Towards a framework of
A Secure E-Qualification Certificate System

Lisha Chen-Wilson
School of Electronic and Computer Science
University of Southampton
Southampton, United Kingdom
E-mail: lcw07r@ecs.soton.ac.uk

Dr David Argles
School of Electronic and Computer Science
University of Southampton
Southampton, United Kingdom
E-mail: da@ecs.soton.ac.uk

***Abstract*—we all receive paper based certificates during our study journey, but they are hard to manage to avoid damage or loss. The field of e-Learning provides technological developments, such as e-portfolios, which enable greater power and flexibility in displaying achievements. These may include on-line versions of certificates of the applicant's attainment which overcome the limitations of paper-based versions. However, these "e-certificates" present a number of practical challenges, which so far have not been addressed, such as the validation of claimed e-qualification certificates. This paper addresses the issues, and explores the gap between current e-portfolio tools and the desired e-qualification certificate system. Through analysis of the existing systems and e-certificate use cases, we have identified existing services that can be reused and the services that require further development, 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 e-certificate implementations.**

Keywords — e-qualification certificate, e-certificate, e-portfolio, e-learning, trust

I. INTRODUCTION

Education certificates provide physical evidence of our achievements, milestones of our learning journeys, and are important documents that everyone needs for further study or employment. However, these paper-based certificates also come with management problems. They are easily lost or damaged, and they are hard to prove genuine when presented.

The field of e-Learning provides technological developments, such as e-portfolios, 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 e-portfolio systems. Therefore, the students' claimed achievements within e-portfolios need to be verified. Abrami[1] notes that it is difficult to authenticate the evidence in e-portfolio. The study of how we can engender trust in our on-line versions of certificates / qualification records, and making sure that our sensitive data are not being misused, is still at an early stage.

Currently, there are methods, projects, and commercial systems present in the related domain, such as digital signature, eCert[2], and Europass[3]. However, they don't satisfy our requirements sufficiently due to their various design purposes. (Analysis in section III)

In order to solve the above problems, it is necessary to implement an electronic version of qualification certificates (e-certificate) that are at least as valid as the paper-based certificates, and can be used either as a standalone application or fitted within other applications, such as e-portfolios. It needs to be easy to use and suit all levels of students while including high security methods to prevent forgery. The students need to have control over the usage of such e-certificate, and there must also be a verification method provided. We need to secure the e-certificate system, not just the e-certificate. Figure 1 outlines the challenges and the requirement of a possible solution.

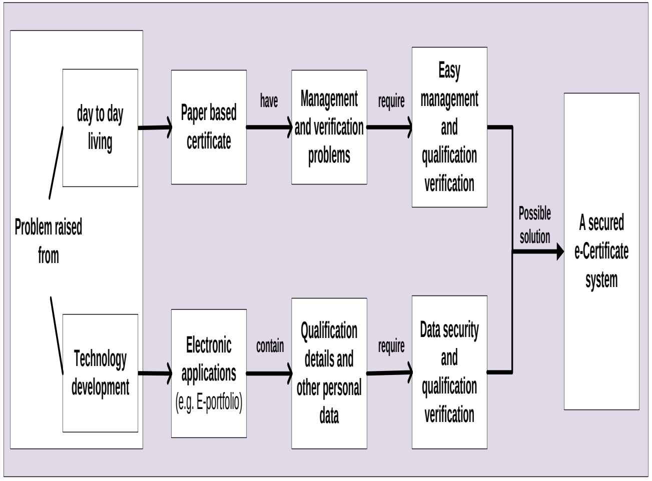

Problem raised from
day to day living
Technology development
Paper based certificate
have
Management and verification problems
require
Easy management and qualification verification
Electronic applications (e.g. E-portfolio)
contain
Qualification details and other personal data
require
Data security and qualification verification
Possible solution
A secured e-Certificate system

Figure 1. Challenges and Requirements.

II. DOMAIN RESEARCH: THE CURRENT SITUATION

Before considering an e-certificate system, it is important to review the context of the paper-based certificate, its certification process, and its related areas, such as the e-portfolio research. These will identify the requirements and methodology to investigate the e-certificate system.

Four main areas were considered as directly related to the e-certificate system, which are shown diagrammatically in Figure 2.

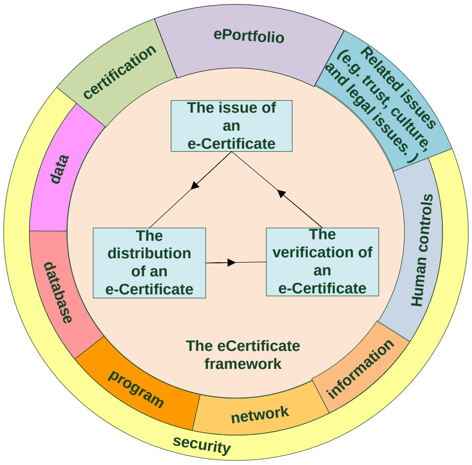

ePortfolio
certification
Related issues (e.g. trust, culture, and legal issues..)
data
Human controls
database
information
program
network
security
The issue of an e-Certificate
The distribution of an e-Certificate
The verification of an e-Certificate
The eCertificate framework

Figure 2. Related area of e-certificate

- An e-certificate is an end product of a successful certification process.
- Its security control will be the key factor of a successful system.
- Its structural design will affect the adaptability to other systems, such as e-portfolios, which is one of its main usage areas.
- Its social impact, such as trust, culture, and legal issues need to be addressed

From this figure, we may note that the e-certificate system is considered to involve three processes: issue, distribution, and verification; and has four main factors that affect the system: certification, security, e-portfolio, and related issues.

Certification: the certification process for an academic achievement involves the processes of registration and examination, and can be paper-based, computerized, or practically. The certificates, as the end result of a successful certification process, sometimes come with time limitation, such that revocation and re-certification is required[4]. Therefore, in our case of an e-certificate system, it requires the personal data and qualification records to be stored electronically to identify the person who we are issuing to, and verify that they have passed the relevant exams. The system will also need to have functions for validating and revoking any issued e-certificates when necessary.

Related issues: Different countries have different cultures, data protection acts, and legal issues; this may have an effect on the e-certificate system design. For a digitally signed certificate, the Europass[3] clearly states that, "The Europass Certificate Supplement is not: a substitute for the original certificate;" or "An automatic system that guarantees recognition", while the Digitary[5] claims that their digitally signed documents are legally valid and tamper evident. To be a true replacement of the paper-based certificate, our designed e-certificate will need to have the same legal effect as the paper-based certificate. The legal issue will be the main area to be investigated.

Security: To secure a computer-based system, we need to find out what threats it faces, what vulnerabilities it has, what controls it needs; and consider them through five components: hardware, software, data, policies and people; we also need to determine the right balance between the three goals: confidentiality, integrity and availability. In our case of e-certificate, we need to consider all these areas in our design, and find the right balance among the goals so that the system is user friendly while maintaining a high level of security.

E-portfolio: There are six types of e-portfolios. One that relates to the e-qualification certificate is the presentation e-portfolio, which is used for students and graduates to give evidence of learning or achievement and showcase their qualifications and competencies while moving into or through the workforce or further education.

The e-framework has been the backbone to help build interoperable tools for eLearning, such as the ones for e-portfolios[6, 7]. It has been facilitated by choosing a Service Orientated Architecture (SOA)[8]. The Service Orientated Reference Model (SORM)[9] was conceptualized to encapsulate the e-framework research process. The eP4LL (E-portfolios for Lifelong Learning) project developed a reference model for E-portfolios for the e-framework[10]. 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[11].

The main body of research into e-portfolios 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 e-certificate 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[10], an eP4LL project member, comments on his blog: "Security and Trust: the [e-portfolio] Reference Model sidestepped this key issue". However, the SORM methodology has been identified to investigate e-certificates.

From the benefits and issues of the e-portfolio studies, it is required that the e-certificate system design:

- needs to suit students with low IT skills
- prevent forgery
- protect privacy
- allow for verification of the certificates
- satisfy legal requirements, such as data protection, copy right, Intellectual Property Rights (IPR), ownership and stewardship
- allow for easily transfer of certificates between different systems
- minimize data storage requirements

III. Related Systems and Methods: What is Already Available

A. Digitally signed document

Technologies exist in related domains, such as digital signatures, which are used in e-documents to provide authentication, integrity, and non-repudiation. However, for the requirements of an e-qualification certificate, it has critical security holes and missing functions: for example, it uses the keys to verify the modification of the document, but doesn't start the validation of the public key certificates' status automatically. This may result in a forgery being accepted if the key has been compromised. Furthermore, even the signer's public key certificate has been validated, but the signed document itself hasn't. In our case of an e-qualification certificate, the 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 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, therefore, a simple digital signing of the document alone doesn't solve the problem.

B. Europass

The European Community provides a Europass Certificate Supplement and a Diploma Supplement[3]. 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. Also, the document is not suitable as a standalone proof of qualification in an e-portfolio as its detailed records, such as individual module marks, may work against required privacy issues.

C. the eCert project

A e-certification project, eCert[2], has explored the issues of three-party authentication and produced an award verification demonstrator. But it only verifies input qualification records against linked institution databases, which will be limited. By using this method, it also increase the risk of database attacks to those institutions. What's more, it doesn't involve e-certificates, so our paper-based certificate problem remains unsolved.

D. The Chinese Certificate Information Verification service

The Certificate Information Verification services in China[12] is a e-certification service similar to eCert. With different set of input and output 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. And again, this service doesn't deal with e-certificates.

E. Digitary (Digital Notary)

The Digitary system[5] issues, distribute and authenticate e-certificates over the internet with the system installed to institutions individually. Students need to login to their institution's system to access and manage their e-certificates, such as set access tokens for individual reviewers. Reviewers can then access the e-certificates 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 e-certificate, except the system only works for institutions individually, this is good for the e-certificate issuing process, but is not suitable for reviewers who need to verify information received from a wide range of institutions. It also comes with storage issues as it requires the system to maintain all students' e-certificates, their different version, and the corresponding access tokens for life,

IV. Formation of Use Cases: The New System

We attempted to adopt the Service Orientated Reference Model to investigate an e-certificate system as an e-Certification technique. Hence, for our first step, the e-certificate usage patterns are identified and formalized as use cases. This process involves identifying the e-certificate stakeholders, developing the cases where these stakeholders act, whilst considering similar techniques that address similar issues.

A. Stakeholders analysis

The e-certificate has three stakeholders, as showed in Figure 3: the issuer, owner, and reviewer. They perform three processes: issue, distribution, and verification.

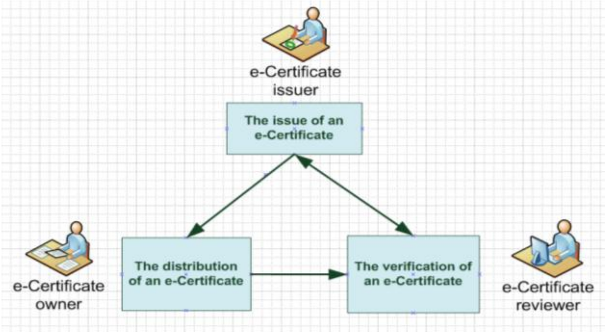

e-Certificate issuer
The issue of an e-Certificate
e-Certificate owner
The distribution of an e-Certificate
The verification of an e-Certificate
e-Certificate reviewer

Figure 3. E-certificate Stakeholder and Activities

An e-certificate issuer is a body that creates and issues the certificate, such as a college or a university. They may:

- issue a huge range and amount of certificates
- restrict database access control for any in coming verification request to minimize database attacks

An e-certificate 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 be from about the age of 14, with no upper age limit
- may hold low, high, and/or special level of qualifications
- may have qualifications achieved in different areas of UK (world-wide certificates are considered as out of the scope for this study)
- have differing levels of IT skills
- may or may not have an e-portfolio account

An e-certificate reviewer is a body or a person who receives the certificate in support of an application. This may be an academic institution or an employer. They:

- could be an individual or big organizations
- may receive e-qualification certificates as part of applications or within e-portfolios
- may have few IT skills or may have a team of IT literate staff with high tech IT equipments
- may need to check a few qualifications occasionally or may need to check a huge amount of qualifications efficiently
- may need to review varied levels of qualifications that was issued across the UK

B. *Scenarios*

With these three stakeholders in mind, scenarios have been set up to help with the understanding of the situation, depicted in Table 1.

TABLE I. USE CASE SCENARIOS

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 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.
issue	The exam board issues the e-certificates for students. But it may need to be withdrawn at a later stage. -- 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) give support for the withdrawal mechanism; c) issue the e-certificates
receiving award	The students receive their e-certificates, and view the contents. -- This needs security methods to control that no one other than the students themselves can view their own e-certificates.
manage	A student specifies certaine-certificates to be visible to particular employers. – The student needs to be able to control which e-certificate(s) for which employer(s) and 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

C. *Use case diagram*

The scenarios are shown diagrammatically as use cases in Figure 4.

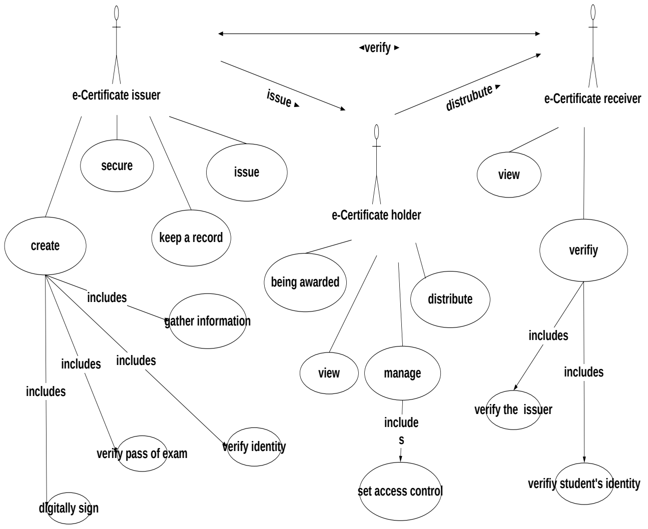


Figure 4. E-certificate use case diagram

D. *Use case analysis*

From these use cases, we may note that the e-certificate system involves assertion, trust and privacy issues during its three processes.

E-certificate assertion: the system need to be self certificating to prove its genuine, and also to allow reviewers to further confirm it. This is important from both the reviewers' perspective, as it allows them to place value in the artifact, and for the issuers, as it insures the reputation of the certificates' quality; especially as it is in the owners' interests to aggregate their own attainments. As well as generating these assertions, it should be possible to withdraw them. Parallels can be drawn with Public Key Infrastructure certificate systems, which provides the required method while also maintaining a revocation list of keys which are invalid as they have been compromised[13].

E-certificate privacy: e-portfolio 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[14]. This means the owner can tailor their portfolio to best support their application. This also applies to e-certificates, as no matter whether it is used standalone or within an e-portfolio, one aim is to give students control over who can see their e-certificates and for how long. This can prevent untrustworthy reviewers republishing the e-certificate without the owners' permission. For example to an e-portfolio bank which recruitment agencies might access. 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"[15].

Stakeholder Trust: A fundamental requirement from the use cases is the need to establish trust amongst stakeholders, such that one stakeholder can place faith that the identity of another is true, as no value can be placed in assertions generated, or any private data shown, to a party whose identity cannot be verified. Ensuring that "chains of academic trust", which are constructed as learners "gain acceptance into […] programs in large part by their standing in […] previous education", must be able to be replicated within an e-certificate system[16]. 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[17].

Distributed Stakeholders: To "stimulate large-scale uptake" of users[10], e-certificate tools need to define "architecture of participation". The e-certificate 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[18].

V. GAP ANALYSIS: WHAT IS REQUIRED AS A WHOLE

The next stage in the SORM methodology, with the use cases defined, is to perform a gap analysis against current techniques and services to discover what can be reused and which technical gaps need to be addressed.

Existing services: a) Service Orientated Architecture: By adopting the SOA of the e-Framework one meets the distributed stakeholder use case as SOA provides architecture of participation. b) Federated Identity: The formation of stakeholder trust has been addressed in previous e-framework projects, including e-portfolio projects, by utilizing the open-source federated identity system Shibboleth[11]. It is based on SAML (Security Assertion Markup Language) published by OASIS, and provides a decentralized solution for institutions to share trusted user identities between each other, such that a home user identity is valid at any of the partner institutions within the federation[19]. It would provide a framework for e-certificate 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 or adapted in order to associate the identity token of an assessor with an issued certificate.

Required Services: Current research is missing services to certify the veracity of any XML structure; therefore it isn't possible to create e-certificates to assert that an XML fragment representing the qualification is genuine. Such as mentioned before, 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 e-certificate as this signed document itself is a certificate, and may have been revoked, therefore, need to be validated. We are dealing with a certificate[2] issue which involves public key certificate and e-qualification certificate.

VI. BRIDGING THE PROFILE GAP: WHAT SERVICES CAN BE ADAPTED AND WHAT NEEDS DEVELOPMENT

A. Assertion Techniques

XML Signatures: An enveloped XML signature can be used so an issuing body can sign that a qualification is genuine and this signature can then be verified as required. To ensure that the qualification XML elements are not tampered after it has been signed, a digest of the document structure can be taken to accompany the issuers' signature, allowing a reviewer to recalculate the digest to assert the certificate is original. However, we also need to validate the certificates' state against two types of certificate revocation list (CRL): whether the signer's key has been compromised or the qualification certificate has been redraw. Without these assertions, we cannot say that the e-certificate can be accepted. Unlike digital signing, all these processes need to carry out automatically. A timestamp can also be added to enhance its integrity.

XML Watermarks: An alternative could be to watermark the XML document. Usually used to prevent and detect "unauthorized duplication and distribution" of data to enforce copyright, XML watermarks can also be used for integrity protection[20, 21]. Unlike an XML signature, a watermark might not be obvious to an end-user, and hence provides extra security through obscurity. Typically a watermarked document will require less file space than a signed document, meaning an e-certificate would be easier to store and transfer between e-Certification stakeholders[21]. However, it only asserts the document's integrity, but it cannot validate the source, in this case, the signer.

B. Privacy Techniques

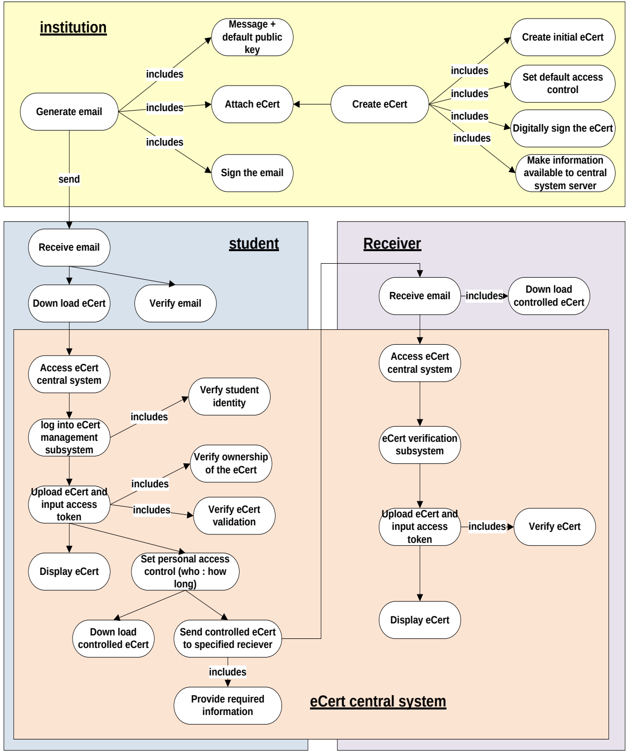
Content Extraction Signatures (CES): The privacy issue can be tackled by adopting the CES with created access tokens. CES have been developed to "enable selective disclosure of verifiable content"[22]. CES would allow an document signer to sign the document in fragments with a set of signatures, and these individual fragments can be blinded or extracted by the receiver with the corresponding keys. The access token will control who can see the document and for how long. Applying these to e-certificates, 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 e-certificate could 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 access control.

VII. Proposed Solution: The System Design

The system design aims to solve the problems that arise from our current situation, satisfy the e-certificate 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*"[23]. When used with interoperable e-portfolio XML schemas, this makes it easy for any e-portfolio vendor to integrate e-certificate services into their application; hence enabling and encouraging user take up and participation between users using software from potentially different providers.

The system design overview: The institution will create and issue a digitally signed, time stamped, and access-controlled e-certificate to the specified student through a secured emailing system. The student view and set new access controls to the received e-certificate through a central system before sending it out to further reviewers. The reviewers also use the central system to view and verify the access-controlled e-certificate. It is shown diagrammatically in Figure 5.



institution
Message + default public key
includes
Generate email
includes
Attach eCert
Create eCert
includes
Sign the email
send
includes
Create initial eCert
includes
Set default access control
includes
Digitally sign the eCert
includes
Make information available to central system server
Receive email
student
Down load eCert
Verify email
Receiver
Receive email
includes
Down load controlled eCert
Access eCert central system
Verfy student identity
includes
log into eCert management subsystem
Verify ownership of the eCert
includes
Upload eCert and input access token
includes
Verify eCert validation
Display eCert
Set personal access control (who : how long)
Down load controlled eCert
Send controlled eCert to specified reciever
includes
Provide required information
eCert central system
Access eCert central system
eCert verification subsystem
Upload eCert and input access token
includes
Verify eCert
Display eCert

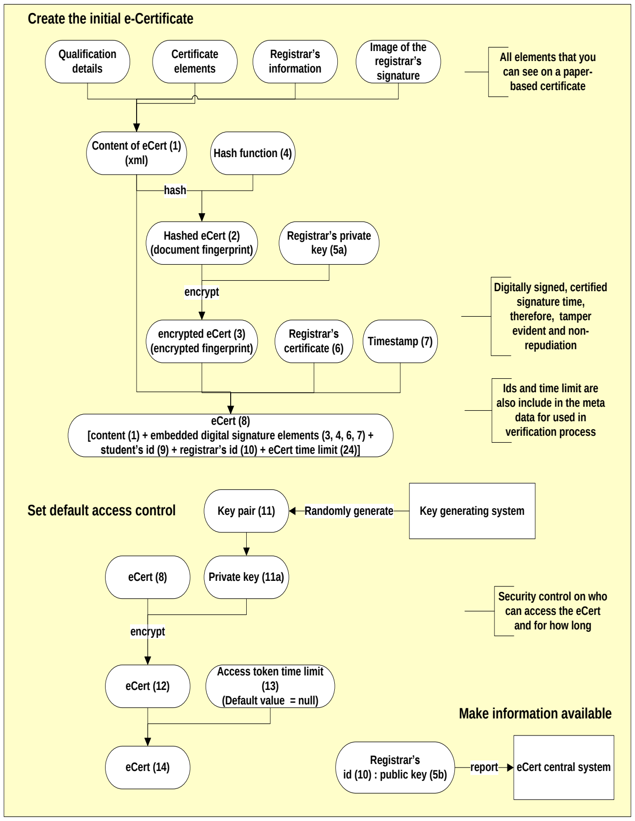
Figure 5. E-Certificate system over view

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

The system will be constructed in two parts: an issuing system and an online central system. The issuing system can be installed in individual institutions. The online central system will also be constructed in two parts: a management subsystem (for students) and a verification subsystem (for reviewers). It will provide services for e-certificates that may be issued from any involved institutions, and will be the single reference point nationwide. This will prevent confusion where the reviewers don't know which system to choose or which can be trusted, especially when they have many e-certificates issued by different institutions. This will also has the advantage of enabling close monitoring and control against fake systems.

All institutions that would like to use the system to issue e-certificates will need to be certified first, ideally a professional education body, e.g. the Ministry of Education, can be the roof of the trust node, so that no bogus institutions can be involved. All members that represent their institution, e.g. a registrar, will also need to be certified, and to be traceable back to the institution. This is shown in Figure 6.

Every student needs to register a student account when they start study at fifth form or college (the level that they will start to receive all sources of qualification certificates). The registration process will verify who the student is (same process as registering to a course at college). Each student will be assigned a unique student id nationwide. This student id will last for life. Every e-certificate that the student achieves will contain this id as proof of ownership.



Create the initial e-Certificate
Qualification details
Certificate elements
Registrar's information
Image of the registrar's signature
All elements that you can see on a paper-based certificate
Content of eCert (1) (xml)
Hash function (4)
hash
Hashed eCert (2) (document fingerprint)
Registrar's private key (5a)
encrypt
Digitally signed, certified signature time, therefore, tamper evident and non-repudiation
encrypted eCert (3) (encrypted fingerprint)
Registrar's certificate (6)
Timestamp (7)
Ids and time limit are also include in the meta data for used in verification process
eCert (8)
[content (1) + embedded digital signature elements (3, 4, 6, 7) + student's id (9) + registrar's id (10) + eCert time limit (24)]
Set default access control
Key pair (11)
Randomly generate
Key generating system
eCert (8)
Private key (11a)
Security control on who can access the eCert and for how long
encrypt
eCert (12)
Access token time limit (13) (Default value = null)
Make information available
eCert (14)
Registrar's id (10) : public key (5b)
report
eCert central system

Figure 6. Create e-certificate

All certified institutions are required to use the same standards and methods, so that the issued e-certificates can be verified by the central system nationwide. All e-certificates will be in XML format, and provide information such as "valid time" and "issue time" to meet the requirements of re-certification, revocation, and to deal with future software update issues. Every e-certificate will have access control values e.g. who can see it and for how long. This is to retain control of the distributed e-certificates, protect the students' privacy, and prevent any unauthorized use in the future. These will be signed using the method of CES. Timestamp will be used with digital signature to ensure tamper evident document, which can neither be repudiated, not accessed without authorisation.

The institution is responsible for keeping the private key (signing key) secured, and making the public key available to the central system. The students are responsible for keeping their e-certificates and the corresponding access information. In the case of loss of the original e-certificates, the institution must be contacted for reissue.

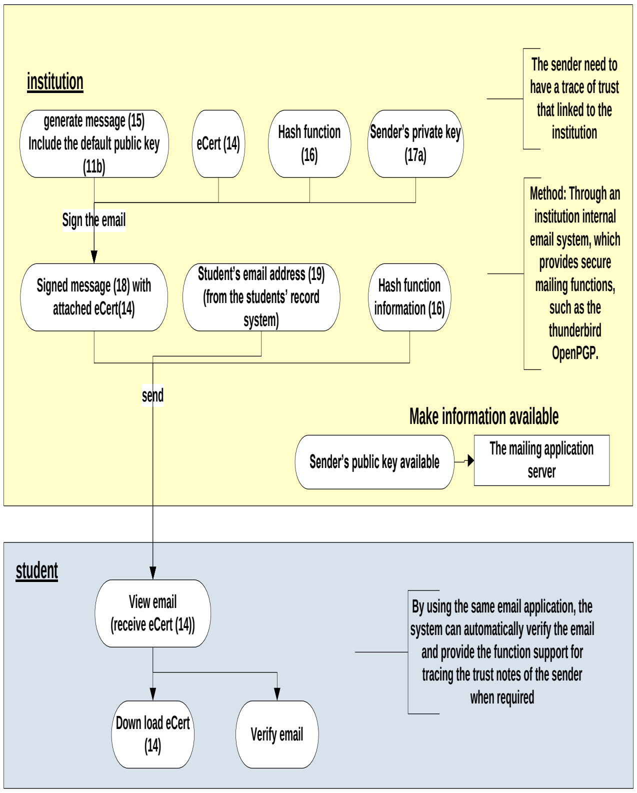

institution
generate message (15) Include the default public key (11b)
eCert (14)
Hash function (16)
Sender's private key (17a)
The sender need to have a trace of trust that linked to the institution
Sign the email
Signed message (18) with attached eCert(14)
Student's email address (19) (from the students' record system)
Hash function information (16)
Method: Through an institution internal email system, which provides secure mailing functions, such as the thunderbird OpenPGP.
send
Make information available
Sender's public key available
The mailing application server
student
View email (receive eCert (14))
Down load eCert (14)
Verify email
By using the same email application, the system can automatically verify the email and provide the function support for tracing the trust notes of the sender when required

Figure 7. Distribute e-certificate: institution →students

The institution will send the e-certificate to the specified student through its internal email system which supports secure mailing functions. This email will be signed, such that the email will be verified when received, and the sender's certificate can be traced. Here, the sender can be different from the signer, e.g. an administrator. The student will receive the digitally signed and encrypted e-certificates through email; he/she can verify the email, trace the trust note of the sender, but can't view the e-certificate without uploading it into the central system. This is to ensure e-certificate privacy, and prevent misuse of stolen e-certificates due to unexpected mailing errors. This is shown in Figure 7.

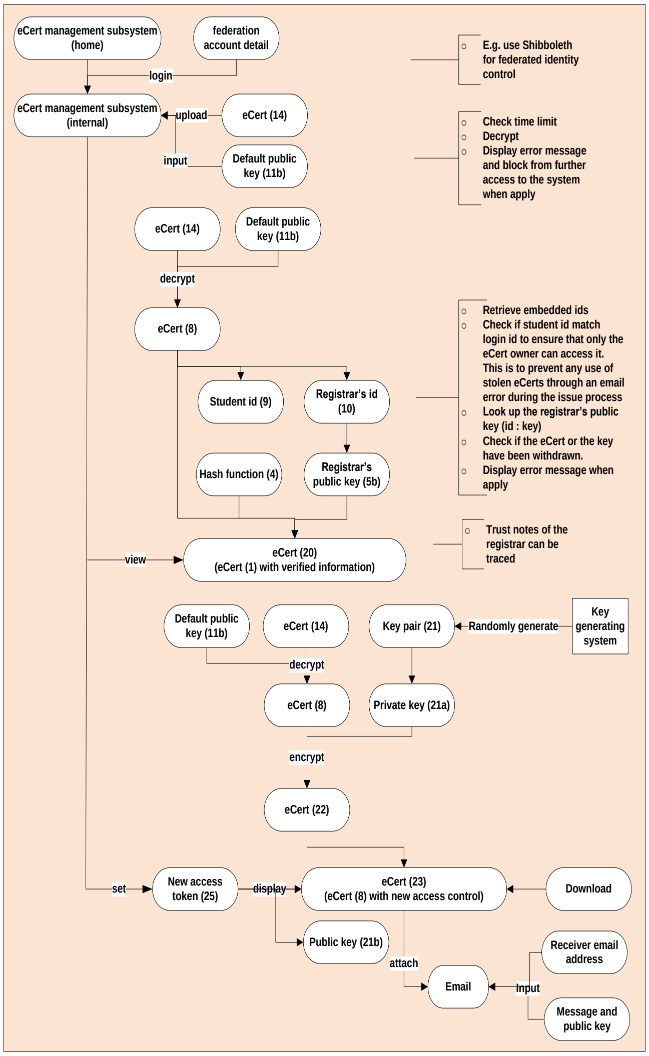

eCert management subsystem (home)
federation account detail
login
eCert management subsystem (internal)
upload
eCert (14)
input
Default public key (11b)
E.g. use Shibboleth for federated identity control
Check time limit
Decrypt
Display error message and block from further access to the system when apply
eCert (14)
Default public key (11b)
decrypt
eCert (8)
Student id (9)
Registrar's id (10)
Hash function (4)
Registrar's public key (5b)
Retrieve embedded ids
Check if student id match login id to ensure that only the eCert owner can access it. This is to prevent any use of stolen eCerts through an email error during the issue process
Look up the registrar's public key (id : key)
Check if the eCert or the key have been withdrawn.
Display error message when apply
view
eCert (20) (eCert (1) with verified information)
Trust notes of the registrar can be traced
Default public key (11b)
eCert (14)
Key pair (21)
Randomly generate
Key generating system
decrypt
eCert (8)
Private key (21a)
encrypt
eCert (22)
set
New access token (25)
display
eCert (23) (eCert (8) with new access control)
Download
Public key (21b)
attach
Email
Input
Receiver email address
Message and public key

Figure 8. E-Certificate central system - management subsystem

Students need to login and upload the e-certificate to the management subsystem to view and set new access tokens. Here, the federated identity system Shibboleth will be adapted for the login control. Once the e-certificate is uploaded and the access token entered, the system will automatically carry out the validating processes, which will include a)whether the uploaded e-certificate is belonged to the student – prevent access to stolen e-certificates that come with corresponding access tokens, b)the access token is correct and within the access time limit, c)the e-certificate has not been modified, withdrawn, and is within the valid time limit, such that no recertification is required yet, d)the signing key has not been compromised. This is shown in Figure 8.

For viewing and verifying an e-certificate, reviewers only need to upload the received e-certificate and enter the access token into the verification subsystem; the verified e-certificate will be display automatically if it has successfully passed all the validation checking processes. This is shown in Figure 9.

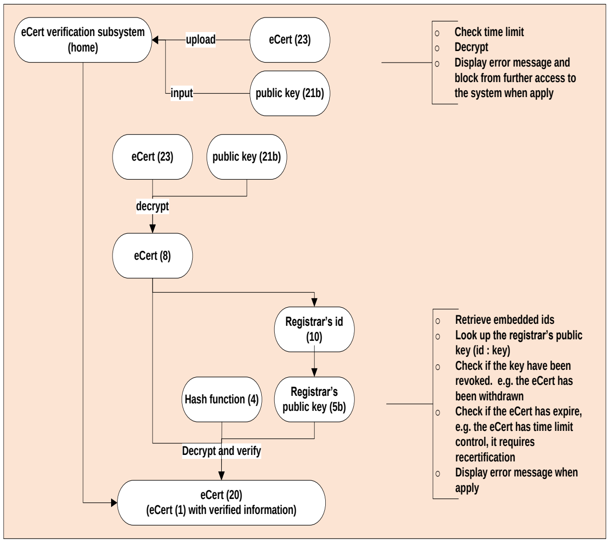

eCert verification subsystem (home)
upload
eCert (23)
input
public key (21b)
Check time limit
Decrypt
Display error message and block from further access to the system when apply
eCert (23)
public key (21b)
decrypt
eCert (8)
Registrar's id (10)
Retrieve embedded ids
Look up the registrar's public key (id : key)
Check if the key have been revoked. e.g. the eCert has been withdrawn
Check if the eCert has expire, e.g. the eCert has time limit control, it requires recertification
Display error message when apply
Hash function (4)
Registrar's public key (5b)
Decrypt and verify
eCert (20)
(eCert (1) with verified information)

Figure 9. E-Certificate central system - verification subsystem

VIII. VALIDATION OF DESIGN

Self validation of the system design has been carried out against the e-certificate use cases, it is believed that it meet all the specified requirements. Interviews have also been carried out within the University of Southampton, some year 3 students, HR managers, exam board officers have been carefully selected to represent the three stakeholders. Received commends are positive, they were happy to see the secure controls meeting their needs in different stages, while some concerns have also been raised, such as the file size for mailing; and who may hold the responsibility of the central system, as it has the need of being trusted by all involved institutions nationwide – e.g. do they all trust the Ministry of Education that is suggested in this paper? Overall, the preliminary results indicate that the system's structure and security design is successful, and could form the basis for future implementations. Further validation will be carried out with IT security professionals, industry employers, and different levels of education institutions, to spot any security holes and required functions.

IX. FUTURE WORK AND CONCLUSION

From the e-certificate challenges, gap analysis, technology researches, to the new system design, we have proposed a solution for a secured e-certificate system.

This system design does not require any e-certificate copies and sensitive data, such as private keys, to be stored in the system, while it provides all the required services through a secured environment. This feature has a huge advantage of minimizing the chances of being attacked and saving storage, especially when its usage is nationwide, and the e-certificates need to last for life. This becomes increasingly significant as the system grows in size.

We also need to look into the legal issue of digital signed document as this is the key issue of whether the designed e-certificate system can eventually replace the paper-based system.

X. REFERENCES

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

[2] Chen-Wilson, L.e.a., Secure Certification for e-portfolios, in ICALT: International Conference on Advanced Learning Technologies. 2008, IEEE: Santander, Spain.,

[3] European Communities. Opening doors to learning and working in Europe [cited 28 January 2008]; Available from: http://europass.cedefop.europa.eu/europass/home/hornav/Introduction.csp

[4] James H. Shore, S.C.S., Certification, Recertification, and Lifetime Learning in Psychiatry. 1994.

[5] Digitary. 2008 [cited 2008 August]; Available from: http://www.digitary.net/aboutus.htm

[6] Wilson, S., K. Blinco, and D. Rehak, An e-Learning Framework - A Summary. 2004, JISC-CETIS: London.,

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

[8] 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.,

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

[10] Rees Jones, P., Specifying an e-Portfolio: a Personal View. 2006, CETIS / JISC: Nottingham.,

[11] 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

[12] China Higher-education Student Information and Career Center (CHESICC), T.C.I.V.s.i.C., http://www.chsi.com.cn/about_en/,

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

[14] Grant, S., Clear e-portfolio definitions: a prerequisite for effective interoperability., in ePortfolio Conference. 2005: Cambridge.,

[15] 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.

[16] Richards, G., et al., The validation and brokering of competence: Issues of trust and technology. Interactive Learning Environments, 2007. 15(2).

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

[18] O'Reilly, T. What is Web 2.0? 2005 [cited Mar2008]; Available from: http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html.

[19] Bhatti, R., E. Bertino, and A. Ghafoor, An integrated approach to federated identity and privilege management in open systems. Communications of the ACM, 2007. 50(2).

[20] Zhou, X., et al.Query Based Watermarking for XML Data. in 2nd ACM Symposium on Information, Computer and Communications Security. 2007. Singapore: ACM.,

[21] Yao, R., et al., A Novel Watermark Algorithm for Integrity Protection of XML Documents. International Journal of Computer Science and Network Security, 2006. 6(2).

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

[23] Papazoglou, M., Service-Orientated Computing: Concepts, Characteristics and Directions, in International Conference on Web Information Systems Engineering. 2003, IEEE: Rome.