Secure Certification for ePortfolios

Lisha Chen-Wilson, Patrick Newcombe, Piers Royce, Samuel Ong, Timothy Wonnacott, Gary Wills, David Argles
Learning Societies Lab, University of Southampton, UK
[lcw07r, pn204, psr104, so304, tpw104, gbw, da] @ecs.soton.ac.uk

Abstract

Students often build up portfolios of their achievements as they study and present them when they apply for jobs or for further study. Of increasing interest is the concept of an online "ePortfolio" which enables greater power and flexibility in displaying achievements. However, the issue of cheating needs to be addressed, especially where certificates of attainment are being presented.

An eCertification project, named "eCert", has recently been run at Southampton in order to explore these issues. This paper documents how we approach the validation of applicants' claims of attainment.

1. Introduction

In education, portfolios provide a useful way for learners to document their achievements which could be of interest to potential employers. Recently, the development of a personal ePortfolio system has been encouraged, with the intention that such a system should ultimately replace the current paper-based system.

While the development of ePortfolio offers user a huge advantages and enormous help to lifelong and distance learners [1,2,3], its security issues is urgently need to be addressed in order to prove its genuine and to protect against fraud. However, there are no implementations that have explored the underpinning technology/mechanism.

A project, called "eCert", was set up at the University of Southampton to explore such issues. EdExcel, a UK national certifying authority, agreed to work with us. There were considered as having two possible approaches towards the problem solving: a) an online certification system (eCertification): a process to certify the qualifications of an e-portfolio through a web server, b) digital certificate of qualifications (eCertificate): a certificate that is issued in a digital form and through a secure certification and verification method. This paper demonstrated how the eCertification route is approached.

2. The Initial Design

In eCertification, three parties are involved in the transaction: the ePortfolio holder (e.g. the student / system user), the ePortfolio receiver (e.g. potential employer) and the Certifying Authority (e.g. the exam board). It was assumed that the ePortfolio holder and the ePortfolio receiver would communicate with a certifying authority, and that all three parties would rely on underlying eCertification web services. Figure 1 indicates the important interactions that need to occur within such a system.

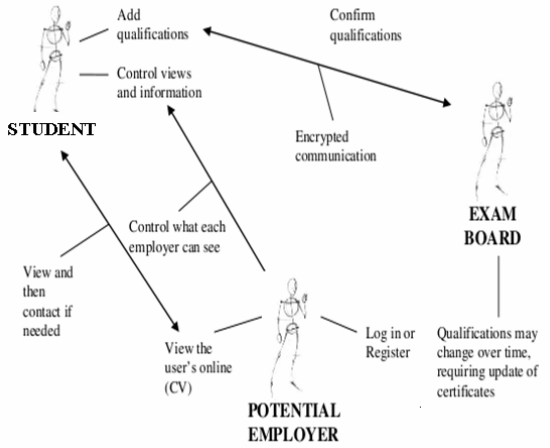

Figure 1: Functionality required in the eCert project

3. The Security Model

A number of decisions on security has been taken:

1. The data is to be regarded as important and therefore should be properly secured
2. There should be minimal transfer of data

3. It should not be possible to browse the data; all queries should be of the format, <claimed award> and the response, <true/false>
4. The award holder (student) should determine who may see their award details

As the student builds up their award profile, the Certification Server contacts the Awarding body (e.g. EdExcel in our case, but as many awarding bodies as possible ought to be part of a full scheme). This is done on an "is this true" basis, with a true or false answer being returned. The student's profile then builds up with a series of certified claims. It is also likely that there may be some unverifiable claims (e.g. an award from a body that is not part of the scheme). In practice, it was found that a fourth possibility was "pending" - i.e. it should have been possible to verify the claim, but for some reason the Certifying Body hasn't responded yet; maybe their server is down.

The system has also provided a function for the student to select which awards they want to present to a given employer, which is done via a tick box grid. Once an award profile for a particular employer has been built up, the student will be given a code by the Certification Server. This code is then sent to the employer, who can use this to log in to the Certification Server to see the student's award profile. The web page that they see gives a "stamp" indicating the status of the claim.

All communications are encrypted and digitally signed so the source can be verified. This entails the use of both public and private key encryption.

The nice thing about this approach is that all original data remains with the Certifying Authorities. The Certifying Sever simply communicates with these authorities to confirm or deny claims, and no data is passed on from this point – all communications involve the Server.

4. The eCert Implementation

With the security model decided upon, implementation was now a straight-forward design, build and test exercise. The screen shot in Figure 2, a preview CV page, is presented here to help in understanding what the system looks and feels like in use.

Explanation of Figure 2: once a student builds up a set of certified awards, he/she can call up a "View Summary" page to allocate awards to employers via a grid. The student can see the view that the particular employer will get via a "Preview your CV" page as shown in Figure 2.

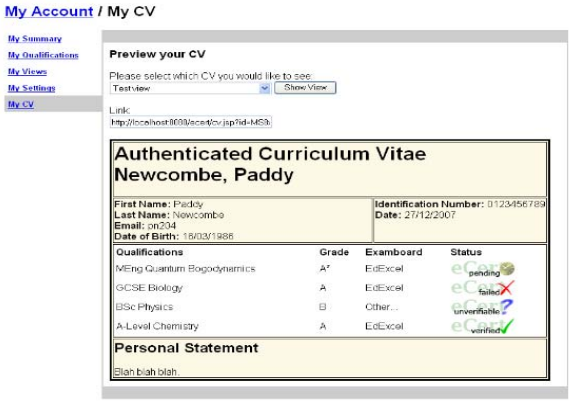

Figure 2: Preview CV page

It will be noticed that Figure 2 includes test data rather than genuine information!

5. Conclusions

The purpose of this project was to investigate the issues involved in setting up an eCertification system, particularly from the security point of view. In order to make it realizable within a realistic timeframe, the scope was limited, and focused particularly on the delivery end, linking to the ePortfolio Holder and the ePortfolio Receiver.

So far, the project has explored security issues in the eCertification route, particularly in the client-facing side of the process. The next step will be to consider issues of scalability, the need to communicate with multiple awarding body servers, and to explore the eCertificate route.

6. References

[1] Bhattacharya, M., Mimirinis, M. "Creating ePortfolio with OSP", *icalt,* pp.947-948, Seventh IEEE International Conference on Advanced Learning Technologies (ICALT 2007), 2007

[2] Colyer, S. and Howell, J. (2002). Beyond the shoe box: Developing an ePortfolio for Leisure Sciences students. In *Focusing on the Student.* Proceedings of the 11th Annual Teaching Learning Forum, 5-6 Perth February 2002.

[3] Paretti, M.C., (2004), Work in progress: using e-portfolios to assess communication skills, Proceedings of the 34th Annual Frontiers in Education, FIE 2004, 20 – 23 October 2004