Giving You back Control of Your Data
Digital Signing Practical Issues and the eCert Solution

Lisha Chen-Wilson, Andrew M Gravell, David Argles
Learning Societies Lab, School of Electronic and Computer Science, University of Southampton, United kingdom
{lcw07r, amg, da}@ecs.soton.ac.uk

Abstract

As technologies develop rapidly, digital signing is commonly used in eDocument security. However, unaddressed issues exist. An eCertificate system represents the problem situation, and therefore is being used as case study, in a project called eCert, to research for the solution. This paper addresses these issues, explores the gap between current tools and the desired system, through analysis of the existing services and eCertificate use cases, and the identified requirements, thereby presenting an approach which solves the above problems. Preliminary results indicate that the recommendation from this research meets the design requirements, and could form the foundation of future study of solving digital signing issues.

1. Introduction

As digital technologies continue to develop rapidly, these impact on many daily tasks which rely on technology. Many of our paper-based documents are being gradually replaced by their electronic versions, such as eTickets, email, online banking, and ePortfolios. These technologies are powerful, flexible, and bring huge advantages. However, when come to transfer digital data between three or more unknown parties, there exists a major security issue: how can the receiver believe that the transfer data is from the expected person, and that it has not been modified in any way; and how can the sender ensure that their data will not be misused.

Example 1, An electronic version of qualification certificate (eCertificate): An eCertificate will be issued to a learner by an exam board, and then further distributed to selected reviewers by the learner. While forged certificates exist in paper-based certificate systems, this problem also exists in the electronic version of certificates as digital documents can be easily copied and modified.

Example 2, Mobile IDs: The traditional method of proving your age, vocation, or skills are by using all sorts of ID cards, such as citizen card, student card, and driving license. It would be nice if we could integrate all these required proof documents into our mobile phone, letting it become the only device that we may need to carry when we leave home. However, we are facing security issues, such as how can we let the guard of a pub believe that the age proving eDocument on the mobile truly belongs to you, is issued from the expected authority, and has not been modified since?

The common problems: There are lots of similar scenarios between these two cases. They represent a common situation that authentication of data is required when transmitting between two or more, but not always known, parties.

They both involve trust between three stakeholders, the eDocument issuer, the owner and the reviewer.

a. The reviewer needs to trust that the eDocument belongs to the claimed person, is issued from a trusted body, and hasn't been modified since it was issued; needs to trust the issuer and the verification system being used
b. The eDocument owner needs to trust the received eDocument as being truly from the expected issuer; trust the reviewer not further distribute or misuse the information
c. The issuer needs to trust the identity information provided by the applicant (the owner) before the eDocument can be issued; trust the reviewer not to perform any unauthorized action while opening the channel to the backend database during verification process.

To satisfy the trust, all need to address the security requirements: Confidentiality: only the specified person should be able to access it; Privacy: owner should retain control over the distributed eDocument; Integrity: no unauthorized modification should be allowed; Authentication: self-validating, can be verified; Identity: proof of ownership, and you are who you claim to be; Validation: withdrawn situation can be handled; Lifetime validation: would remain valid even if the issuing authority no longer exists; Trustworthiness: issuer can be tracked down to a trusted authority.

2. Limitation of digital signing

Digital signing is an efficient way to prove the issue of and prevent modification of an eDocument, and therefore it is currently used as the eDocument security method. However, it is most suited static documents, but not for documents with changing states:

Content validation: a digitally signed document can have its modification, signer, and the signer's CA validated, but not the content of the document. This is crucial to eCertificate as this signed document itself is also a certificate, which may have a valid period (e.g. first aid certificate), and may be revoked in a later stage (e.g. if it is discovered, after the certificate has been issued, to have cheated in exam or to have plagiarized). The problem we are dealing with is a (certificate)^2 issue, which involves the issuer's public key certificate and the qualification certificate as a whole.

Auto request of validation: Current PKI doesn't start the validation of the public key certificates' status automatically. It will only process if required. In the case of eCertificate, this is a critical security hole as it may result in a forgery being accepted if the key has been compromised.

This is explained in Figure1.

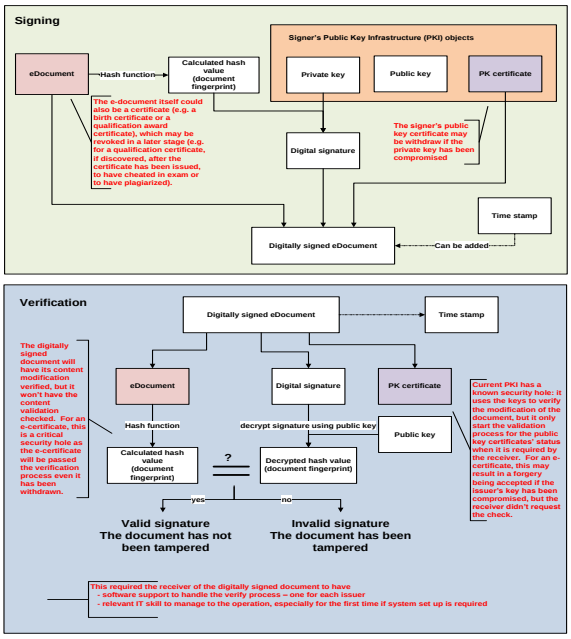

Figure 1. Issues when applying digital signing

3. Issues when applying digital signing

When forward transfer of a digitally signed eDocument after the first stop is required, it comes complicated trust and key management issues.

3.1. Digital signing with independently distribute approach

If we use a digitally signed document to replace the paper-based document within the existing issue, distribution, and verification process path, e.g. from institution to learner, then learner to reviewer, this raises service support and privacy issues. It will require all the receivers (the eDocument owner and all reviewers) to have service support to handle the verification process on reception; once the reviewer has access to one document, he can access any documents that are signed in the same way. This is against the confidentiality and privacy requirement in some situations.

3.2. Digital signing with individual institutional approach

As digitally signed documents require service support and key management for forward distribution, an institutional approach is commonly used to avoid these: a) eDocuments will be issued and stored in the institution's system; b) the system will also provide management and verification service; c) eDocument owners can access the system to set access control of their own eDocument before sending out the links and access keys to the specified reviewers; d) the reviewers can access the system to view and verify the eDocuments through the provided links and access keys

An institutional approach can overcome the service support issue as it provides the management and verification services within the institution. It can also address the privacy and confidentiality issues by setting system access values. However, other new issues then arise: the approach requires huge storage as it needs to store all the issued eDocuments for a lifetime; the support service provides an active channel to the backend database, which could increase the risk of attack rapidly; it is heavily reliant on the issuing institutions, lifetime validation is a problem if the institution no longer exists; it is inconvenient for the receivers to access their eDocuments when the eDocuments are issued from many different institutions. E.g. a student may need to log into many different institutions to access and manage his/her eDocuments received throughout the study journey.

3.3. Digital signing with linked institutions plus central service approach

Alternatively, linked institutions with a central service approach may be used: a) a central online system provides the management and verification service for all member institutions; b) all institutions issue eDocuments under the same standard, and then upload to the central system; c) the owners can access the online management system to set access control of their own eDocument before sending out the link and access token to the specified reviewer; d)the reviewer can access the online verification system through the link and use the access token to view, verify, and download the eDocument.

Compared with the individual institutional approach, this approach addresses the lifetime

validation issue, and also solves the inconvenience problem as the users only need to access one reference point for all the eDocuments. However, this approach requires even bigger storage as it needs to store all the issued eDocuments from the joined institutions for a lifetime; this also increases the risk of database attacks as a bigger database contains more information; what is more, who will host such a system? It must be trusted by all institutions as it holds the information for all of them. But, the English government has a track record of losing our sensitive information, and in some cases, the whole database.

4. Case study – the eCert project

The problems that we are facing need answers. The eCertificate example requires digital signing for non static documents and forward transfer of the document; it represents the typical problem situation, therefore, it is used as case study to research for a solution.

4.1. Motivation

The field of eLearning provides technological developments, such as ePortfolios, which are being explored as an improvement over paper-based portfolios in the job and course application process. However, forged certificates exist due to poor security in ePortfolio systems. Therefore, the students' claimed achievements within ePortfolios need to be verified. Abrami[1] notes that it is difficult to authenticate the evidence in ePortfolio. The JISC (Joint Information Systems Committee) is funding the project, eCert, to research for a potential solution, which is just what our case study about.

4.2. Domain research

The eFramework has been the backbone to help build interoperable tools for eLearning, such as the ones for ePortfolios[2, 3]. It has been facilitated by choosing a Service Orientated Architecture (SOA)[4]. The Service Orientated Reference Model (SORM)[5] was conceptualized to encapsulate the eFramework research process. The eP4LL (EPortfolios for Lifelong Learning) project developed a reference model for ePortfolios for the eFramework[6]. The RIPPLL (Regional Interoperability Project on Progression for Lifelong Learning) has tackled the authentication issue between institutions it links by using a SSO (Single-Sign-On) system, where the identity of a user is supported by their home institution when accessing other institutions' systems[7].

The main body of research into ePortfolios has been into defining reference models for the domain, such that these can be developed into a body of interoperable reference implementation services and tools. It is apparent that although the eP4LL models define the use cases for the exchange of portfolio data, from an eCertificate perspective they are limited, as neither has described explicitly the security issues raised by transmitting data between multiple, and not always known, parties; and there still is no mechanism to authenticate the veracity of the portfolio data transmitted between institutions in RIPPLL. As Peter Rees Jones[6], an eP4LL project member, comments on his blog: "Security and Trust: the [ePortfolio] Reference Model sidestepped this key issue". However, the SORM methodology has been identified to investigate eCertificates.

4.3. Existing systems

There are existing systems dealing with the authentication of qualification. However, they were built for specific purposes, and couldn't address the security requirements involved in data transmission that we noted above. For example:

Europass: the European Community provides a Europass Certificate Supplement and a Diploma Supplement[8]. These provide facsimiles of award certificates and information about the qualification. However, the system clearly states that, "The Europass Certificate Supplement is not: a substitute for the original certificate;" or "An automatic system that guarantees recognition". But, this is not good enough for the security in real world.

The Chinese Certificate Information Verification service [9]: The service will take unique student numbers and unique certificate numbers as input, and output the specified qualification detail along with the student's personal detail, including a photo. It provides more reliability to the viewers as it also verifies the identity of the person. But this method doesn't suit every country, e.g. it against the data protection law in UK. Also, this service only verifies qualification records, but not eCertificates.

Digitary (Digital Notary) [10]: the system issues, distributes and authenticates eCertificates over the Internet with the system installed to institutions individually. Students need to login to their institution's system to access and manage their eCertificates, such as set access tokens for individual reviewers. Reviewers can then access the eCertificates through the received URLs using the access tokens; this may involve registration process depending on the access level that was set. This is the closest system to our idea of the eCertificate, however, it uses an institutional approach when applying digital signing, therefore, there exist the storage, security, lifetime validation, and usage issues mentioned above.

4.4. Use cases analysis

The eCertificate scenarios have been set up to help with the understanding of the situation. It is depicted in Table 1

Table 1. Use Case Scenarios

	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 e-certificates 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 of a wild range.
withdraw	An exam board found out that an e-certificate was miss-issued, and needs to be withdrawn. -- This needs security methods to support the withdrawal mechanism
issue	The exam board issues the e-certificates for students. -- This needs security methods to a) indicate that the e-certificates are issued by the exam board, in order to prove its genuineness, and prevent unauthorized editing and copying after issue; b) issue the e-certificates;
receive	The students receive their e-certificates, and view the contents. -- This needs security methods to ensure that no one other than the students themselves can view their own e-certificates.
manage	A student specifies certain e-certificates to be visible to particular employers. -- The student needs to be able to control which e-certificate(s) for which employer(s) and are for how long they would be valid. The system design needs to be user friendly, suitable for users without IT skills
distribute	A student sends the selected e-certificate(s)to potential employers -- The student should be able to send the e-certificate(s) alone or within an e-portfolio. -- For students sending the e-certificates through e-portfolio accounts, only the selected e-certificate(s) in the account should be visible to the employer(s).
review	An employer views the received e-certificate(s) -- This needs security methods to a) ensure only the specified employer can view the e-certificate(s), but not anyone else; b) protect from modifying and unauthorized copying.
verify	The employer verifies the received e-certificate(s) -- The system need to be able to verify all level qualifications that are issued using the same standard from any education institutions nationwide, and check that the e-certificate and the key are still valid

The scenarios are shown diagrammatically as use cases in Figure2. The use cases indicate that the eCertificate system involves many issues during the processes:

Assertion: the system need to be self certificating to prove it's genuine, and also to allow reviewers to further confirm it. As well as generating these assertions, it should be possible to withdraw them. Parallels can be drawn with Public Key Infrastructure certificate systems, which provide the required method while also maintaining a revocation list of keys which are invalid as they have been compromised[11].

Privacy: ePortfolio reference models include the functionality for owners to be able to create different "views" where "information relevant to a particular purpose" is selected by the owner for a selected audience[12]. This means the owner can tailor their portfolio to best support their application. This also applies to eCertificates, as no matter whether it is used standalone or within an ePortfolio, one aim is to give students control over its usage This is a similar paradigm to Web 2.0 social networking sites were a user can "categorize their network [of friends] into different access groups with different access privileges"[13].

Rights: the learners have not only needs, but also rights. They have the ownership of their qualification attainments, same as paper-based certificates. These are personal data, and the owners have the right to store, manage, share and track, "under their control, with their consent, and for their benefit"[14].

Stakeholder Trust: A fundamental requirement from the use cases is the need to establish trust amongst stakeholders. Once more parallels can be drawn with PKI systems where trust networks have to be engineered in order for any other user to see value in the key certificates generated. This is typically achieved either with a hierarchy of globally "trusted nodes called Certificate Authorities" (CA) or by anarchy based methods such as Pretty Good Privacy (PGP) where chains of trust are formed between users who already know each other[15].

Distributed Stakeholders: To "stimulate large-scale uptake" of users[6], eCertificate tools need to define "architecture of participation". The eCertificate system won't work unless there is a significant body of universities and employers who will accept them. This concept is defined within the Web 2.0 community as the network effects that are achieved when "Users Add Value" and encourage further users to participate[16].

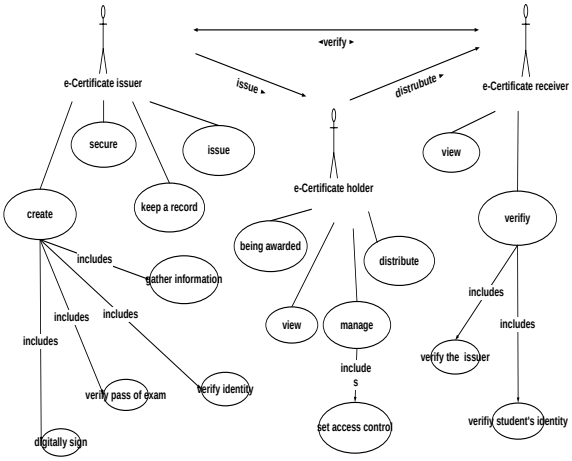

Figure 2. eCertificate use case diagram

4.5. Gap analysis:

Existing services: a) Digital signing: digital signatures are used in e-documents to provide authentication, integrity, and non-repudiation. By adopting digital signing method, adding an issuer's signature to an eCertificate can meet part of the eCertificate assertion use case as it can provide proof of the certificate's source and evidence of modification, and it also meet part of the stakeholder trust use case as the CAs provide chain of trusted nodes. b) Service Orientated Architecture: By

adopting the SOA of the eFramework one meets the distributed stakeholder use case as SOA provides architecture of participation. c) Federated Identity: The formation of stakeholder trust has been addressed in previous eFramework projects, including ePortfolio projects, by utilizing the open-source federated identity system Shibboleth[7]. It would provide a framework for eCertificate stakeholders to be able to lookup and verify the identities of other stakeholders; and therefore be able to place trust in their identity. However, such systems may need to be extended in order to associate the requirements of eCertificate system.

Required Services: Current research is missing services to certify the veracity of any XML structure; it isn't possible to create eCertificates to assert that an XML fragment representing the qualification is genuine. Therefore, services are required to address the lifetime validation, trust and key management, and privacy issues while solving the $(\text{eCertificate})^2$ problem.

4.6. Bridging the profile gap

Auto verification of CRLs: to solve the $(\text{certificate})^2$ problem, we need to validate the certificates' state against two types of certificate revocation list (CRL): whether the signer's key has been compromised or the actual content certificate has been redrawn. Therefore we need to maintain the document's revocation list as well as the signer's certificate revocation list (CRL). We can provide a service to automatically verify the status against both of these lists, without the need of raise a request by the reviewers.

XML metadata: the ownership, usage, and privacy issues can be solved by generate the related information in XML metadata while employing the enveloped and enveloping signature method to create an eCertificate; allow the owner to set access control to the document while retaining the integrity of the digital signature.

An independent system that provides verification service would be an ideal to solve the lifetime validation issue. However, it needs to overcome the storage and security issues.

4.7. Goals

According to the research information and analysis result, the eCert system designed is aim to: Maintain information privacy, and ensure that the owner can have control over the usage of their eCertificates; Prevent unauthorized modifying, and could be verified in a legal context; Lifetime validation, independent from issuing body. Allow for verification nationwide; Easy to use while maintain security controls, suit low IT skill users, both students and reviewers; Can be accessed through the issuing organizations, or any owner preferred ePortfolio, or be used as a standalone application.

4.8. System design

As a result, the eCert system was designed to contain three subsystems for issuing, management, and verification services, showed in Figure3:

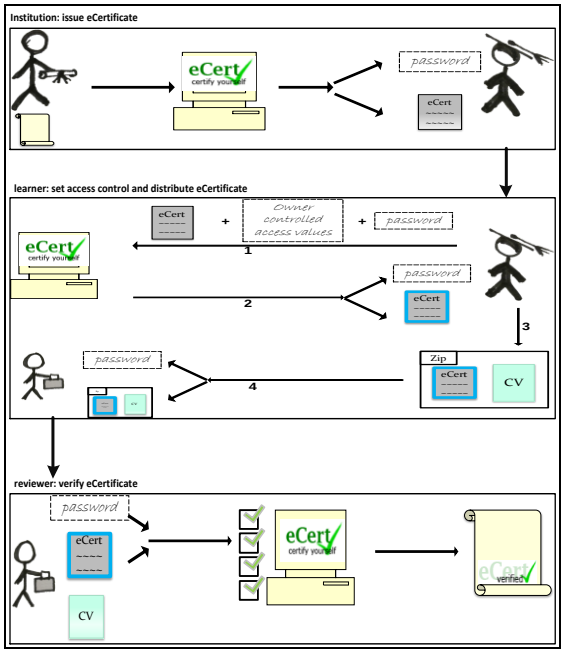

Figure 3. eCert system design flow diagram

1. The eCert issuing subsystem will create and issue eCertificates. An eCertificate may contain three sections where applicable: an electronic version of the award qualification certificate; the transit file of the supported information about the qualification and the organization; and the skill assessment file that the certification was based on. The eCertificate will be digitally signed and encrypted to ensure assertion and prevent unauthorized access; it will also contain build-in functions to allow usage control settings while maintain the integrity of the digital signing.
2. The eCert management subsystem will be access controlled. It will enable the eCertificate owners to view and set control to their own eCertificates, e.g. who can see what (which sections) and for how long, and hence produce specific views for specified reviewers within specified time.
3. The eCert verification subsystem will take eCertificates and their co-responding access keys as input, using their decrypted data and build in functions to verify the state of the signers' public key certificates and the award qualification certificates (whether they have been revolved); validate the award expire time and access expire time; verify the digital signature against content modification; and display the file when successfully pass all the above processes.

The eCert issuing subsystem is for registered educational organizations only. The management subsystem and verification subsystem will be

provided through the eCert online central system. In addition, there will be an eCert application for all stakeholders to download. The application will provide the management and verification services as the online central system. Therefore, the eCertificates can be accessed locally, and then automatically verified through the network. This has benefit of avoiding uploading files, it would be particular useful when verify a large number of eCertificates is required.

4.9. Advantages

Compared with the other methods and approach which mentioned above, the eCert system offers huge advantages:

Ownership: the eCert system is designed with user centric approach, the eCertificate is in the owner's hand, and the owner has full control of it. E.g. owner can set access control to an eCertificate, and it can be stored to the owner's preferred repositories while still maintaining verification functions;

Technical: the system contain functions to handle the (eCertificate)2 and the auto validation problems; also allowing setting for usage control while could still be verified against the initial issuer's digital signature.

Usage: provides a single access point, convenient access for learners and reviewers with eCertificates that have been issued from a wide range of register educational organizations;

Lifetime validation: an eCertificate can be verified independently without referring to the issuing institution, the central system provides the required services for any issued eCertificates even when the issuing institution no longer exists.

System storage: the system doesn't store any eCertificates copies or sensitive data in the system, while providing all the required services through a secured environment. It minimizing the required storage. This becomes increasingly significant as the system grows in size, especially when its usage is nationwide, and the eCertificates need to last for life

Security: as our sensitive data are not stored in the system, and there is no traffic raised against any organisations' database due to the verification process, we can avoid many of the potential attacks;

Trust: the central system is only there to provide a service, as our sensitive data are not stored in the system, there will be no risk of our data being lost. Regarding people in general, who don't trust government bodies to hold their personal data, this approach makes having such a central system possible.

4.10. Demo and workshop feedbacks

The eCert project has been through the research, analysis, design, and design review phases, and is now at the end of the demonstrator development stage. Positive feedbacks have been received from conferences and workshops internationally. Joe Wilson[17], one of the workshop participants, wrote on his blog: "… Some really useful example uses from across UK… can be used to verify exam results, project work, ePortfolios. … can see lots of applications for this. Potentially useful links to Bologna process and E-Certification E-pass work".

5. Conclusion

From the eCert challenge, a potential solution has been successfully proposed. As the eCertificate problems represent the situation that the digital signing issues faced, the principle of the eCert solution can be employed to solve the digital signing issues that applied in many other situations.

6. References

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

[2] Wilson, S., K. Blinco, and D. Rehak, Service-Oriented Frameworks - Modelling the infrastructure for the next generation of e-Learning Systems. 2004, JISC-CETIS: London.

[3] Smith, R., Briefing Paper - e-Framework. 2006, JISC: London.

[4] Lethbridge, T.C.e.a., Object-oriented software engineering : practical software development using UML and Java. 2nd ed. 2005, Maidenhead: McGraw-Hill Education. xxv, 533.

[5] Wills, G., et al., An E-Learning Framework For Assessment (FREMA), in 11th International Conference for Computer Assisted Assessment. 2007: Loughbourgh.

[6] Rees Jones, P., Specifying an ePortfolio: a Personal View. 2006, CETIS / JISC: Nottingham.

[7] Hartnell-Young. E, A.S., S. Kingston, P. Harley, , *Joining up the episodes of lifelong learning: A regional transition project.* British Journal of Educational Technology, , 2006. **37(6) 853-866**.

[8] European Communities. *InformationOn/EuropassCertificateSupplement/navigate.action*. 2008 28 January 2008 .

[9] China Higher-education Student Information and Career Center (CHESICC), T.C.I.V.s.i.C.,

[10] Digitary. 2008 August, 2008.

[11] Tanenbaum, A., Computer Networks. 2003, London: Pearson Education.

[12] Grant, S., Clear ePortfolio definitions: a prerequisite for effective interoperability., in ePortfolio Conference. 2005: Cambridge.

[13] Razavi, M.a.L.I., *A Grounded Theory of Information Sharing Behaviour in a Personal Learning Spaces*, in *20th anniversary conference on Computer Supported Cooperative Work*. 2006, ACM: Alberta.

[14] *Sadd, G. What do you think I am*. in *London Learning Forum*. 2010. London, UK.

[15] Perlman, R., An overview of PKI trust models. IEEE Network, 1999. 13(6).

[16] O'Reilly, T. *What is Web 2.0?* 2005 Mar2008.

[17] Wilson, J. *eCert program*. 2010 10 September 2010.