Solving the e-Portfolio Certificate Problem

David Argles, Learning Societies Laboratory, University of Southampton, UK, da@ecs.soton.ac.uk

Lisha-Chen-Wilson, Learning Societies Laboratory, University of Southampton, UK, lcw07r@ecs.soton.ac.uk

Tao Guan, Learning Societies Laboratory, University of Southampton, UK, tg2@ecs.soton.ac.uk

Abstract: ePortfolios are of particular interest as a means of supporting and encouraging life-long learning and continuing personal development. A current problem in this context concerns the inclusion of certification of attainment – the electronic equivalent of paper award certificates. At its heart is an interesting problem of three party trust extended over the lifetime of the student. This paper outlines the key issues, offers a proposed solution, and indicates how work is proceeding on an on-going UK-funded project which will deliver and evaluate a demonstrator to test the effectiveness of this solution.

Introduction

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. Such an approach is favoured because it can engender an atmosphere of support and encouragement in terms of maintaining a life-long commitment to personal growth and development. Of increasing interest is the concept of an on-line "ePortfolio" which enables greater power and flexibility in displaying achievements. In the UK, a number of projects have been implemented, such as the eP4LL project (Rees-Jones et al, 2006), which have led to the development of a reference model (Rees-Jones, 2006). Research indicates that such ePortfolios offer a number of advantages over paper-based ones, such as the potential for the inclusion of a rich set of materials; an ePortfolio may include dynamic art or film that would be impossible to include in a paper-based portfolio, for example (Chen-Wilson et al, 2008).

One aspect of ePortfolios that has not yet been adequately addressed is that of certification, where certificates of attainment may be presented in support of an application for a job or a place on a course of further study, for example. The process of confirming the veracity of an academic award via paper certificates is well established, and the potential for exploitation is also well understood. In the on-line world, the concepts of digital signing, watermarking, and non-repudiation are also well understood, with technologies available to support such processes. However, in the case of ePortfolios, the certification of student attainment presents an interesting problem, since it is difficult to authenticate the evidence in this situation (Abrami, 2005). Conventional verification normally focuses on two-party authentication, with a third party typically involved as an arbitrator, or "trusted third party". However, we will see that in the ePortfolio context, three parties will all need to establish mutual trust, with the arbitrator being a fourth party. Other interesting challenges also present themselves in this context.

In order to explore these issues, a government-funded project has been set up and is currently running in the UK. The aim of the project is to clarify design requirements, to build a demonstrator that meets these requirements, and then to test the demonstrator to check that it solves the problems identified. This paper documents the lessons learned so far about how we may best approach the validation of students' claims of attainment.

In the context of on-line security, the term "eCertificate" is widely used to refer to any form of electronic certificate that is used to give assurance. This creates a problem in the current context however, since we wish to reserve the term "eCertificate" specifically for the electronic document that validates a student's attainment in the educational (possibly e-) Certification process, and this definition will be used throughout this paper. Although the use of a term such as "eDiploma" would help to avoid such confusion, the corresponding term "eDiplomafication" doesn't work well.

The Problem

We wish to implement an electronic version of qualification certificates (eCertificates) that are at least as valid as the paper-based certificates, and that have currency either as a standalone document or within other applications, such as ePortfolios. It needs to be easy to use and to suit all levels of students while including high security methods to prevent forgery and other forms of abuse. The students need to have control over the usage of such eCertificates, and there must also be a verification method provided so the receiver of such a certificate can check its validity. The eCertificate system needs to be secured as well as the eCertificate.

We may note that an eCertificate system involves three processes: issue, distribution, and verification. The certification process for academic achievement includes the processes of registration and examination, and can be paper-based, computerised, or practical. The certificates, as the end result of a successful certification process, may come with a time limitation, so that revocation and re-certification is required (Shore, 1994). Therefore, an eCertificate system requires personal data and qualification records to be stored electronically to identify the person we are issuing to, and to verify that they have passed the relevant exams. The system will also need to have a function for validating and revoking any issued eCertificates when necessary, since some awards will time-limited (e.g. as in the case of First-Aid courses), and in other cases it could be later discovered that the award is invalid, for example if plagiarism has been discovered.

In drawing up a design for an eCertificate system, we may note that different countries have different cultures, a different understanding of what protections should be provided by an eCertificate system, different approaches to data protection, and different legal frameworks. In order to deal with this, work on the current system is focused on the UK situation, although the requirements for other approaches are being borne in mind.

The "Three Party Authentication" Problem

The eCertificate has three stakeholders, as shown in Figure 1: the issuer, owner, and reviewer. Three processes are involved: issue, distribution, and verification.

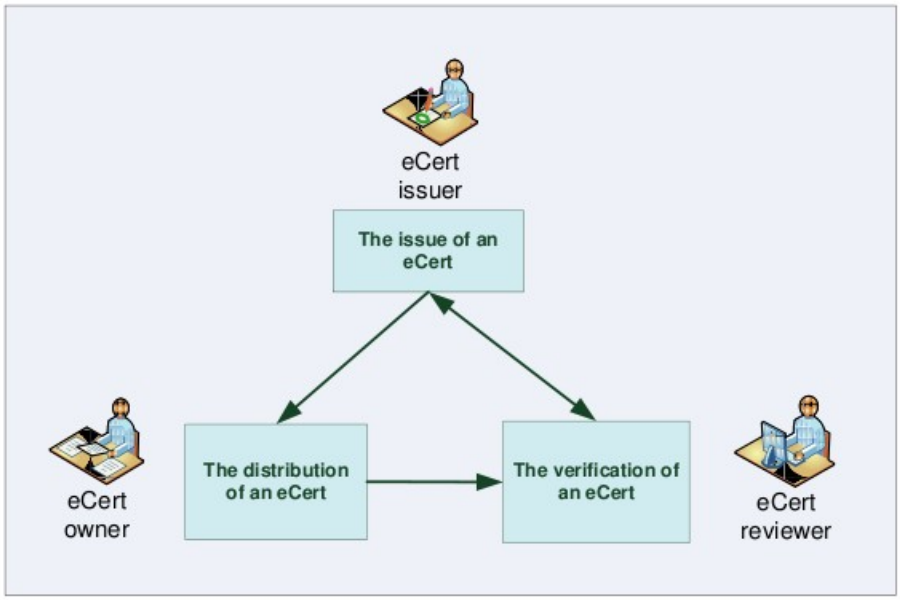

Figure 1. eCertificate Stakeholders and Activities

An eCertificate issuer is a body that creates and issues certificates, such as a college or a university. They may issue a huge range and number of eCertificates; and restrict database access control for any incoming verification request in order to minimize database attacks.

An eCertificate owner is the certificate holder who has successfully passed the qualification certification process and gained the award, such as a student or a graduate. They may gain qualifications at any age or stage of life; have qualifications awarded by a range of eCertificate issuers; have either extensive or little IT expertise; and they may or may not have an ePortfolio account.

An eCertificate reviewer may be a body or a person who receives the eCertificate in support of an application. They may represent either an academic or a business concern; could be a small or large organisation; may have a low or a high IT skills threshold; may have a small or a large throughput in eCertificates; and they may need check awards from a range of issuers.

We may note that this "three party authentication" requires trust to be established between all three parties. The issuer needs to maintain a reputation for credible awards; they do not want to be known as an awarding body that is linked with suspect eCertificates, for example, so it important that their eCertificates can be proven not to have been tampered with. The owner (student) also wants to know that they can trust the credibility of the award they have obtained; but they also need to trust the reviewer not to misuse the information on the certificate, for example by harvesting the information and selling it on to recruitment agencies. The reviewer needs to be able to trust issuer, not only to maintain standards, but also to have protected against fraud (e.g. if a corrupt employee were to accept a bribe to produce a fake eCertificate); and similarly, to trust the owner not to have tampered with the eCertificate.

The "Lifetime Validation" Problem

In standard approaches to computer security, authentication and validation are typically considered as instantaneous activities – the system authenticates a user and validates their request or data now. Longer periods of time are necessary in transaction processing, but authentication and validation are still only relevant for the duration of the transaction. Indeed, long periods of authentication are undesirable, so it is common for "sessions" to be "logged off" or terminated if they exceed a predetermined length of time.

If we consider the three party authentication problem outlined above, it can be seen that the effective "transaction" period lasts for the entire lifetime of the eCertificate owner. Considering the parallel of paper certificates, many of us can probably think of people who have continued studying well past the age of retirement. Yet they may still be presenting awards they acquired as children, decades previously.

The important factor in this is the lifetime of the eCertificate owner. During their lifetime, it is almost certain that awarding bodies will have come and gone, so an eCertificate system needs to be able to validate an award long after the issuer has ceased to exist. Similarly, reviewers will come and go, although this is less of a problem in practice. The implication of this is that an eCertificate system needs to be independent of both issuer and reviewer and to be able to provide a mechanism for the eCertificate owner to continue to provide evidence of their attainment long after the issuer has disappeared.

The "eCertificate Squared" Problem

Digital signatures can be used to to provide authentication, to ensure integrity, and to offer non-repudiation of a communication. Thus, using such an approach can provide proof of the source of a document and evidence of any modification. The use of Cas can also provide a chain of trusted nodes. However, it is not possible to certify the veracity of an XML structure; as a result, it is not possible to assert that an XML fragment is genuine. Thus it is possible to validate the signer, the signer's CA, and any modifications – but it is not possible to validate the content of the document itself. This is crucial to the eCertificate, as the signed document is itself a certificate which may have a period of validity, or may even be revoked at a later stage. We may call this problem the "eCertificate^2" (eCertificate Squared) problem, since we need to have a certificate of a certificate.

The Proposed Solution

Content Extraction Signatures (CES) enable us to tackle the privacy issue by adopting the CES approach with created access tokens. CES have been developed to "enable selective disclosure of verifiable content" (Bull et al, 2003). CES would allow an document signer to sign the document in fragments with a set of signatures, and these individual fragments can be blinded or extracted by the receiver with the corresponding keys. An access token controls who can see the document and for how long. Applying these to eCertificates, the initial access token and qualification fragments can be signed individually, and then extracted, reformed, and signed by the student with a new access token. With different sets of access values, the eCertificate may then be sent to different reviewers with different access levels while the signed certificate fragment remains untouched. However, we need to lock the document to prevent further extraction, so that the reviewers cannot get hold of the qualification fragment without the required access control.

The system design aims to solve the problems that arise from our current situation, satisfy the eCertificate use case requirements, and avoid the drawbacks that the existing systems have. The development of the system will adopt the SOA of the e-framework to meet the distributed stakeholder user case. SOA allows developers to build applications from sets of services with well defined interfaces and is achieved without "*tight coupling between transacting partners*" (Liu et al, 2003). When used with interoperable ePortfolio XML schemas, this makes it easy for any ePortfolio vendor to integrate eCertificate services into their application; hence enabling and encouraging user take up and participation between users using software from potentially different providers.

The key stakeholders have already been identified, and are indicated in figure 1 above. Following on from this, Use Case Scenarios have also been identified and are given in table 1. From these use cases, it is possible to derive the system design. Further details of this are given in (Chen-Wilson et al, 2010). In overview, the system design works as follows. The institution creates and issues a digitally signed, timestamped, and access controlled eCertificate to the specified student through a secured emailing system. The student then views it and sets new access controls to the received eCertificate through a central system before sending it out to further reviewers. Next, the reviewers use the same central system to view and verify the access controlled eCertificate. This is shown diagrammatically in Figure 2.

processes	**Scenarios and conditions**
create	An exam board checks that the students have successfully passed the particular exams, and are who they claim to be, and then creates the eCertificates accordingly. This involves identification and verification against the exam board's database. The creation process needs to have standard control for both low and high level qualification certificates in order to suit educational institutions across a wide range.
issue	The exam board issues the eCertificates for students. But it may need to be withdrawn at a later stage. This needs security methods to (a) indicate that the eCertificates are issued by the exam board, in order to prove its genuineness, and prevent unauthorised editing and copying after issue; (b) give support for the withdrawal mechanism; (c) issue the eCertificates
receiving award	The students receive their eCertificates, and view the contents. This needs security methods to ensure that no-one other than the students themselves can view their own eCertificates at this stage.
manage	A student identifies certain eCertificates to be visible to particular employers. The student needs to be able to control which eCertificates may be seen by which employers and for how long they would be valid. The system design needs to be user friendly and suitable for users with low IT skills
distribute	A student sends the selected eCertificate(s)to potential employers. The student should be able to send the eCertificate(s) alone or within an e-Portfolio. For students sending the eCertificates through ePortfolio accounts, only the selected eCertificate(s) in the account should be visible to the employer(s).
review	An employer views the received eCertificate(s). This needs security methods to (a) ensure only the specified employer can view the eCertificate(s), but not anyone else; (b) protect from modifying and unauthorised copying.
verify	The employer verifies the received eCertificate(s). The system needs to be able to verify all level qualifications that are issued using the same standard from any educational institution nationwide, and check that the eCertificate and the key are both still valid.

Table 1: Use Case Scenarios for eCertificates

The system design is constructed in two parts: an issuing system and an online central system. The issuing system can be installed in individual institutions, and produces the certificate of attainment. The online central system itself is constructed in a further two parts; a management subsystem (for students) and a verification subsystem (for reviewers). It provides services for eCertificates that are issued from any associated institutions, and is the single reference point nationwide. This prevents confusion where the reviewers don't know which system to choose or which can be trusted, especially when they are likely to receive many eCertificates issued by different institutions. This will also has the advantage of enabling close monitoring and control against forgery and abuse within the system.

Any institution that would like to use the system to issue eCertificates will need to be certified first, ideally by a professional education body, e.g. the Ministry of Education. This should be the apex of the trust node, and should ensure that no disreputable institutions can be validated. All members that represent their institution and confirm the institution's awards, e.g. the registrar, will also need to be certified, and should be traceable back to the institution. This is shown in Figure 2.

Each student also needs to register a student account when they start study at six form or college (or the level at which they will start to receive award certificates). The registration process verifies who the student is in the same way that they enrol on a course at college). In this process, each student is assigned a student id which is unique nationwide and lasts for the entire life of the student. Every eCertificate that the student achieves contains this id as proof of ownership.

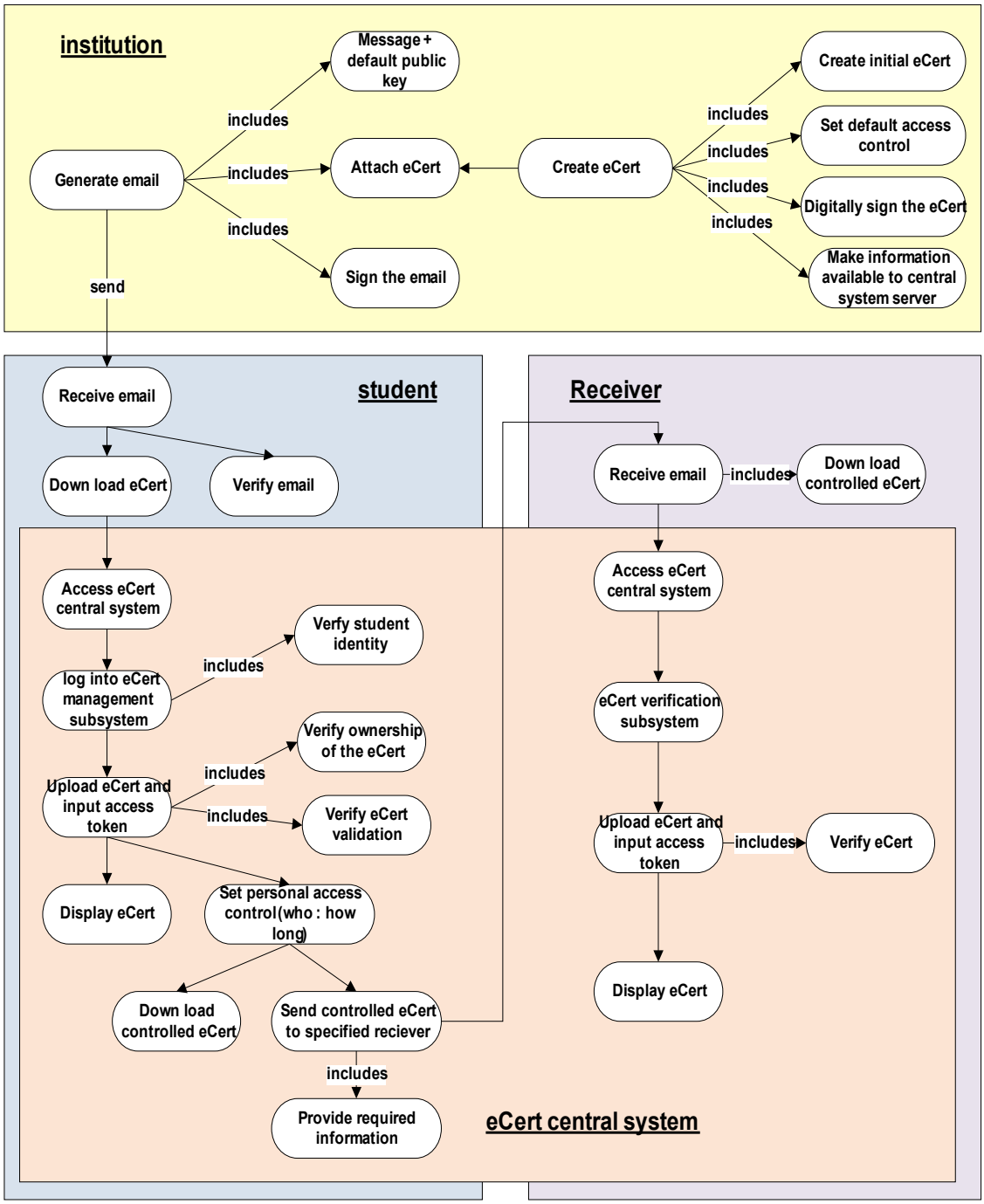

Figure 2: eCertificate System Design

The Test Plan

In order to test the proposed solution to the eCertificate problem, the UK-based Joint Information Systems Committee (JISC) have funded a project to confirm the system design, to develop a demonstrator, and then to test the demonstrator with the UK ePortfolio community. The project is planned to begin in January 2010 and to complete by the end of December in the same year. The various key stages of the project are illustrated in figure 4.

Pre-project work has been undertaken to validate the design so far, and initial results have been encouraging. Concerns include potential file size of the certificates which must be sent out by email; and there is concern over the nature and role over the central system. In the UK, government has a track record of losing entire databases of

sensitive personal information! However, it would seem that the current proposed system is consistent and sound, and will enable the design requirements to be met in full.

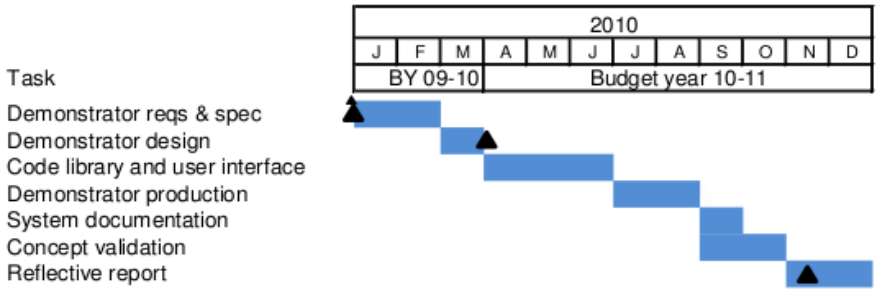

Figure 4: Gantt Chart indicating key stages in the funded "eCert" project

The nest steps are to consult the UK ePortfolio community for further feedback, to build the demonstrator, and then to test this out, again within the UK community, to ensure that the design works in practice, not just on paper. However, it would be extremely helpful to also have feedback on a wider scale from other countries. This will enable us to keep the wider view in mind and to avoid potential dead-ends

Conclusion

In this paper, we have proposed a solution for a secured eCertificate system. This system design does not require any eCertificate copies, or sensitive data such as private keys, to be stored in the system, yet it provides all the required services through a secured environment. This feature offers the huge twin advantages of both minimising the risk of being attacked, and of saving storage, especially when its intended usage is (at least) nationwide, and the eCertificates themselves need to last for life.

The current funded phase of this project entails the production of a demonstrator to test these ideas out. It will be essential to gain the views of the community across as broad a spectrum as possible to ensure that the design delivers an appropriate, relevant, and workable solution. If successful, the project will deliver a set of open-source tools operating as web services that may be employed by other products such as proprietary or open-source ePortfolio systems, for example.

References

Rees Jones, P., A. Smallwood, and S. Kingston, (2006) e

Portfolio for Lifelong Learning. Project Report. JISC: Nottingham.

Rees Jones, P., (2006), Specifying an e-Portfolio: a Personal View. CETIS / JISC: Nottingham.

Chen-Wilson, L. et al., (2008) Secure Certification for e-Portfolios, in ICALT: International Conference on Advanced Learning Technologies. IEEE: Santander, Spain.

Abrami, P. C., & Barrett, H. (2005). "Directions for research and development on electronic portfolios." Learning and Technology, 31(3).

James H. Shore, S. C. S. (1994). Certification, Recertification, and Lifetime Learning in Psychiatry.

Chen-Wilson, L, et al, (2010) Towards a Framework for a Secure E-Qualification Certificate System. International Conference On Education Technology And Training, IEEE: China

Bull, L., P. Stankski, and D. McG. Squire, (2003). Content Extraction Signatures using XML Digital Signatures and Custom Transforms On-Demand, in The Twelfth International World Wide Web Conference. Budapest.

Liu, Q., R. Safavi-Naini, and N. Sheppard, (2003). Digital rights management for content distribution, in Conerences in Research and Practice in Information Technology. Austalian Computer Society.

Acknowledgements

The authors would like to thank the UK-based Joint Information Systems Committee (JISC) for the funding provided to develop this e-Certificate demonstrator.