Secure Certification for e-Portfolios

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

In a number of countries, students build up portfolios of their achievements as they study. These are then presented when they apply for jobs or for further study. Various projects exist which are exploring the "e-Portfolio" concept where such portfolios are maintained and presented online, enabling greater power and flexibility in displaying achievements. However, the validation of certificates of attainment which the student is presenting has not been addressed until now.

The process by which achievements are verified is called "eCertification". It raises interesting issues as it involves three-party authentication. An "eCert" project has recently run in order to explore these issues. This paper records the lessons learned about how we may best approach the process of validating students' claimed awards in such an environment.

Keywords

e-Portfolios, e-Certification, security, authentication

1. Introduction

Portfolios have been in use in education in the UK and elsewhere for a number of years, particularly for the 14 to 19 year old sector of the population. They provide a useful way for these young learners to document their academic achievements, along with other achievements which could be of interest to potential employers; they also have potential for supporting and motivating lifelong learners. Recently, the development of a personal e-Portfolio system has been encouraged, with the intention that such a system should ultimately replace the current paper-based system. A number of projects have been implemented, such as eP4LL [1], which have led to a reference model for e-Portfolios [2].

e-Portfolios offer a number of advantages [3,4,8]. They:

1) allow for the inclusion of a rich set of source materials
2) can be more easily accessible remotely
3) can be accessed more rapidly
4) aid learner feedback
5) encourage learner reflection
6) encourage learner involvement in establishing an appropriate personal development plan
7) can be updated and shared more quickly
8) offer the potential for third party verification of qualifications

Whilst such an approach is good for the 14 to 19 year old learner group, it can also be of enormous help to lifelong and distance learners with frequent minor portfolio updates encouraging such learners to persevere. This is particularly true where awards are confirmed on a rolling basis, thereby encouraging continued commitment to study against competing life demands at home and at work.

There is a crucial process of verification of claims of achievement made by the student that needs to be included for any e-Portfolio system to be truly useful. To date, no current e-Portfolio implementations have explored the underpinning technology or mechanisms required to implement the process of e-Certification (on-line authentication of awards). This is true across the world. Thus the European "Europass" provides a Certificate Supplement and a Diploma Supplement. These provide facsimiles of award certificates, but the system clearly states that, "The Europass Certificate Supplement is not: a substitute for the original certificate;" or "An automatic system that guarantees recognition" [5]. Yet this form of validation has been addressed and implemented securely in other contexts such as eCommerce and on-line auctions. A project entitled "eCert" was set up to produce an award certification demonstrator which would enable such issues to be explored.

EdExcel, a UK national certifying authority, agreed to work with the project to explore potential models for such a system and to create a proof-of-concept system. The eCert project has made no attempt to provide something which might be used directly in real delivery systems at this stage. However, it is properly designed, and has produced code which is located in a Source Forge open source code repository, providing a sound basis for the future development of a system which could go live, and most importantly, has enabled exploration of key design issues in e-Certification.

2. The Initial Design

From the outset, it was recognised that the eCert project raised interesting questions. In particular, many conventional security scenarios assume two stakeholder transactions, with any third party involved being an attacker. In eCertification, three parties are involved in the transaction; any external attacker becomes a fourth party. Furthermore, we are not only dealing with access to resources with the attendant issues of authorisation, but also with verification of information provided, so issues of trust are involved. The original design is given in figure 1.

The assumption was that the e-Portfolio holder (e.g. the student) and the e-Portfolio receiver (e.g. the university to which they had applied) would communicate with a certifying authority, and that all three parties would rely on underlying e-Certification web services.

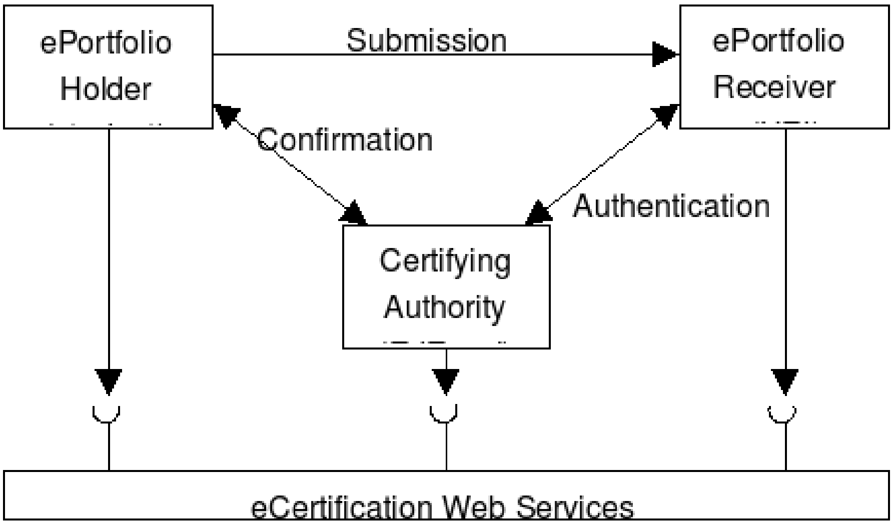


Figure 1: Original design for eCert project

Following the e-Portfolio framework [2], one would assume that a security protocol called "Shibboleth" should be used; this was therefore carefully explored. Shibboleth has been developed as a means of authenticating users who are seeking to gain access to resources in a multi-resource-holder domain. Figure 2 indicates how Shibboleth works.

When considering such a protocol in the context of e-Certification, we may note that there is considerable complexity involved and a significant set-up time. The pay-off comes in using Shibboleth for resources sited on multiple servers in a single transaction. Furthermore, it specifically focuses on authorisation – is this user authorised to access this resource? It therefore finds a natural home in contexts such as the Grid community and in applications such as "Athens", a bibliographic database linking to multiple sources [6].

However, the e-Certification context has very different requirements. In this case, the single basic transaction consists of an e-Portfolio holder submitting information to an e-Portfolio Receiver, who needs verification that it is authentic from a Certifying Authority. It is also helpful if an e-Portfolio Holder can communicate with the Certifying Authority to confirm awards before submitting them. We are not therefore interested in setting up a session token which can be reused across multiple servers. We are also more interested in validating information than in determining authorisation to access resources, although it is presumably not desirable for the Certifying Authority's database to be made publicly available.

With this in mind, it was apparent that Shibboleth was not appropriate for the e-Certification context, and that simpler protocols would be more efficient and effective.

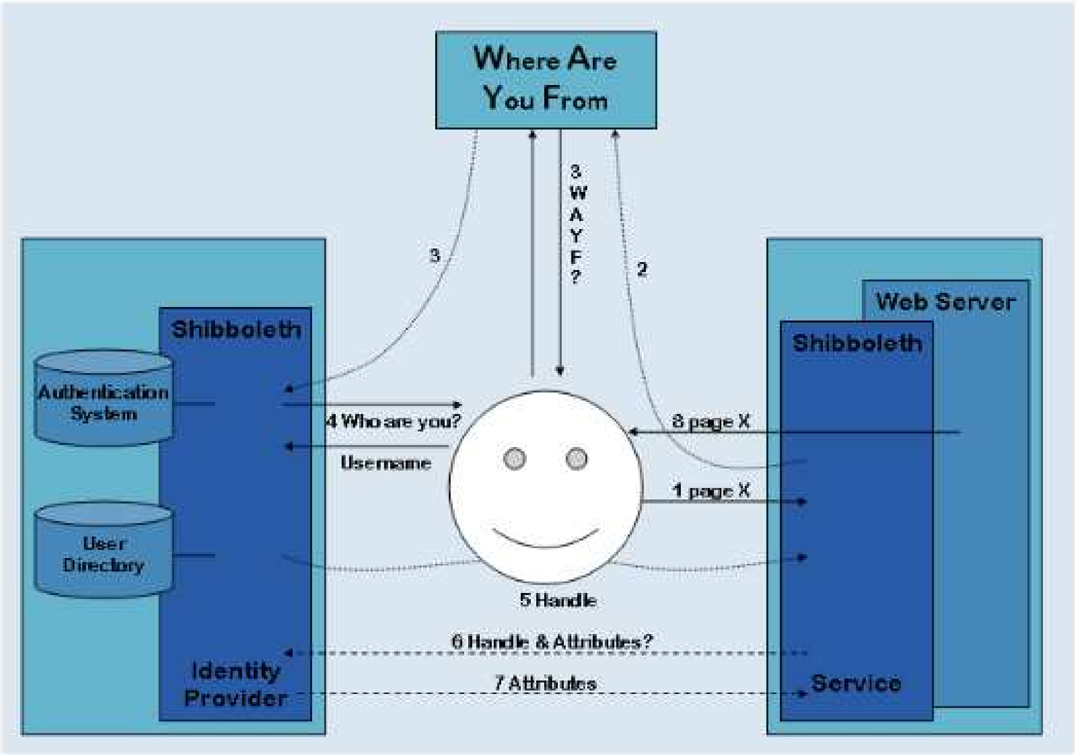


Figure 2: Steps in operation of Shibboleth protocol

A list of requirements was drawn up for the eCert implementation.

1) The system should be a proof of concept, demonstrating how grades and qualifications entered by the user into an e-Portfolio system may be certified.

2) Three stake holders must be considered (user, exam board, potential employer).

3) The user should be able to log onto the system and store exam grades, including a personal statement into his/her e-Portfolio.

4) Grades and qualifications to be certified automatically.

5) User may create multiple views (“eCVs”).

6) User has control over content in each “eCV”.

7) Main page shows all the views in a table and allows editing of views.

8) User controls who can see their views.

9) System to demonstrate how security and authentication can be performed in ePFs.

10) System to be a dynamic web-based application.

11) System to have secure and familiar log in and sign up procedures.

12) Modular structure employed to facilitate future integration with fully-functioning ePFs.

13) User can modify the e-Portfolio whenever needed, perhaps over a period of years.

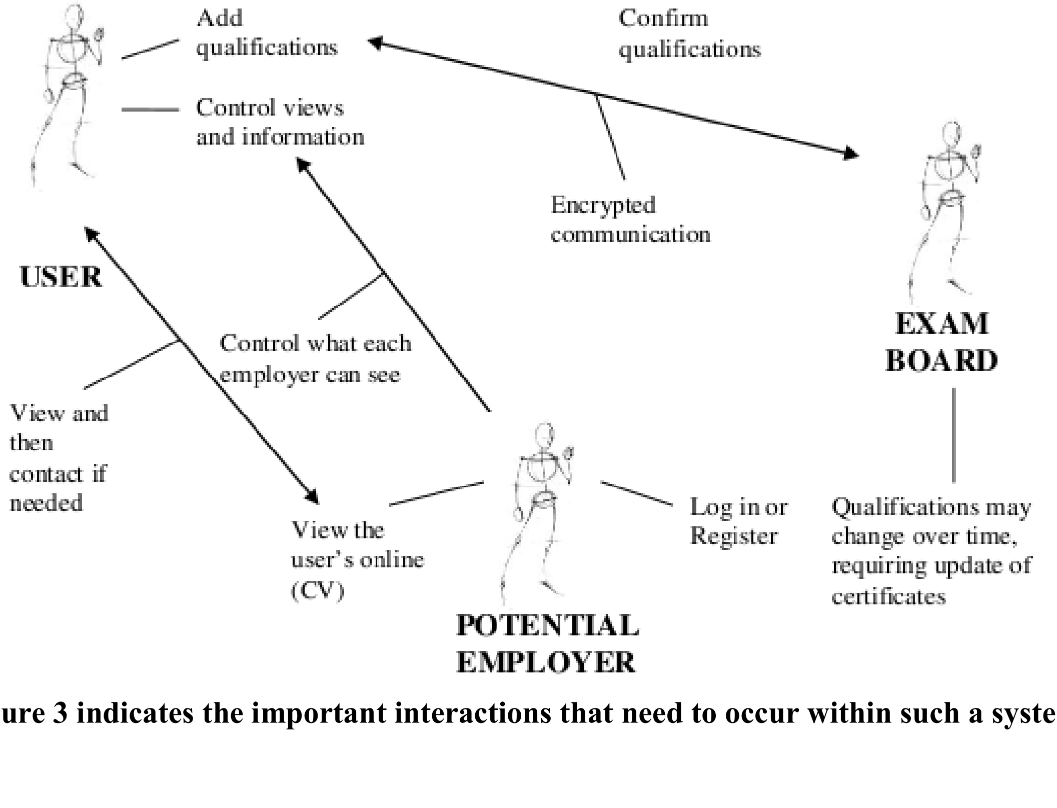

Add qualifications
Confirm qualifications
Control views and information
Encrypted communication
USER
EXAM BOARD
Control what each employer can see
View and then contact if needed
View the user's online (CV)
Log in or Register
Qualifications may change over time, requiring update of certificates
POTENTIAL EMPLOYER

Figure 3 indicates the important interactions that need to occur within such a system.

3. The Security Model

A number of decisions need to be taken about security policy before any implementation can be produced. This not only concerns who can see what and when, but also what the value is of the data concerned. For example, one might decide that information about qualifications is less valuable than banking details, so the level of security could be lower if it aids usability of the system. However, one might decide that the level of security should be higher to prevent identity theft, for example.

For this project, the following decisions were 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

The outworking of these decisions led to some fascinating design criteria. The basic concept was that there would be a Certification Server – the Certifying Authority in the original design. This provides a service to the e-Portfolio Holder (student) who can build up a set of e-Portfolio certificates, each one tailored for a specific e-Portfolio Receiver (e.g. employer). Because of design policy 3 above, it is not possible for the student to browse their awards and select from a list, rather they have to be entered individually. Although this could be annoying for the student, it prevents attackers from intercepting the communication and obtaining all the student's qualifications in one go. Similarly, it prevents the employer from taking the student's details and making a general enquiry to see withheld awards.

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 as in design policy 3 above. The student's profile then builds up with a series of certified claims, and hopefully none denied! 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 final step in building up their profile is for the student to select which awards they want to present to a given employer, which is done via a tick box grid.

Having built up an award profile for a particular employer, the student is now 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.

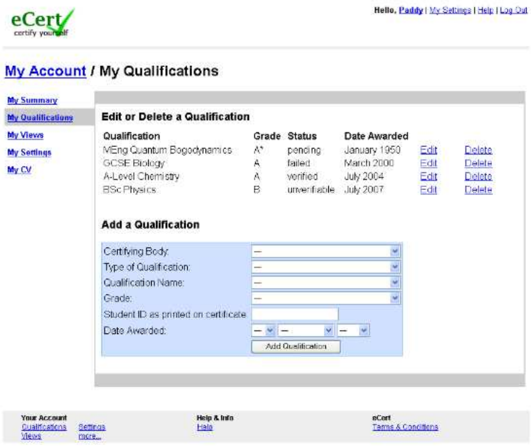
All communications are encrypted and digitally signed so the source can be verified. This entails the use of both public and private key encryption.

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. There are two screens that help in understanding what the system looks and feels like in use. The first of these is given in figure 4, and shows how the e-Portfolio Holder builds up their set of certified awards. In order to do this, they must provide their name, student number, year of award, and claimed award. Both name and number are necessary since a student may change name, or two students may have the same name.

Once this has been done, the student can call up a “View Summary” page where they can allocate awards to employers via a grid as mentioned above. The Server then allocates a code to a particular view which the student can then send to the potential employer. The student can see the view that the employer will get via a “Preview your CV” page as shown in figure 5.



My Account / My Qualifications

Edit or Delete a Qualification

Qualification	Grade	Status	Date Awarded		
MEng Quantum Bogodynamics	A*	pending	January 1950	Edit	Delete
GCSE Biology	A	failed	March 2000	Edit	Delete
A-Level Chemistry	A	verified	July 2004	Edit	Delete
BSc Physics	B	unverifiable	July 2007	Edit	Delete

Add a Qualification

Certifying Body:	--
Type of Qualification:	--
Qualification Name:	--
Grade:	--
Student ID as printed on certificate	
Date Awarded:	-- -- --
	Add Qualification

Figure 4: The eCert Qualifications page

Figure 5: Preview CV page

5. Conclusions

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

Some of the issues arising from this project clearly derive from the standpoint taken on data availability. In the UK, it is understood that, as the person who gained the award, I decide whether I let you (the employer) know about a specific award or not. I don't misrepresent the information, I simply choose how much to tell the employer. In other cultures, it might be considered that all of a student's awards should be public knowledge – this would then radically change the security model one chose to employ.

It has been considered that it would be convenient to distribute digitally-signed e-Certificates of attainment to graduating students. This project has shown that such an approach would need considerable further thought, otherwise a student's award certificates would rapidly appear in the public domain.

Furthermore, such an approach would greatly increase the risk of attack and forgery.

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

6. References

[1] Nottingham University e-Portfolio Project, (2007), http://www.nottingham.ac.uk/e-Portfolio/, Last accessed: 28 January 2008

[2] Rees-Jones, P., (2007), http://www.elframework.org/refmodels/epll/, Last accessed: 28 Jan 2008

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

[4] Wang, L. (2002). Student Perceptions of Relative Advantages in Physical Versus Online Submission of Multimedia e-Portfolio Projects in Graduate Coursework. In P. Barker & S. Rebelsky (Eds.), Proceedings of World Conference on Educational Multimedia, Hypermedia and Telecommunications (pp. 2017-2018). Chesapeake, VA. 2002

[5] European Communities (2008), http://europass.cedefop.europa.eu/europass/home/vernav/InformationOn/EuropassCertificateSupplement/navigate.action, Last accessed: 28 January 2008

[6] ATHENS, (2008), http://www.athens.ac.uk/. Last accessed: 28 January 2008

[7] Shibboleth, (2007), http://shibboleth.internet2.edu/, Last accessed 28 January 2008

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

[9] Nicholas L, et al., (2005), Certified Assessment Artifacts for e-Portfolios, icita, pp. 130-135, Third International Conference on Information Technology and Applications (ICITA'05) Volume 2, 2005

[10] 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