A User-Centric Approach for Secured eDocument Transmission: Digital Signing Practical Issues and the eCert Solution

Lisha Chen-Wilson, Lester Gilbert, Gary B Wills, Andrew M Gravell, David Argles
Learning Societies Lab, School of Electronic and Computer Science, University of Southampton, United kingdom
{lcw07r, lg3, gbw, amg, da}@ecs.soton.ac.uk

Abstract

Digital signing is commonly used in eDocument security, but does not address all requirements such as fine-grained access control and content status validation. A system for distributing electronic educational certificates (eCertificates) is used as a case study in the eCert project. This paper describes the issues, identifies the required use cases, explores the gap between current techniques and the desired system, and presents a design which meets the requirements. A preliminary implementation confirms that the design is a sound one, and can be used to solve digital signing issues in related scenarios such as mobile IDs and healthcare records.

1. Introduction

As digital technologies continue to develop rapidly, they 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 we come to transfer digital data between three or more unknown parties, there exists a major security issue:

- how can the receiver believe that the data is from the expected person,
- that it has not been modified in any way;
- how can the sender ensure that their data will not be misused?

Example 1, An electronic version of a 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 easily be 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 doorman at a night club 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?

Example 3, Sharing Healthcare Records: Increasingly medical records are being stored electronically. This creates potential problems for patients, doctors and clinicians who may need to provide partial or time-limited access to third parties such as third party health providers and medical insurance companies. As with any eDocument, validation is essential, but it is also paramount that patient confidentiality is not violated, and that embarrassing private information cannot be forwarded to potentially malicious agents such as newspapers.

The common problems: There are many similarities scenarios between these three cases. They represent a common situation where 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.

- 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
- The eDocument owner needs to trust the received eDocument as being truly from the expected issuer; trust the reviewer not to further distribute or misuse the information
- 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, we 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;
- Status validation: it should be possible to withdraw certification after issue of the eCertificate;
- 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, and prevent modification, of an eDocument, and therefore it is currently used as the eDocument security method. However, it is suited to static documents, but not to documents with changing status:

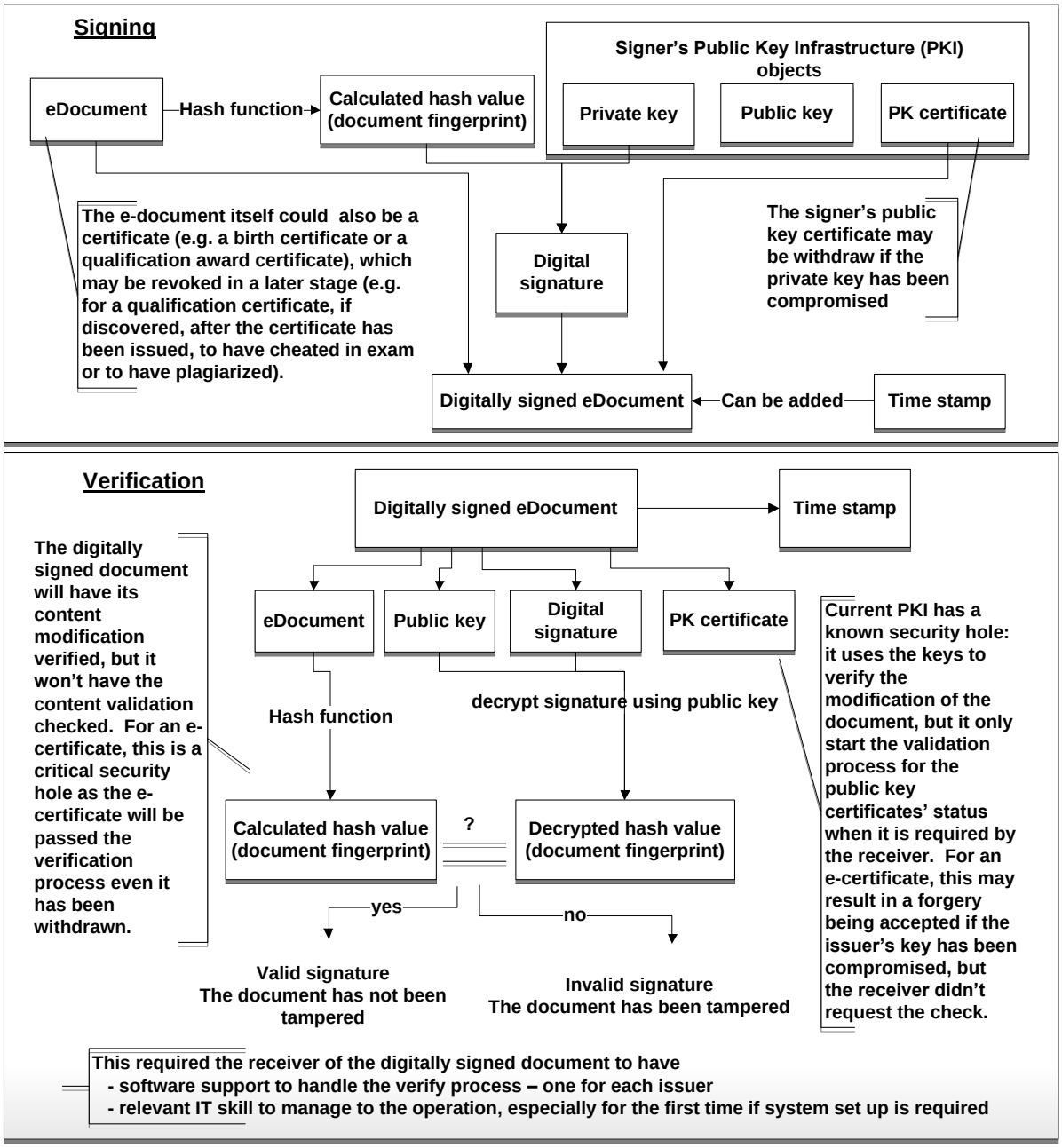

Figure 1. Issues when applying digital signing

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 an eCertificate as this signed document itself is also a certificate, which may have a period of validity (e.g. first aid certificate), and may be revoked at a later stage (e.g. if it is discovered, after the certificate has been issued, that the person has cheated in an exam or have plagiarized). The problem we are dealing with is a certificate-squared, or $(certificate)^2$, issue, which involves the issuer's public key certificate and the qualification certificate as a whole.

Auto request of validation: Current Public Key Infrastructure (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.

These issues are shown diagrammatically in Figure1.

3. Issues when applying digital signing

When we need to forward a digitally signed eDocument, the trust and key management issues become complicated.

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, they can access any documents that are signed in the same way. This is against 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 this:

- eDocuments will be issued and stored in the institution's system;
- the system will also provide management and verification service;
- 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;
- 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 is necessary 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 UK government has a track record of losing our sensitive information, and in some cases, the whole database[1].

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[2] notes that it is difficult to authenticate the evidence in ePortfolio. Related work has been ongoing at the University of Southampton exploring possible mechanisms for transferable eCertificates in a user-centric context[3, 4]. 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 JISC eFramework has been the backbone to help build interoperable tools for eLearning, such as the ones for ePortfolios[5, 6]. It has been facilitated by choosing a Service Orientated Architecture (SOA)[7]. The Service Orientated Reference Model (SORM)[8] was conceptualized to encapsulate the eFramework research process. The eP4LL (EPortfolios for Lifelong Learning) project developed a reference model for ePortfolios for the eFramework[9]. 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[10].

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[11], an eP4LL project member, comments on his blog: "Security and Trust: the[12] 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[13]. 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[14]: 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 the UK. Also, this service only verifies qualification records, but not eCertificates.

Digitary (Digital Notary) [15]: 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 case analysis

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

The scenarios are shown diagrammatically as use cases in Figure2. The use cases indicate that the eCertificate system involves many issues during the processes. These involve assertion, privacy, rights, stakeholder trust, and distributed stakeholders.

Table 1. Use Case Scenarios

	Scenarios and conditions
create	An examination 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 examination 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 examination 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

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[16].

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"[17].

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"[18].

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[19].

Distributed Stakeholders: To "stimulate large-scale uptake" of users[11], eCertificate tools need to define "architecture of participation". The eCertificate system will not 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[20].

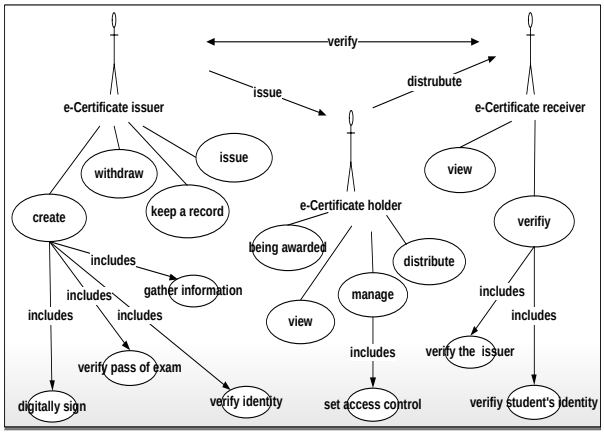

Figure 2. eCertificate use case diagram

4.5. Gap analysis:

Existing services: a) Digital signing: digital signatures are used in eDocuments 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 (SOA): 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[10]. 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. Structure design

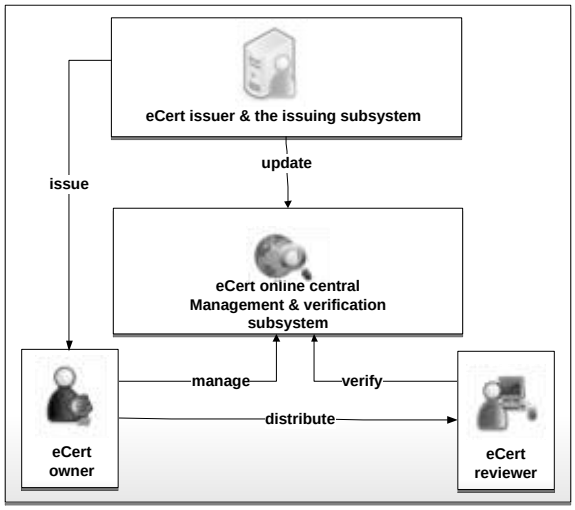

Figure3: transmitting eDocuments with a central service with no storing approach

The three typical system structures for handling digitally signed documents, which mentioned in section 3, are employed in many existing systems, such as mobile eBoarding cards, secured mailing systems and commercial eCertificate systems. However, they were designed for specific purposes, their limitations affect them to be applied in the eCertificate situation efficiently.

For the aim of meeting the eCertificate requirements, a new system structure design is proposed as the base of the eCertificate system framework: a centralized service approach for distributed eCertificates, this is show in Figure 3.

- a central online system provide the management and verification service for all joined institutions;
- all institutions issue eCertificate under the same standard independently, and then issue them to the owners;
- the owners can access the online management system to set access control of their own eCertificate before sending out to the reviewers;
- the reviewers access the online verification system to verify the eCertificate with the received access information;

Compare to the other structures that mentioned earlier, this new system structure combines their advantages, provides convenience access point, while employ eDocument distribution approach, which will not only satisfy the ownership right, but could also save huge system storage and avoid database attacks dramatically.

However, with this approach, we back to our three way transmitting situation, and need to address the keys management, privacy and confidentiality issues that we described earlier.

4.9. System design

As a result, the eCert system was designed to contain three subsystems for issuing, management, and verification services[21], showed in Figure4:

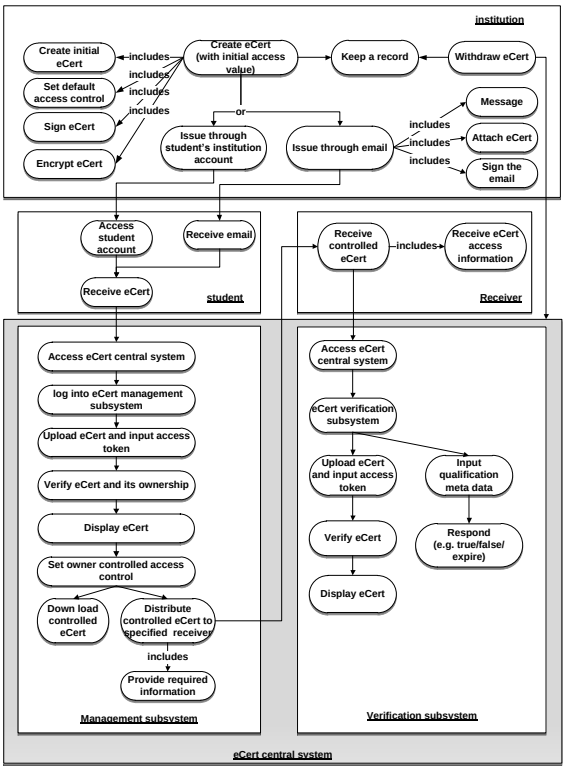

Figure4. eCert system design overview

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. This is shown Figure5.

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.

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.

Figure5. The interface design of a verified eCertificate

4.10. System policy

In order to secure such a system, a number of decisions and assumptions have been taken:

- every student will register a unique student ID when they start study at sixth form or college (the level that they will start to receive all sources of qualification certificates);
- This registration process will verify who the student is (same process as register to a course at college), and assign each student with an unique student ID nationwide
- This student ID will last lifelong
- Every eCertificate that the student achieved will contain this student ID along with the eCertificate ID as prove of ownership
- Student : student id → 1 : 1
- Student id : eCert id → 1 : many
- All eCertificates will be digitally signed with eCert signing method and then encrypted before issue
- All institutions 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, so that no fake institutions can be involved. All members that represent their institution, e.g. a registrar, will also need to be certified, and can be traced back to the institution.

- To ensure that only the eCertificate owner can change the access value to their own eCertificates but not anyone else, a login access control to the management subsystem is required.
- only authorized issuer from the registered education institution can access the issuing system.
- As every institution will have difference attribute names in database tables, and may using different methods to collect the required information when forming a paper-based certificate; with the purpose of easy fit the eCert system into any institution, the eCert system will let the institution to form the base of the award qualification file using the existing method, and take over from a print-ready for paper-based certificate stage, and from that, set links to collect any required information. This should simplify the configuration on system setup when install.

4.11. Advantages

Compared with the other methods, approaches, and existing systems, the eCert system offers huge advantages [22]:

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 $(\text{eCertificate})^2$ 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 minimizes 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 organizations' 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.

4.12. System implementation

The design has been implemented in order to demonstrate its technical correctness.

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

Code library: The core of eCert system implementation is a open source code library, providing basic supports for the eCert issuing, management, and verification system development. The code library is built in Java, with the programming environment of J2SE 1.6. The eCert code library includes a number of features that meets the requirements of the eCert demonstrator development:

- Support for digitally signing XML documents with the eCert signing method, compatible with ESTI European Digital Signature standard.
- Support for digitally-signing and verifying files with given key stores.
- Support for Key Pair generating (variant lengths), converting (from/to String) and file encryption/decryption with RSA/DSA algorithm.
- Support for domain file processing, including producing qualification files, adding file metadata, setting access control, multiple digitally signing prepared files, file compression and decompression, and fully verifying signed qualification files.

Demonstrator: 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 supports. All web pages share a common interface design for system

consistent, with different colour scheme to distinguish the three systems in between. Different pages are rendered by loading different sub-pages in the menu and content areas using the Ajax technologies.

5. eCert evaluation

The eCert solution has been evaluated in three steps:

- Whether the design meets the requirement
- The usage of the eCert system in its related applications
- The applicability of the eCert concept in other eDocument transmitting domains

5.1. eCert system design evaluation

The eCert used a mixed-model research methodology: the Delphi methodology[23] was employed for the evaluation of eCert system design alongside the SORM development methodology, to determine whether the design meets the requirements, step by step throughout the development stages. Following this method, a group of domain experts in the UK were selected for the purpose of security system design, ePortfolio study, and represent of the stakeholders. These included employment managers, IT security experts, exam board managers, and ePortfolio researchers. Two workshops have been run during two stages of the development to collect the professional opinions from these experts: one at the end of the system design stage, aiming to evaluate and adjust the system from the strategic level; and the other one on demo completion stage, where the system was brought back to the domain experts after the design adjustments and demonstrator production, aiming to evaluate the system from the technical level.

In addition to following the Delphi method, workshops and presentations have also taken place in national and international computing security related conferences to collect the opinions from a wider range of domain experts, such as a "round table" run at the EdMedia 2010 conference at Toronto, Canada [24].

After each round, feedback was reflected, and as a result, the system (including the design, demo, documentation, and reports) were adjusted accordingly. For example

- the eCert file structure now includes the transcript file to enhance its usage nationwide;
- a photo of the student can now be added as one of the evidence files and bound with the eCertificate to enhance the security, but optional when preferred for the sake of privacy;
- more work has been spent on system comparing between the new design and the existing systems, and the explanation of the chosen approach are given in more detail.

Towards the end of the project, much positive feedback has been received from conferences and workshops internationally while negative feedback was mainly related to the future work that can't be completed in the current project. Joe Wilson[25], 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*".

5.2. eCert system usage evaluation

With the eCert system design successfully passed the evaluation process through the Delphi method, the usage of the eCert system is then evaluated through a subproject named "Integrating eCertificates within ePortfolio Systems", to test whether it could not only be used as a standalone application, but could also be serviced within other related applications, such as ePortfolios.

The evaluation subproject was carried out by a group of four Masters degree computer science students.

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 access and visibility parameters.

In addition to this, the group has developed mechanisms for eCertificate integration within the University of Southampton's home-brewed ePortfolio system, "eFolio", and an Australian open-source ePortfolio system, "Mahara". Both systems can now be fully utilised by those with eCertificate qualifications.

The group has completed all of its primary and secondary goals. As a result, it proves the usage of the system successfully as the eCert system can not only be used standalone but can also be plugged into other applications. In return, the eCert system's accessibility and scalability have also been improved after taking a considerable number of observations and recommendations from this subproject.

5.3. eCert concept evaluation

The aim of the research is to explore the eDocument transmitting issues, propose a solution for a secured eDocument transmitting framework, so that the securely transmitted eDocument could be verified in a legal context, and valid lifetime, while the owner can remain control over its usage. As the case of eCertificate study represents the typical

eDocument transmitting issues, it is believed that the concept of its solution could in turn solve the eDocument transmitting issues in other cases. Therefore, with the aim of proving this hypothesis, and to evaluate the applicability of the eCert protocol in a wider context, the concept of the eCert solution is being tested under a further subproject, Mobile eID. Mobile eID explores the issues that arise in implementing the eCert protocol within a mobile platform, which provide protected and certifiable electronic identity (eID) information through mobile devices.

Consider the following situation: young looking Bob goes out clubbing and often has to certify his age to enter. By presenting his paper ID, his is forced to disclose all the sensitive information on that document, not only the age. Unfortunately he left the required ID document at home, and even though his wallet contains a lot of other ID cards, nothing else is acceptable. Disconsolate, Bob comes back home. The idea of this subproject was to apply the eCert technique, present an ID documents as digitally signed, owner controlled ID certificates through mobile devices. The eCert for eID managed in mobile devices proved itself as the tool able to be always available and to provide a huge variety of ID in order to avoid the previous scenario.

The Mobile eID project has exploited the underlying technologies, studied the current ID system, compared the eCert with the analysis of the eID problem domain, and thereby derived a new working solution for a mobile Android environment managed by the eCert protocol. More importantly, the user-centric approach of eCert also allows the eID owner to personally manage the ID information and to display only what is required. However, since the eCert system is implemented particularly for e-qualification certificates, a reverse engineering process to adapt the eCert system is required during the mobile eID system development.

As a result, the successful outcome of this subproject proved that the concept of the eCert protocol could be the answer for the eDocument transmitting issues in other related domains.

6. Conclusion

The eCert project, as a case study, has successfully proposed a solution for a user-centric, secured eCertificate management system. It has addressed the $(\text{eCertificate})^2$ problem that exists within the traditional digital signing method when it is applied to non static content eDocuments; it defined the eCertificate file structure, so that it contains not only the qualification award information, but also the transcript information and any supported evidence files, which can be in any format; it has proposed a new digital signing method to cooperate with the designed file structure and to meet the eDocuments' ownership right. The new signing method not only bound the related files together, but also allow the eCertificate owners to set access control value of who can see what and for how long to the signed eDocument, while remaining the integrity of the signature, without the need of re-signing by the initial issuing body; an additional encrypt key will be added after the signing to ensure that only the receiver with the corresponding decryption key can access the file; it has also proposed a newly designed centralized verification service for such digitally signed and access controlled distributed eCertificates. The system provides security control for verification against eCertificate expire time, access period, ownership, signing key status, qualification award status, owner controlled section display. The whole design worked together to ensure the issued eCertificates can be securely distributed and verified independently from the issuing body and satisfy the ownership right, without requiring storage in the verification system. This also provides huge advantages of lifetime validation and the avoidance of many database attacks.

The protocol has been tested and evaluated through its demonstrator following the selected research methodology; the design principle has been tested through a subproject, integrating eCert in ePortfolios, to evaluate the usage of eCertificate in other applications; the concept of the eCert solution has been tested through a subproject, the Mobile eID, to evaluate the applicability of such concept in wider situations. All the test and evaluation results are successful, indicated that the proposed eCert protocol will not only meet the eCertificate challenge, but also solve the eDocument transmitting security issues, and can be applied in a wider domain.

As the eCert demo is just there to demonstrate the eCert concept and design, it only uses self signed certificates and a dummy database throughout the system development and testing. Future work can be to investigate and evaluate the eCert system by employing real CAs and linking to real institution databases for further testing, and adding more functions to improve the system's user interface when the system is going to be used in the real world.

7. References

[1] J. Sturcke, "Government offers reward in hunt for lost data," in *Guardian*, ed, 2007.

[2] P. C. Abrami, and H. Barrett, "Directions for research and development on electronic portfolios," *Canadian Journal of Learning and Technology / La revue canadienne de l' apprentissage et de la technologie*, vol. V31(3) Fall / automne, 2005.

[3] L. Chen-Wilson, P. Royce, P. Newcombe, S. Ong, T. Wonnacott, G. Wills, D. Argles, , "Secure Certification for e-Portfolios," in *World Conference on Educational Multimedia, Hypermedia and*

Telecommunications (ED-MEDIA), Vienna, Austria, 2008, pp. 1716-1722.

[4] L. Chen-Wilson, R. Blowers, A. Gravell, and D. Argles, "Towards an secured e-Certificate System for use in e-Portfolios," in *V International conference on Multimedia and Information and Communucation Technologies in Education (m-ICTE)*, Lisbon, Portugal, 2009, pp. 1466-1470.

[5] S. Wilson, K. Blinco, and D. Rehak, "Service-Oriented Frameworks - Modelling the infrastructure for the next generation of e-Learning Systems " DEST (Australia), JISC-CETIS (UK), and Industry Canada, 2004.

[6] R. Smith, "e-Framework Briefing Paper," the Joint Information Systems Committee (JISC), UK, and the Department of Education, Science and Training (DEST), Australia, 2006.

[7] T. C. Lethbridge, Ed., *Object-oriented software engineering : practical software development using UML and Java*. McGraw-Hill Science/Engineering/Math, 2005, p.^pp. Pages.

[8] G. Wills, Bailey, C., Davis, H., Gilbert, L., Howard, Y., Jeyes, S., Millard, D., Price, J., Sclater, N., Sherratt, R., Tulloch, I. and Young, R., "An E-Learning Framework For Assessment (FREMA)," in *11th International Computer Assisted Assessment Conference (CAA)*, , Loughborough University, UK 2007.

[9] P. Rees Jones, A. Smallwood, and S. Kingston, "e-Portfolio for Lifelong Learning Reference Model Project (eP4LL)," University of Nottingham,2006.

[10] A. S. Hartnell-Young. E, S. Kingston, P. Harley, , "Joining up the episodes of lifelong learning: A regional transition project," *British Journal of Educational Technology* 2006.

[11] P. Rees Jones, A. Smallwood, and S. Kingston, "Specifying an e-Portfolio: a Personal View," University of Nottingham.2006.

[12] S. Grant, "Clear e-portfolio definitions: a prerequisite for effective interoperability," in *ePortfolio conference*, Cambridge, UK, 2005.

[13] European Union. (2004). *Opening doors to learning and working in Europe: Information On Europass Certificate Supplement*. Available: http://europass.cedefop.europa.eu/europass/home/hornav/Introduction.csp (Access Date: 28 January 2010)

[14] CHESICC. (2005). *The Certificate Information Verification services in China, China Higher-education Student Information and Career Center*, . Available: http://www.chsi.com.cn/about_en/ (Access Date: 02 September 2008)

[15] Digitary. (2008). *Secure Electronic Documents*. Available: http://www.digitary.net/aboutus.htm (Access Date: 12 August, 2008)

[16] A. Tanenbaum, *Computer Networks*, 4th ed.: Pearson Education, 2002.

[17] M. Razavi, and L. Iverson,, "A Grounded Theory of Information Sharing Behaviour in a Personal Learning Spaces," presented at the 20th anniversary conference on Computer Supported Cooperative Work, Alberta, 2006.

[18] G. Sadd, "What do you think I am: Trusted Relationship Management," presented at the London Learning Forum, London, UK, 2010.

[19] R. Perlman, "An overview of PKI trust models," *IEEE Network*, vol. 13, pp. 38-43, 1999.

[20] T. O'Reilly. (2005). *What is Web 2.0?* Available: http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html (Access Date: 05 March 2008)

[21] L. Chen-Wilson, and D. Argles, "Towards a framework of a secure e-Qualification certificate system," in *IEEE 2nd International Conference on Computer modeling and simulation (ICCMS)*, SanYa, China, 2010, pp. 493-501.

[22] L. Chen-Wilson, A. Gravell, and D. Argles, "Giving You back Control of Your Data: Digital Signing Practical Issues and the eCert Solution.," in *IEEE World Congress on Internet Security (WorldCIS)*, London, UK, 2011.

[23] G. Rowe, and Wright, G.,, "Expert Opinions in Forecasting. Role of the Delphi Technique," in *Principles of Forecasting*, ed: J. Armstrong, 2001, pp. 125-144.

[24] D. Argles, L. Chen-Wilson, and T. Guan, "Solving the e-Portfolio Certificate Problem," in *AACE World Conference on Educational Multimedia, Hypermedia and Telecommunications (EdMedia)*, Toronto, Canada, 2010, pp. 1006-1011.

[25] J. Wilson. (2010). *eCert program*. Available: http://www.joewilsons.net/2010/09/e-cert-programme.html (Access Date: 10 September 2010)