via a sub-set of social networking sites creates the need for review and monitoring of any effects on internal security, for auditing and re-auditing of the levels of assurance required to access services and webpages and for review of the accepted third parties. Social networking sites may decline in popularity and therefore usefulness, others may appear and need to be considered as contenders for linking. The University obviously has no control over third parties – in particular changes to terms and conditions may be problematical. If the university provides a facility whereby students can link third party accounts with their Kent IT account that implies a degree of approval or complicity with that third party, even though other methods of authentication would always be available. It is therefore important that the ethics of that organisation, particularly in respect of the exploitation of personal data for the purposes of profiling and targeted advertising are monitored. The University is unlikely to wish to retain, let alone exploit, much of the information and personal data (eg photographs, friends lists, wall posts) that some social networking sites, allow to be passed during the process of federated access management. For this reason the current linking service never requests this data nor uses it if it is passed. It is therefore important that the University does not give the impression that it is collecting this data.

## **4 Conclusions**

- There are benefits for users and the organisation in extending and widening access to the University's on-line services and developing and promoting additional services to achieve this.
- Technologies can be developed to securely incorporate social networking and other third party authentication mechanisms into the on-line systems and resources of HEIs.
- By attaching appropriate Levels of Assurance to the University's on-line resources and to third party accounts and linked accounts, security implications for the project's proposals can be minimised.
- Social networking sites such as Facebook and Twitter should not to be seen solely as tools of entertainment and social communication.
- Social networking tools are no longer purely the domain of the young, well educated and affluent but have an extensive distribution amongst all age groups, nationalities and across social divides.
- Students have their own sense of where the boundaries lie between social life and academic life and some of the tools and technologies they use have a role in both worlds

The project concluded that tools could be developed and policies and procedures adapted to permit the use of third party sites, in particular social networking sites, to register and authenticate their users

in order for them to gain access to the University of Kent website without creating unacceptable risk to the security of the users or the University's systems. It was also concluded that the adoption of measures to facilitate these enhancements would also improve the service provided to alumni by creating easier access to alumni mail and other services aimed at alumni. This in turn would strengthen the bonds between the University and its alumni.

More widely the project found that although students did not wish to see a complete blurring of the boundaries between educational resources and social networking software, this did not mean that they would not use applications such as Facebook to send and receive communications, which would be beneficial to their studies<sup>5</sup>. Social Networking applications were seen as just one of an arsenal of tools, which many young people now use to search, organise and disseminate data for both social and academic use. The project also concluded that the reach of these social networking tools has now spread far beyond the original user base of college students and other young people and are used by all age groups and across social and international groups. To the wider community the message would seem to be that it may be a mistake to dismiss social networking as merely entertainment and gossip. Students and other young people have become very adept at adapting technologies to solve their problems and to suit their needs.

As for the conclusions relevant to JISC it seems likely that the benefits which ensue from the recommendations of the project would also be expected at other Higher Education Institutions that adopted them and that the Account linking software developed by the project could be easily adapted for use by other institutions. The keynote speech at the JISC11 event in March 2011 mentioned the need to use technology to attract and retain students and maintain a relationship throughout their careers and as alumni. The project team are of the opinion that the work of Logins for Life definitely falls into this category.

## 5 Recommendations

General recommendations to come from the project are that HEIs need to be aware of the technologies and devices that their students and future students may use, and that it may be possible to leverage their identity management capabilities without introducing unmanageable risks into HE systems. This approach can be extrapolated to communications with alumni and other groups. In a time of increasing competition and higher fees we need to harness all possible methods to maintain good relationships with our community.

Recommendations for JISC would be that the Logins for Life project should not be seen as a discrete piece of research into what can be done now to improve and enhance engagement and continuation but as one part of an on-going commitment to widen the methods of communication, engagement and identity management that HE considers as useful tools.

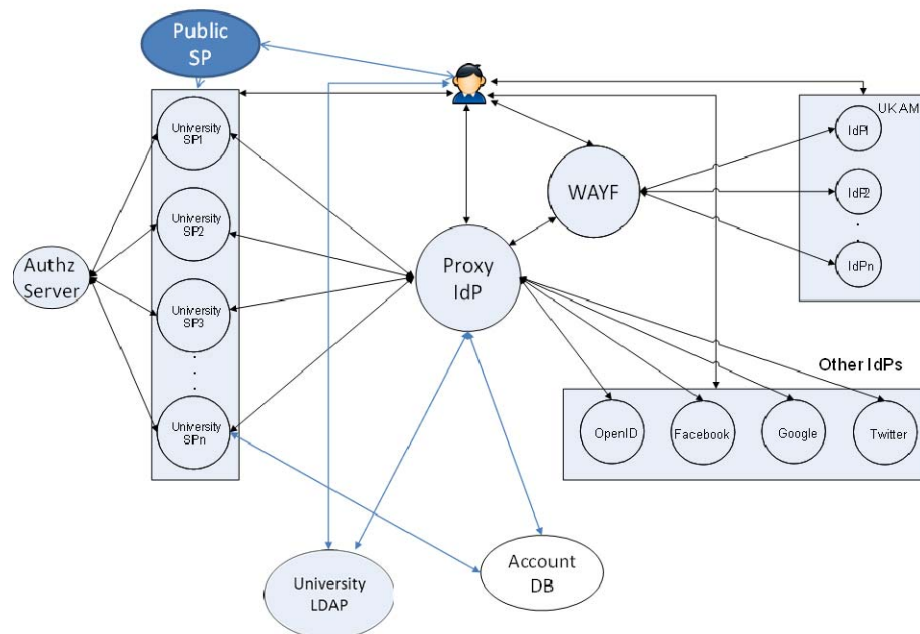
The account linking tool developed by the school of Computing utilises Levels of Assurance to protect and appropriately expose the University's resources. However this did reveal a rigidity and lack of granularity in the current NIST specification. The project chose a somewhat arbitrary LoA of 1.5 for a log in using a third party account which had been previously linked with a Kent account. This was chosen as a midpoint between a login with a Kent account (LoA 2) and a log in with an unlinked third party application account (LoA 1). This may be an area for further investigation. It seems unlikely that this project is alone in noting the limitations of the NIST LoA specification.

---

<sup>5</sup> It should be noted that this particular aspect of integration wasn't part of the original project scope, but that it did seem prudent to pursue this course of questions while we had their attention to feed into possible future work within the University and beyond

## 5.1 Recommendations for Account Linking Service

- The recommended architecture for a university site is shown in figure 1 below



- Key components of this architecture as follows:
  - The set of University Services (SPs) that wish to utilise this model for user access, single sign on and authorisation.
  - An Authorisation Server which is a standalone policy decision point (PDP). This makes authorisation decisions for all the university SPs based on the attributes of the user and the Level of Assurance (LoA) of the user's authentication session. It can be configured with many different policies, in either the PERMIS [12] or XACML [13] policy languages, and the protocol allows each SP to choose which policy it prefers to be used.
  - A University LDAP service which holds the attributes of the users, which are to be used by the Authorisation Server in making the access control decisions. The LDAP service is also used to provide authentication of local users, based on the usernames and passwords that it stores.
  - An Account Database which holds Persistent Identifiers (PIs) of the various accounts that each user has at various Identity Providers (IdPs) and which the user has chosen to use to access the university services.
  - A Proxy IdP which is the interface between all the university SPs and the outside IdPs. The SPs trust the Proxy IdP to ensure that each user has been properly authenticated by an IdP and that the correct Level of Assurance (LoA) is returned to them along with the user's attributes.
  - A set of external IdPs which are trusted to authenticate users correctly. The current set that is supported by the released code is: the IdPs of the UK Access Management Federation, Facebook, all OpenID identity providers, Google, and Twitter. Other external IdPs can easily be added by writing the appropriate protocol handling code.
- All the software to support the above architecture is available as open source code, either from Feide (simpleSAMLphp) or the University of Kent (Authorisation Server, Proxy IdP, Facebook code of proxy IdP and Account Database)
- Specific protocol features that are used by this architecture are as follows
  - The protocol between the University SPs and the proxy IdP is standard SAMLv2 [11]. Two notable features that are used are:
    - the AttributeConsumingServiceIndex, which is set by the SP to tell the Proxy IdP which user attributes it requires
    - the <authnContextClassRef> element of the <RequestedAuthnContext> which is set by the SP to tell the Proxy IdP which LoA value is required to access the service.

- b. The protocol between the University SPs and the Authorisation Server is the SAML-XACML protocol [11].
  - c. The protocol between the Proxy IdP and the UK Access Management Federation WAYF service is Shibboleth v2.0.
  - d. The currently supported protocols between the Proxy IdP and the various other external IdPs are: Facebook, OpenID and Twitter.
5. The architecture can be individually tailored by universities, to include as many or as few SPs as it requires, and as many or as few external IdP as it requires. New external IdPs can be added by adding new protocol handling modules to simpleSAMLphp. The architecture can also be tailored by having one Authorisation Server per SP instead of one per site, with each Authorisation Server holding the specific policy of the SP.

## **5.2 Limitations of Current Architecture**

We assume that every UK University has an LDAP service that is accessible using standard LDAP protocols. Any university which does not have such an LDAP service, will need to modify the Proxy IdP code in order to access its local attribute store and authentication service using whatever protocols are supported.

## **5.3 Deficiencies in Current Protocols**

The Proxy IdP asks each UK Access Management IdP to return all the attributes that it holds about the user that it is willing to release. Whilst this is currently not a problem, since the set of attributes is typically very small (often just two: the eduPersonTargetedID and eduPersonPrimaryAffiliation), in the long term this may not be ideal. Whilst each University SP asks the Proxy IdP for exactly the correct set of attributes that it needs to make an authorisation decision, the mechanism that is used – setting the AttributeConsumingServiceIndex in the SAML request – is not scalable when used by the Proxy IdP since it would need to combine all the indexes from all the SPs into one large set of indices for the university site as a whole. The University of Kent has produced an enhancement to the SAML protocol which allows the set of attributes that is required to be dynamically set in the Authentication request (as it already can be today in the SAML Attribute Request message). However the SAML Authentication request does not allow the set of attributes to be dynamically requested, but only statically set in the metadata and then dynamically requested by using the AttributeConsumingServiceIndex to point to the correct element of meta data. We believe that the SAML protocol would be much more flexible if this enhancement were made to it.

## **6 Implications for the future**

The project recommends that JISC considers further research into the levels of trust that exist and can be developed between social networking tools and Higher Education. The Logins for Life project had no direct contact with owners of third party applications but felt there were areas that might be explored to the mutual benefit of these organisations and to Higher Education. Currently the default exchange of information between organisations such as Facebook and organisations that ‘federate’ with them are based firmly on commercial principles. Higher Education would most likely wish to explore a different set of principles, in part to create a separation between them and the commercial world and therefore engender a different level of trust with the users. The project found that some students worried that the University would have access to their personal information if they ‘linked’ their accounts with Facebook. Applications from the commercial world that attempt to link with social networking applications generally request access to areas which Higher Education would have no interest in – friends lists, photographs, wall posts etc. Further research might explore how linking with different classes of organisation, with associated different levels of trust and different degrees of amalgamation, might be differentiated.

The implications of this work for others in the field will depend to what extent they leverage these technologies. If the principle is accepted that we need to engage better and for longer with our prospective students and our alumni, then the use of tools such as Kent's account linking service to leverage social networking sites are useful in this quest. HEIs need to examine to what extent they wish to embrace these changes. Decisions need to be taken about:

- which third party sites will be acceptable,

- what level of assurance they provide,
- what level of assurance and authorisation is needed to access online resources, and
- what policies and procedures are needed to cover these new systems.

Widening the ways in which protected resources can be accessed will undoubtedly have an impact on security so risk assessments are vital. Provision of alumni facilities like alumni email and logins for life will over time have a considerable impact on the number of accounts which an institution maintains and administrative tasks associated with this will also be implicated. How to remove dormant or dead accounts without removing live but only occasionally used ones is also an issue that will need to be addressed.

There is scope for a great deal of further development work. Understandably there may be nervousness about how deeply HEIs want to become involved with commercial social network providers since they control the APIs, as well as how much personal data can be input or retrieved. Thus the development of apps that can push or pull personalised data directly into these social networking applications will always be problematical. However if the University, the wider community and JISC agree that there are benefits in embracing the use of third party accounts as methods of registration and authentication then the development of useful, easily accessible apps could be seen as additional benefits which will increase the take up amongst users. The JISC funded UEA Wolfie project<sup>6</sup> has already completed good work in this area.

In the registration process for HEIs the application to UCAS is currently an external process which comes between an initial approach to the University's website and the creation of an IT account at the chosen institution. This inevitably results in some duplication of information or at the very least the need to merge accounts. It might be beneficial to examine ways of creating a process whereby the personal data given by a prospective student at an initial interaction with a HE website – quite probably through a social networking application – could be re-used in the UCAS application and follow the applicant through the various stages of the offer and subsequent conclusion.

If Kent adopts the recommendations of the project there will be costs as detailed in the reports and possible further development would be needed. Even without this there will be need to review the third party sites periodically and to introduce procedures to manage a potentially large increase in IT account data and email accounts. A further on-going process will be to audit new resources introduced to the University's systems to assess what level of assurance they should have. The costs of these additional tasks should be seen as being offset by an increased number of applicants, reduced costs in password management, enhancement of the University's reputation and an increase in the size of the alumni database with an associated potential for increased donations to the University.

## 7 References

1. "OpenID Foundation website", n.d., <http://openid.net/>.
2. "Test Pilot: Accounts and Passwords Study: Aggregated Data Samples", n.d., <https://testpilot.mozillalabs.com/testcases/password-distribution/aggregated-data.html>.
3. "UK Facebook Statistics for August 2010 | Clicky Media™ the Digital Marketing Agency", n.d., <http://www.clickymedia.co.uk/2010/08/uk-facebook-statistics-for-august-2010/>.
4. "ueaWolfie", n.d., <http://ueawolfie.jiscinvolve.org/wp/>.
5. Stefan Wahe, David Wasley, "Appropriate Access: Levels of Assurance | EDUCAUSE", n.d., <http://www.educause.edu/Resources/AppropriateAccessLevelsofAssur/162629>.
6. JISC, "JISC Identity Management Toolkit", n.d., <https://gabriel.lse.ac.uk/twiki/bin/view/Projects/IdMTToolkit/WebHome>.
7. Ana M Martínez Alemán, "Online social networking on campus : understanding what matters in student culture /",
8. "Multiple Affiliations Study", n.d., <https://gabriel.lse.ac.uk/twiki/bin/view/Projects/MultAffiliations/>.

---

<sup>6</sup> <http://ueawolfie.jiscinvolve.org/wp/>

9. "IS Smart Phone/Mobile Device Survey 2010 - Information Services - University of Kent", n.d., <http://www.kent.ac.uk/is/surveys/2010/mobile/>.
10. See <https://openid.org/home> (last accessed 26 March 2011)
11. OASIS. "Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0", OASIS Standard, 15 March 2005
12. D.W.Chadwick, A. Otenko. "RBAC Policies in XML for X.509 Based Privilege Management" in Security in the Information Society: Visions and Perspectives: IFIP TC11 17th Int. Conf. On Information Security (SEC2002), May 7-9, 2002, Cairo, Egypt. Ed. by M. A. Ghonaimy, M. T. El-Hadidi, H.K.Aslan, Kluwer Academic Publishers, pp 39-53.
13. OASIS "eXtensible Access Control Markup Language (XACML) Version 2.0" OASIS Standard, 1 Feb 2005
14. OASIS "SAML 2.0 profile of XACML, Version 2.0". OASIS committee specification 01, 10 August 2010

## 8 Appendices

Other documents not directly referred to as "project outputs" but may be of specific interest are:

- Kent student views on the access and use of online services – survey results and analysis <http://www.kent.ac.uk/is/projects/loginsforlife/downloads/L4L-online-survey-analysis.pdf>
- Analysis of stakeholders views on the project's aims and proposals <http://www.kent.ac.uk/is/projects/loginsforlife/downloads/L4Life-stakeholders-report.pdf>