JISC Final Report

Project Information			
Project Identifier	*To be completed by JISC*		
Project Title	A framework of a secure e-qualification certificate system		
Project Hashtag			
Start Date	4th January 2010	**End Date**	31st March 2010
Lead Institution	University of Southampton		
Project Director	Dr. David Argles		
Project Manager	Lisha Chen-Wilson		
Contact email	lcw07r@ecs.soton.ac.uk		
Partner Institutions	(none)		
Project Web URL	http://ecert.ecs.soton.ac.uk/		
Programme Name	Access and Identity Management		
Programme Manager	Christopher Brown		

Document Information			
Author(s)	Lisha Chen-Wilson, David Argles		
Project Role(s)	Project manager and director		
Date	18 March 2011	**Filename**	eCertProjectFinalReport.pdf
URL	http://ecert.ecs.soton.ac.uk/publications/eCertProjectFinalReport.pdf		
Access	This report is for general dissemination		

Document History		
Version	**Date**	**Comments**
0a	15 February 2011	First Draft Final Report
0b	18 March 2011	Second Draft Final Report
1	31 March 2011	Final Report

Table of Contents

1 Acknowledgements

This project was funded by the Joint Information Systems Committee (JISC) under the Access and Identity Management programme. We are grateful for the help and advice of both the ePortfolio team at the International ePortfolio Development Centre in the University of Nottingham and of Clive Church throughout the project.

2 Project Summary

There is a tension in the world of security between a desire to keep control of data centrally, and putting control into the hands of the user. In the world of ePortfolios, confirmation of award data is currently only possible via a centralised service. Using a new signing method to solve what we call the "eCertificate squared" problem, the eCert project has developed a test system to investigate the issues that arise when control of award data is put in the hands of users.

We have published:

1. an open source eCert code library; and
2. a demonstrator indicating how the code library may be used.

The code library enables the secure transfer of documents, and also allows the user to define the scope of the data which should be visible to a reviewer together with the time frame in which it may be viewed, whilst the demonstrator indicates how the code library may be used. These were what we committed to at the start of the project. However, the project has run very successfully, attracting attention from a variety of places world-wide. By reorganising, it has been possible to extend the project without exceeding the original budget. As a result, we have also produced:

3. an example of eCert implemented in “eFolio”, the University of Southampton's own ePortfolio system;
4. an example of eCert implemented in “Mahara”, the widely-used open source ePortfolio system;
5. “Mobile eID”, an example of eCert used for ID verification on the Android mobile phone platform.

These are all available from the eCert project website (http://ecert.ecs.soton.ac.uk/), together with all the project documentation.

3 Main Body of Report

3.1 Project Outputs and Outcomes

Output / Outcome Type *(e.g. report, publication, software, knowledge built)*	**Brief Description and URLs (where applicable)**
Project deliverables	Workpackage1: requirements and specification • Deliverable 1: Problem analysis, use case scenarios, requirements analysis and specifications made available on project website. http://ecert.ecs.soton.ac.uk/publications/workpackage1.pdf Workpackage2: design • Deliverable 2: Design document made available on project website. http://ecert.ecs.soton.ac.uk/publications/workpackage2.pdf • Workpackage3: code library Deliverable 3: The code library http://ecert.ecs.soton.ac.uk/development/ • Deliverable 4: The code library documentation http://ecert.ecs.soton.ac.uk/development/ • Workpackage4: demonstratorDeliverable 5: The eCertificate demonstrator http://ecert.ecs.soton.ac.uk/development/ • Workpackage5: concept validation Deliverable 6: The system test and evaluation results http://ecert.ecs.soton.ac.uk/development/document/eCert.pdf Workpackage6: report and documentation Deliverable 7: Reflective report http://ecert.ecs.soton.ac.uk/publications/FinalReport-v0c.pdf • Deliverable 8: System documentation http://ecert.ecs.soton.ac.uk/development/document/eCert.pdf
Additional subprojects	Additional to the original plan, the eCert protocol has been further evaluated thought two subprojects: • The evaluation for the use of eCertificate in ePortfolio was carried out as a GDP (group development project), by 4 Masters degree computer science students, under a subproject named “Integrating eCertificates within ePortfolio Systems”. ○ During this time the GDP Group has made a considerable number of observations regarding the existing eCert code base and subsequently formulated several recommendations to improve its accessibility and scalability. ○ The group has explicitly produced a working web

	service (or Application Programming Interface - API) to be positioned above the code base and provide public-facing methods for eCertificate verification. Methods have also been provided to allow the downloading of transcript and evidence files, and the modification of their visibility parameters. ○ In addition to this, the GDP group has developed mechanisms for eCertificate integration within the eFolio and Mahara platforms. Both systems can now be fully utilised by those with eCertificate qualifications. ○ With these developments in mind, the GDP group has completed all of its primary and secondary goals. • The evaluation for the use of the eCert protocol in other domains was carried out under a subproject named "eCert with Mobile eID". This subproject investigated the features of eIDs and the mobile environment, compared eCertificate with eID, and developed a working solution for a mobile eID system that is managed by the eCert protocol. The successful test and evaluation results indicated that the proposed eCert protocol will not only meet the eCertificate challenge, but also solve eDocument transmission security issues, and can be applied in a wide variety of domains.
Online information	Within the first month of the project there was a website created, http://ecert.ecs.soton.ac.uk/ , informing people about the project. A project blog, http://blogs.ecs.soton.ac.uk/ecert/, and wiki, http://wiki.ecert.ecs.soton.ac.uk/index.php/Main_Page, have also been created to record our thoughts, project meeting minutes, and development documents.
Project documents	Licences: Creative Commons licence [txt] Project workshop reports: First workshop report [pdf] Second workshop report [pdf]
Conferences & Publications	Chen-Wilson, L., Gravell, A. and Argles, D. (2011) Giving You back Control of Your Data: Digital Signing Practical Issues and the eCert Solution. In: *The World Congress on Internet Security (WorldCIS-2011)*, 21-23 February 2011, London, UK. Schiano di Zenise, M., Vitaletti, A. and Argles, D. (2011) A User-Centric Approach to eCertificate for Electronic Identities (eIDs) Management in Mobile Environment. In: *The World Congress on Internet Security (WorldCIS-2011)*, 21-23 February 2011, London. Argles, D., Chen-Wilson, L. and Guan, T. (2010) Solving the e-Portfolio Certificate Problem. In: *EdMedia 2010*, 29th June - 2nd July 2010, Toronto, Canada. (Submitted)

	Chen-Wilson, L. and Argles, D. (2010) Towards a framework of a secure e-Qualification certificate system. In: *The 2nd International Conference on Computer modeling and simulation (ICCMS 2010)*, 22-24 January 2010, Sanya, China.
Other conferences and presentations:	Project outline: JISC start up meeting, 3rd March 2010, Greenwich, UK [ppt] eCert requirements and the proposed system design: Project first workshop, 15th April 2010, Nottingham, UK [ppt] E-qualification Certificate System for E-portfolio: Project second workshop, 7th September 2010, Nottingham, UK [ppt] Giving you back control of your data: FAM10, 7 September 2010, 5th October, Cardiff, UK [ppt] Digital signing practical issues and eCert solutions: WorldCIS2011, 21-23 February 2011, London, UK download to play offline London learning forum, 5-7 June 2010, at the Savoy Place, London JISC Innovation Forum, 28-29 July 2010, at Royal Holloway, Egham, UK
Source code, online demo and videos	The code and technical documentation is available as open source under the new BSD license. Code library: • source code • JavaDoc eCert demonstrator: • source code • online demo system • video • documentation eCert for eID • source code • video • publication
Knowledge and experience	This project has enabled the team to visualise and construct a user-centric solution to the problem of maintaining

	confidentiality in a world of linked data. As the project has generated interest and gained momentum, it has become possible to explore the initial concept in more depth, to define more clearly what is at the heart of the "eCert" concept, and to develop examples of how the protocol may be applied in widely varying contexts. It has also been possible to develop some of these examples as practical demonstrators, which has led to a deepened understanding of issues that arise when theory is applied in practice. The project has had its fair share of problems throughout its life, including the departure of the main code developer halfway through the development cycle. This has been an object lesson for the team in noting that risk assessment is not an arbitrary exercise done to meet requirements, but an essential part of pre-project planning. In spite of considerable experience and care taken to ensure a shareable approach to the task of programming the code library, we still hit the problem that a number of aspects of the initial code library proved to be idiosyncratic and potentially problematic. Running the subprojects proved invaluable in the task of identifying such issues and correcting them before the end of the parent project. Summarising the issues learnt in this domain: • Time spent at the outset developing a sound structure for the code to be developed is time well spent. This should be done before a line of code is written. • It is important to insist that designs and structures are shown to the management team. If there is reluctance to make these visible, there is probably a problem. • Learn to ask the right questions. Try and frame the questions to make sure that you will get at the heart of the matter. • Team development is potentially expensive, but pays huge dividends. In particular, paired programming can be enormously beneficial, especially in the long term. • Plan for a layered software structure. With a suitable "bridging layer," it is possible for development to continue on the underlying code library whilst practical applications are being simultaneously developed. This has the further advantage that potential problems with the underlying code library can be identified whilst initial development is still live. • On a practical note – make sure that server applications do not use static variables! It will be clear from previous sections that the project has generated global interest from Australia to the USA and Canada. Whilst there has been a focus given to dissemination in the UK, interaction with expert audiences world-wide has been extremely helpful in assessing and refining the eCert principle.

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

Background

In this project, we began by noting that paper-based portfolios have been in use in education in the UK for a number of years, particularly for the teenage 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. More recently, the development of online personal ePortfolio systems has been encouraged, with the intention that such systems should ultimately replace the current paper-based system.

We noted that ePortfolios offer a number of advantages, and that whilst they are good for the younger learner group, they can also be of enormous help to lifelong and distance learners, with frequent minor portfolio updates encouraging such learners to persevere.

Abrami[1] notes that it is difficult to authenticate the evidence in e-Portfolio. The study of how we can engender trust in our on-line versions of certificates/qualification records, and making sure that our sensitive data are not being misused, is still at an early stage. Currently, there are methods, projects, and commercial systems present in the related domain, such as digital signatures, eCert[2], and Europass[3]. However, in each case, they provide limited functionality, and therefore are insufficient to satisfy our requirements.

In order to solve these problems, we determined to implement an electronic version of qualification certificates (e-Certificate). Research at the Learning Societies Lab at the University of Southampton had noted that potential security loopholes exist in the validation of paper qualifications, and that an e-Certificate system offered the possibility to improve security in this area. This project was therefore based on its previous work and set out to explore the potential of a possible mechanism for transferable e-Certificates in a user-centric context.

Aims and Objectives

Our aims were to implement an electronic version of a Qualification Certificate System, which would overcome the authorization problems that we faced in ePortfolios. This eCertificate system needed to meet the following specification:

1. to be at least as valid as paper-based certificates;
2. to be usable either as a standalone application or served within other applications, such as ePortfolios;
3. to be easy to use;
4. to suit all levels of students;
5. to include high security methods to prevent forgery;
6. to give the students control over the usage of such eCertificates;
7. to provide a verification method;
8. to secure the e-Certificate system, not just the eCertificate.

Methodology

The eCert project used mixed-model research methods, operating at two levels, strategic and technological, through four phases.

At the strategic level, the SORM methodology was employed for the system development phase. This involved producing an eCertificate use case study, gap analysis, technical investigation, and system design. During the development, the Delphi method was also employed for the design review phase. This included interviews and workshops with institutional and national representatives to consult on matters of procedure, whilst the named consultants (Nottingham and EdExcel) were

---

1 Abrami, P.C. & Barrett, H. *Directions for Research and Development on Electronic Portfolios.* Learning and Technology, 2005. 31(3)

2 Chen-Wilson, L et al, *Secure Certification for ePortfolios*, in ICALT: International Conference on Advanced Learning Technologies, 2008. IEEE: Santander, Spain

3 European Communities. *Opening Doors to Learning and Working in Europe.* Available from http://europass.cedefop.europa.eu/europass/home/hornav/Introduction.csp

consulted with regard to fit within the overall ePortfolio Framework. The consultants were also involved with regard to helping to ensure that the national workshops were appropriately set up and focused.

At the technological level, a demonstrator was built to test the design during the implementation phase. The Delphi method was employed once again in the technological review phase to evaluate the whole system; this was done by bringing the developed system back to the selected representatives to test whether it meets the requirements.

Implementation

The system was implemented in two parts: a code library and a demonstrator. The identified service profile and selected techniques from the gap analysis were used for the code library to base a reference implementation, ready to integrate within a Service Oriented Architecture. A demonstrator was produced to represent the whole framework design that was supported by the library functions.

The core of eCert system is a code library, providing basic support for the eCert issuing, management, and verification system development. The code library is built in Java, with the programming environment of J2SE 1.6. It includes a number of features that meet the requirements of the eCert demonstrator development:

- Support for digitally signing XML documents in enveloped, enveloping and detached ways, compatible with the ESTI European Digital Signature standard.
- Support for digitally-signing and verifying files with given key stores.
- Support for KeyPair generating (varying lengths), converting (from/to String) and file encryption/decryption with RSA/DSA algorithm.
- Support for domain file processing, including production of qualification files, addition of file metadata, setting of access control, digital signing of multiple prepared files, full verification of signed qualification files, and file compression and decompression.

A web interface demonstrator has been produced on top of the code library. The system is developed in MyEclipse Enterprise Workbench 8.5, and implemented using JSP, JavaScript (jQuery), and MySQL for database. The website provides the user interface for the issuing, management, and verification systems, with calls to the code library for functional support. All web pages share a common interface design for system consistency, with different colour schemes to distinguish between the three systems. Different pages are rendered by loading different sub-pages in the menu and content areas using Ajax.

3.3 What did you learn?

The eCert project set out to investigate the viability of putting certified information in the hands of the user, and giving them the opportunity to set the scope and time frame for which others might be able to view such data. At the outset of the project, one domain expert confidently stated that users could not be trusted with their own data, and that such an approach would ultimately compromise data security. Having implemented the eCert system, and having also deployed it in three practical scenarios, it is evident that the approach works, and is no less safe than centralised approaches.

The mobile eID subproject was initiated with permission because the opportunity arose to implement the concept, and it looked to be something that would provide a valuable alternative test. In the event, it proved not only successful, but also extremely interesting. Current mobile technology puts limitations on what can be done, but it is immediately apparent to anyone using it that such an approach is simple to use and immensely powerful.

As the project has progressed, it has become apparent that the eCert approach is widely applicable to a range of scenarios where certified information needs to be transmitted securely, whilst giving the owner the opportunity to retain control over their data.

At a different level, lessons have also been learnt about how to manage changes in plan. The project has not been without its challenges in terms of unexpected staff departure, and unavailability due to ill-health, for example. The lessons learnt here have been noted above in section 3.1.

3.4 Immediate Impact

As an exploratory project, the eCert approach has not yet been implemented with live groups of users, only in test-bed situations. However, both the use of eCert in an ePortfolio context, and the use of eCert in a mobile eID context have caused considerable interest. There is interest from the eWork, the Australian Flexible Learning Framework project, with regard to ePortfolio usage, interest from the University of Sapienza with regard to developing the mobile eID aspect of eCert, and interest in eCert with regard to the secure transfer of documents.

3.5 Future Impact

The main impact for eCert lies in the future. Now that the principle has been proved, and the protocol tested in differing contexts to ensure its broad applicability, it needs to be tested with real users. Having produced an implementation in Southampton's own eFolio system, it will be straight-forward to set up a project to evaluate this with specific groups of students.

Because of the way in which the eCert project has spawned two subprojects building on the code base, the code library has already been developed to ensure it is comparatively easy for other developers to take it and implement the eCert protocol in their own systems. It will be important to track such take-up, give any support as necessary, and learn from any issues that might arise as a result.

4 Conclusions

Overall the project has been a great success, and in many ways has exceeded the original aims.

The code and technical documentation can be used either directly or as a case study to further investigate the topic.

The methodology was very successfully applied in this case and lessons learned could be used by similar JISC projects in the future.

5 Recommendations

As a result of running the eCert project, we now know that the eCert protocol will work in practice in a variety of contexts, giving users control over who may see their data and for how long, thus giving them improved protection against identity theft, for example. We also have the eCert code library which has been tested by two different groups of developers via the two subprojects and refined to ensure it is easy to use.

The next step is to roll out an eCert-based system and to test it with real users. Because this involves the security of real user data, the development team would prefer a carefully-planned, phased roll out. Thus it would be good to see:

1. A carefully-monitored trial with a specific group of students in a local institution (e.g. on a single course).
2. An institution-wide roll-out, again with students located within the institution.
3. A roll-out that crosses institutions, for example covering a local area, and with FE/HE cross-over, focussing on say the HE admissions boundary.
4. Alongside the ePortfolio roll-outs, it would be good to see a prototype system set up to evaluate the potential for student data to be kept on smartphones, so that university smartcards could be replaced by a smartphone app. The eCert project has demonstrated how this may be achieved securely and operated simply.
5. The GDP ePortfolio implementation subproject indicated that there are issues relating to the implementation of eCert within different ePortfolio systems. This could be worth evaluating, although it doesn't relate to the value of the eCert protocol itself, but on the design of the ePortfolio sytem.

6. A further development of the eCert protocol would be to use it to cover areas of student-related documentation that are currently problematic, such as files relating to disability, periods of ill-health, and matters relating to “Special Considerations”. The eCert protocol gives a solution to enable time-limited access for restricted groups to sensitive information. Thus a member of a “Special Considerations” panel could be granted access to a student’s personal information for the duration of the panel meeting only. This application is currently only at the design phase, so it needs to be built and tested first to ensure that it works before it can be evaluated in practice.

6 Implications for the future

The eCert protocol is an entirely new concept – were we to be in industry, we would patent it! It is clear from the results of this project that the eCert protocol is not just a solution to the problem of putting control of ePortfolio award data into the hands of the user, it is a useful solution to a wide range of problems.

The code library has been published as agreed at the start of the project, is in the public domain, and is accessible via the usual mechanism of being placed on Source Forge together with the source code and all related documentation. It is therefore available for anyone to use and to implement an eCert solution in their own application.

The lead mobile eID developer has expressed an interest in taking the project through to the next step of hardening the application and selling it. This would involve producing it as an app on the Android “Market”, and it would probably sell for a small amount (a few pounds or euros). If so, it would then generate an income stream, and this might then lead to pressure to develop the app for the iPhone market as well, providing another platform for the eCert protocol to be deployed on.

In the meantime, the replacement core code developer remains at the University of Southampton, and is likely to be there a while longer because of his study commitments. This, together with the fact that the development team is reasonably large, should ensure that there is developer support available for the next two or three years at least. Follow-on projects will also ensure that support continues.

7 References

All helpful documentation, including links to the code library, can be found on the eCert website at:

http://ecert.ecs.soton.ac.uk/

8 Appendices (optional)

All helpful documentation can be found on the eCert website at:

http://ecert.ecs.soton.ac.uk/