Secure sharing of Higher Education Achievement Reports (HEARs) at Newcastle University using SMART – DRAFT 01

Created: 22/08/2012, Updated: 05/10/2012

Authors:
Maciej Machulak (maciej.machulak@gmail.com), Łukasz Moreń (lukasz.moren@gmail.com)

Introduction
The SMART (Student-Managed Access to Online Resources) project started at Newcastle University on the 1st January 2010. Over the years of the project, it has attracted 3 funding rounds from JISC and the School of Computing Science at Newcastle University. Work on SMART has resulted in an advanced research on new technologies for user-centric access management for the Web. Importantly, research on User-Managed Access (UMA), a novel technology for privacy-aware secure data sharing of Web resources, has been conducted by researchers from the University. This allowed to build the SMART Authorization Manager (SMART AM), the first UMA-compliant Authorization Manager that allows end-users to easily compose very flexible sharing settings for their online data. The software has been awarded the prestigious Kantara Initiative IDDY (Identity Deployment of the Year) 2011 award in San Francisco, CA, USA. Moreover, the project has allowed researchers from Newcastle University to actively participate in the User-Managed Access Work Group which is led by Eve Maler. The UMA WG incubates the UMA technology and researchers from the University, with other researchers from around the world, play pivotal roles in this group.

So far, SMART has had 3 phases. In Phase I, an advanced User-Managed Access implementation has been developed using the Java programming language. This implementation has been integrated with a set of exemplar Web applications. Namely, a SMART Authorization Manager and UMA/j middleware have been designed and implemented. Work during this phase has been done in collaboration with University’s Information Systems and Services (ISS). Phase II allowed to improve the software in terms of its functionality as well as code maturity. Phase III, which has ended 31st August 2012, has allowed to integrate the system with UK Federation and deploy it within Newcastle University. The deployed system has been integrated with UK Federation via an advanced software integration layer. This integration layer is a state-of-the-art identity management technology (named Connect), which has been also designed and implemented at Newcastle University. Connect implements Shibboleth to allow users to share their data easily and securely with collaborators from other academic institutions in the UK (i.e., sharing can be established across institutional boundaries). Additionally, an exemplar Personal Data Store (PDS) for Newcastle University academics has been implemented and integrated with SMART AM. This PDS application allows University’s academics to store their high-value personal information and share it across organizational boundaries.
Problem Scenario

One of the scenarios for SMART AM and User-Managed Access at Newcastle University is the “Sharing Trustworthy Personal Data with Future Employers” scenario. This scenario has been submitted to the User-Managed Access Work Group and has been accepted for consideration.

This scenario overlaps greatly with the concept of Higher Education Achievement Reports (HEARs) that are planned to be introduced at Newcastle University. The HEAR is intended to provide a single comprehensive record of a learner’s achievement at a higher education institution such as Newcastle University. It will be an electronic document, which will adhere to a common structure and can be verified by the academic registrar or equivalent officer. However, HEAR leaves unspecified how such document is shared outside of the institution.

In this section, we present a simplified version of the “Sharing Trustworthy Personal Data with Future Employers” scenario that shows existing problems with sharing documents, such as Transcript of Records documents, by students of Newcastle University.

The simplified scenario shows interaction of a student, named Sean, who wishes to apply for a graduate job at CareerMonster website (online application). CareerMonster allows students and professionals to create their personal accounts where they can search through a vast amount of job positions. Once a suitable job position is found, an applicant can submit required information (e.g. personal information, list of attended schools, transcript of records.
documents, etc.). In this scenario, we will focus exclusively on submitting the “Transcript of Records” document.

Steps in the “problem scenario”:

1. Sean visits the CareerMonster website and registers for a new account. This requires Sean to provide his personal details and establish a set of credentials at the application (i.e. Sean has to create a username/password).
2. Sean signs into the CareerMonster website using the newly created set of credentials.
3. Sean searches for the job position of his interest. He then selects the job position and is asked to provide necessary information (e.g. CV, Transcript of Records, etc.).
4. Sean does not have his Transcript of Records with exam marks ready. Therefore, he needs to obtain such a document, which can be done in two different ways:
   a. Sean writes an email to the School’s reception and asks for such document to be prepared. Sean’s request creates a ticket in the School that has to be handled manually by staff of the School of Computing Science. Staff has to:
      i. Verify Sean’s status as a student.
      ii. Print the Transcript of Records with exam marks and verify them.
      iii. Stamp and sign the Transcript of Records.
      iv. Inform Sean that the document is available for collection.
   b. Sean uses an online system provided by Newcastle University (e.g. S3P Portal - https://s3p.ncl.ac.uk) to print out the “Transcript of Records” document. Such printed document contains a statement that this is an official document. This document, however, does not contain any signatures or stamps. Sean takes this document to the reception of School of Computing Science where staff can:
      i. Verify the document.
      ii. Stamp and sign the document.
5. When Sean obtains the Transcript of Records document, he scans it and creates a PDF version.
7. Sean completes the application process for the job position.

A more detailed description of the scenario with thoroughly discussed problems is available at: http://kantarainitiative.org/confluence/display/uma/cv_sharing_scenario

Problems

With regards to the above scenario, there are two major problems that affect the user experience of a student (in this case Sean) when applying for a graduate job position using the CareerMonster online system:

1. CareerMonster would typically require a trustworthy document with exam marks (“Transcript of Records” document) from Sean. This is to prevent Sean from forging such a document and changing his own marks for his own benefit. Therefore, Sean has to either:
a. Engage University staff to obtain a signed/stamped version of the “Transcript of Records” document. Such document is printed by the staff and later has to be scanned and uploaded in a PDF form to the CareerMonster application. This process currently exists at Newcastle University.

b. Print out the “Transcript of Records” from an online system provided by Newcastle University (e.g. S3P Portal - https://s3p.ncl.ac.uk). Such printed document contains a statement that this is an official document but this document lacks any signatures. Therefore, a “Transcript of Records” document in such form may not be sufficient for certain organisations (e.g. career websites - CareerMonster employers, etc) that require to verify such documents. This process currently exists at Newcastle University.

c. Obtain an eTranscript document (e.g. in HEAR format), digitally signed by Newcastle University. This document can be later uploaded to CareerMonster. This document has to be generated every time there are new marks added to Sean’s records, which may be problematic for processes that take months. This process does not yet exist at Newcastle University but is planned to be introduced.

2. Sean is required to create an account at the CareerMonster website. Therefore, he has to manage an additional set of credentials (username and password) for this website. Creating a new set of credentials is a time-consuming process and often results in end-users abandoning the website.

Proposed Procedural Improvements

In order to simplify the process of applying for a job by Newcastle University graduate students and address the problems raised in the previous section, the process of sharing data from Newcastle University has to be improved. Students should be allowed to:

1. Obtain trustworthy University data easily and securely without unnecessary overheads.
2. Share trustworthy University data without the need of engaging University staff or without the need of manually handling data sharing every time any of their data changes;
3. Interact with Web systems using an already existing set of credentials, e.g. University credentials.

With regards to the presented scenario, we focus on:

1. Giving students the ability of secure sharing of data formatted as HEARs directly from the University (e.g. “Transcript of Records” documents) from an existing system - i.e. S3P / Blackboard (or legacy NESS) and without manually handling of such sharing;
2. Allowing students to use their University credentials when signing in to various applications on the Web;
3. Allowing students and graduates to establish continuous access to their educational data (HEARs, Transcript of Records document) without the need of contacting the school’s administration staff;
4. Giving third party services on the Web (employers, career services, other universities) access to up-to-date students' academic records (students do not have to update their documentation during long processes of applying for their graduate job positions).

**Proposed Technological Improvements**

Proposed procedural improvements can be introduced at Newcastle University using the software implemented during SMART projects. User-Managed Access, and the implemented SMART Authorization Manager, augmented with the state of the art identity management technology (Connect), can allow such applications as S3P / Blackboard (or legacy NESS), among many others, to easily expose the existing information (e.g. exam marks or any other data formatted as HEARs) so that these can be securely shared by students outside Newcastle University.

Since systems such as S3P and Blackboard are planned to expose students’ data in a HEAR formatted way through Web APIs, there is a clear need for advanced identity and access management solutions to be implemented and deployed at the University. Therefore, SMART AM, being the state-of-the-art identity and access management suite can provide all necessary access control to this information. Importantly, SMART AM will require user approval before information is shared outside of the University and will also record access requests to user’s information for the purpose of accountability. It will provide a unified UI (User Interface) for end-users to define how data is shared. Such a unified UI for setting access control permissions is critical in highly distributed systems such as that present at Newcastle University. Importantly, user experience in SMART AM is similar to existing systems and does not require end-users to learn new paths of exchanging data, setting permissions, or signing in to Web applications.

**Solution Scenario**

In the solution scenario, we implement the previously discussed procedural improvements - i.e. we allow the student to:

1. Sign in to a Web application using an existing set of credentials (without revealing these credentials to this client application);
2. Submit exam marks (“Transcript of Records” document) directly from the University (in this case the S3P system) without requiring any manual intervention from University staff members.

In this scenario, we make the assumption that the S3P system has been improved and allows to expose exam marks using a Web Application Programming Interface (API) and formatted as HEAR - e.g. marks are available for access using HTTPS at a particular URL - e.g. at [https://s3p.cs.ncl.ac.uk/api/sean.walker/marks](https://s3p.cs.ncl.ac.uk/api/sean.walker/marks). Access control to the API is done using the SMART Authorization Manager.

We also assume that the CareerMonster Web application has been improved and allows to retrieve the data directly from Newcastle University - i.e. the application can be granted
authorization and can issue authorized HTTP requests to specific endpoints available at the University (i.e. in this case the [https://s3p.cs.ncl.ac.uk/api/sean.walker/marks](https://s3p.cs.ncl.ac.uk/api/sean.walker/marks) URL).

Steps in the “solution scenario”:
1. Sean signs in to the CareerMonster website using his existing set of credentials (e.g. Newcastle University credentials) without revealing his credentials to this website.
2. Sean searches for the job position of his interest. He then selects the job position and has to provide necessary information.
3. Instead of manually uploading a trustworthy “Transcript of Records” document, Sean recognises that the website supports direct import from Newcastle University.
4. Sean decides to share his exam marks with CareerMonster directly from the University. He clicks on the “Import” button and is redirect to SMART AM.
5. Sean needs to authorize CareerMonster to be able to access his exam marks from S3P in a secure way. SMART AM mediates the transaction and allows to establish a trust relationship between CareerMonster and S3P.
6. CareerMonster retrieves the Transcript of Records document with certified exam marks directly from S3P (data is formatted as HEAR). Therefore, CareerMonster can trust that this information is trustworthy and has not been forged. Sean does not have to provide a signed and stamped version of the document.
7. Sean applies for the job position as usual.
Demo Implementation

Demo of the solution scenario has been implemented with a custom-built S3P system (real S3P system can be extended in the similar way). The custom-built S3P system has been developed on top of the PDS application that has been developed during Phase III of the SMART project. Additionally, a simple CareerMonster online job application has been designed and implemented.

Custom-built S3P is available at: http://pumahostone.appspot.com
CareerMonster is available at: http://pumarequesterone.appspot.com
The SMART Authorization Manager application is available at: http://test.smartam.net

Summary

In this document, we have described SMART, a project which has resulted in an advanced software being developed at Newcastle University. We have shown that the software is of high value to the University and its integration with existing applications, such as S3P, should be seriously considered by the University and the School of Computing Science. We pointed out that integrating existing systems with SMART AM fits precisely into the University’s strategy of producing formatted HEARs and exposing them securely beyond Newcastle University. Proposed improvements will allow the University to eliminate unnecessary paperwork and significantly reduce administrative costs in a long term. Additionally, these improvements will simplify various processes for students and will allow them to benefit much more from the information that they store at the University.

We have presented a “problem scenario” that discusses an existing process of applying for a job by a Newcastle University graduate student using an exemplar CareerMonster Web application. We have briefly discussed problems with this scenario and we have presented possible procedural and technical improvements. We have then shown how these improvements can be implemented using SMART AM using our “solution scenario”. Proposed improvements have been implemented using SMART AM and two custom-built applications available online.
Appendix A - Screenshots for Solution Scenario

Sean attempts to access his online data at the S3P application.

Sean visits the S3P Web application at Newcastle University. Selects “Newcastle University”.

Sean signs in to Newcastle University with his existing credentials.
Sean sees his personal data stored by the S3P application.

Sean can view his academic record.

Sean then attempts to apply for a job position at the CareerMonster Web application.
Sean visits the CareerMonster Web application. Selects to sign in with his University’s account.

Sean signs in to Newcastle University with his existing credentials.
Sean is presented with a list of available job positions. He attempts to apply for the “Junior Software Engineer” position.

In order to apply for a job position, Sean has to fill in some information or import it from S3P.
Sean is presented with a consent page, where he is required to authorize CareerMonster to access his personal data from S3P. This consent is represented on SMART in form of sharing settings for Sean's name.

Sean’s personal data is retrieved by CareerMonster directly from S3P. Sean then selects to import his academic record from S3P as well.
Sean is presented with a consent page, where he is required to authorize CareerMonster to access his personal data from S3P. This consent is represented on SMART in form of additional sharing settings (this time for Sean’s academic record).

Sean’s academic record is retrieved by CareerMonster directly from S3P. At this point, all required information has been submitted to CareerMonster and Sean can apply for the job position of his choice.
Sean can apply for other job positions if necessary.

Sean can sign in to SMART and view various information regarding his University's data and how this data is shared with other applications.

Sean can view sharing settings for his academic record.
Sean can view how his data is shared with other applications.