UNIVERSITY OF SOUTHAMPTON

FACULTY OF PHYSICAL AND APPLIED SCIENCE

Electronics and Computer Science

ECERT:

A SECURE AND USER-CENTRIC EDOCUMENT TRANSMISSION PROTOCOL

– SOLVING THE DIGITAL SIGNING PRACTICAL ISSUES

By

Lisha Chen-Wilson

A dissertation submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy

August 2013

A SECURE AND USER-CENTRIC EDOCUMENT TRANSMISSION PROTOCOL – SOLVING THE DIGITAL SIGNING PRACTICAL ISSUES

By Lisha Chen-Wilson

ABSTRACT

Whilst our paper-based records and documents are gradually being digitized, security concerns about how such electronic data is stored, transmitted, and accessed have increased rapidly. Although the traditional digital signing method can be used to provide integrity, authentication, and non-repudiation for signed eDocuments, this method does not address all requirements, such as fine-grained access control and content status validation. What is more, information owners have increasing demands regarding their rights of ownership. Therefore, a secure user-centric eDocument management system is essential. Through a case study of a secure and user-centric electronic qualification certificate (eCertificate) system, this dissertation explores the issues and the technology gaps; it identifies existing services that can be re-used and the services that require further development; it proposes a new signing method and the corresponding system framework which solves the problems identified. In addition to tests that have been carried out for the newly designed eCertificate system to be employed under the selected ePortfolio environments, the abstract protocol (named eCert protocol) has also been applied and evaluated in two other eDocument transmitting situations, Mobile eID and eHealthcare patient data. Preliminary results indicate that the recommendation from this research meets the design requirements, and could form the foundation of future eDocument transmitting research and development.

Table of Contents

Table of Tables

Table of Figures

Declaration of Authorship

I, Lisha Chen-Wilson, declare that the thesis entitled "ECERT: A SECURE AND USER-CENTRIC EDOCUMENT TRANSMISSION PROTOCOL - SOLVING THE DIGITAL SIGNING PRACTICAL ISSUES" has been generated by me as the result of my original research. I confirm that:

- This work was done wholly while in candidature for a research degree at the University of Southampton
- I have acknowledged all main sources of help
- Where I have consulted the published work of others, this is always clearly attributed
- Where I have quoted the work of others, the source is always given; with the exception of such quotations, this thesis is entirely my own work
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what has been done by others and what I have contributed myself (declared below and inline with the thesis)

A number of projects, with which I have been involved, have taken place during my research. Aspects of these projects are mentioned in this thesis and certain parts are the result of work completed by other members of the project team, as follows.

- **The eCert-GDP2008 project:** prior to my research focussing on the eCertificate system, a group development project (GDP) entitled eCert was run in the School of Electronics and Computer Science, at the University of Southampton, by a group of four MSc Computer Science students (Piers Royce, Patrick Newcombe, Timothy Wonnacott, and Samuel Ong), to explore the issues and solutions for online qualification authentication. The group successfully designed and developed an online qualification record verification system with selected institutions in January 2008. The design and development of the project was carried out by the group and is summarised as work previous to the eCertificate research in section 4.1 Previous work – the eCert-GDP2008 project. I oversaw the project development as a customer/client, and have published two conference papers [34, 35] as joint author with the group for this work.

- **The eCert-JISC project:** This was a research project that answered the JISC program call for an innovation project to investigate a secure eCertificate system for ePortfolios. On securing the bid, I was appointed manager of the project, entitled eCert, to develop such a system. The literature review, case study, gap analysis, and the proposed initial eCertificate system design described in the following chapters were carried out before the eCert-JISC project had taken place and were used as the basis of the eCert-JISC project. A conference paper [29] was published as a result of this initial design work. During the project, the literature review, background study, case study, and gap analysis have been revisited; the system design has been adjusted; the system demo specification and test plan have been set up. All these are my own work before they were passed to the project assistants for the demo implementation. The project assistants (Tao Guan and Xing Wang) have produced a code library for the required functions, a demo system that calls the support library, and technical documentation. My involvement related to the decision making, system testing and collaboration with the writing of the technical documentation. The system implementation was the project assistants' contribution, and is summarised in section 6.6 System Demonstrator. Two workshop proposals[11, 33] and a conference paper[32] were published during the development. This work has also been published as reported on the eCert project website [28].
- **The eCert-GDP2010 project:** I also set up a group development project (GDP) for a group of four MEng students (Carly Wilson, John Isger, James Leedham, Matthew Peter Edward Diakun) in 2010 to integrate the newly developed eCertificate system into two selected ePortfolio systems (eFolio and Mahara), aimed at testing the usage of the eCertificate system in ePortfolios. The group studied the eCert system and the two selected ePortfolio systems,

reported barriers to implementation, found bugs located in the code library, offered their ideas for eCertificate system improvements, and successfully integrated the eCertificate systems into the two selected ePortfolio systems. The development work summarized in section 7.2.5 is the group's contribution. This work has also been published as reported on the eCert project website [28].

- **The Mobile eID project:** I abstracted the concept of the eCertificate design as the eCert protocol for the secure and user-centric eDocument transmission framework, and set up a Mobile eID project to test the usage of the eCert protocol in a mobile environment, aimed at evaluating the applicability of the eCert protocol in a wider eDocument transmission domain. I carried out the background research for the mobile environment and the eID development, compared the eCertificate system with the required mobile eID system, and set up the project specification before passing it to an MSc student, Michele Zenise, for system development. Zenise studied the eCert protocol and the Mobile eID domain, following which he successfully designed and developed the eID system for the Android mobile platform. The development work of the Mobile eID application as summarized in section 8.3.5 is Zenise's contribution. This work has been published as a journal paper [179].

As project manager, my involvement in the development processes for the three projects mentioned above (eCert-JISC, eCert for ePortfolio, and Mobile eID) impacted on the research carried out for this thesis. The outcomes were analysed and have been mentioned in the following chapters. They were also summarised in a journal paper[31].

In order to further test the usage of the eCert protocol, I also set up an eHealthcare case study, employing the eCert protocol for the eHealthcare patient data transmission. I carried out background research for the eHealthcare environment and patient data transmission systems; I compared and contrasted the proposed eCertificate system, the mobile eID system and the required eHealthcare eCert system. I noted the required adjustments and then proposed the design for the system discussed in this thesis. This work is my own contribution, and is summarised in section 8.2. I have published the work as a conference paper [36].

Appendix B contains the related copyright release information for the published papers. According to each publisher’s copyright policy, procedures have been followed for reusing the materials as the author of the published papers.

Glossary

Definitions for eCertificate-related terms and their relationships are given below.

Authorization and Authentication: Authorization is the concept of allowing access to resources only to those permitted to use them. It is a process of verifying that a known person has the authority to perform a certain operation. Authentication is the process of verifying a person's identity. Thus, an authorization process makes use of the authentication process to identify system users; users can only gain authority after they have passed the authentication process.

Certification: Certification is a process of confirmation that a certain person is qualified to a stated level, in a particular field. This includes the process of identification (who you are) and verification (what qualification you hold). The outcome of a certification process is a certificate. E-Certification will be referred to as an e-Assessment process, such as a student goes through when their learning is assessed in order to determine whether to grant them an award of achievement. For example, a student may take an on-line test, or series of tests, to be granted the award of the European Computer Driving Licence.

eCertificate: A "paperless reward certificate". eCertificate is the term used throughout this thesis to mean the digital form of qualification certificate. It is the electronic qualification information that is associated with individuals – the electronic document itself. In this thesis, eCertificate is not the public key certificate or any other kinds of authentication certificate. It is described in more detail in section 3.2.

Identification: Identity is referred to as attribution to yourself (consciously or unconsciously) of the characteristics that make you different from others[1]. In terms of

[1] TechTarget. (2007). Definition. Available: http://searchsecurity.techtarget.com/sDefinition/

certificate of qualification, identification is a process of identifying a person, i.e. confirming that he/she is who they say they are. This may be done through documents, such as passports or birth certificates, and through physical and biometric recognition, such as fingerprints or signatures. Identification may also be carried out by computer, such as an on-line authentication system, which involves an identification process.

Validation: Validation refers to a checking process to confirm that the stakeholder's requirements are satisfied. It is often invoked in the process of identification and verification. This includes checking that the documents are up to date (not expired), applicable and acceptable by the specified situation. For example, a library card may not be acceptable as a proof of identity outside the library, and a student who was awarded a "First Aid" certificate three years ago may not pass the validation check if the award is only valid for two years before they must attend a refresher course. In the case of eCertificates, it is also especially important to check in case an award has been revoked for any reason. While verification checks whether an eCertificate is a forgery for example, validation checks whether a genuine eCertificate is still valid in the current context.

Verification: Verification is an additional proof of something that was believed (fact, hypothesis or theory) correct[2]. It is usually an internal quality process of determining compliance with a regulation, standard, or specification. In terms of certificate of qualification, verification is an on-line checking process, which verifies that an eCertificate is not a forgery and has not been tampered with, by looking for a match against a trusted system.

Certification processes: A paper-based certificate system will include certification, identification, validation, verification, authorization and authentication during its issue, distribution, and verification processes. The relationships of the terms and processes for the proposed eCertificate system is available in Appendix J.

[2] webopedia. (2007). Definition. Available: http://www.webopedia.com/TERM/

Acknowledgements

This thesis would not have been possible without the help and guidance of several individuals. I am grateful for their support during the period of my PhD.

First, special thanks to my supervisors, Dr David Argles and Dr Andy Gravell, for being excellent teachers and wonderful friends, guiding me, challenging me, and supporting me throughout my PhD research;

Dr Gary Wills, my PhD adviser, for giving me his time, advising me and guiding me throughout my research;

Chris Brown, the Joint Information Systems Committee (JISC) program manager, for his support throughout the eCert project. Piers Royce, Patrick Newcombe, Timothy Wonnacott, Samuel Ong, the eCert-GDP2008 project team; Rob Blowers, Tao Guang, Xin Wang, the eCert-JISC project assistants; Carly Wilson, John Isger, James Leedham, Matthew Peter Edward Diakun, the eCert-GDP2010 project team and Michele Schiano di Zenise, the Mobile eID project developer, for their hard work and support in the eCertificate-related projects. All colleagues in the Learning Societies Lab, for their comments, suggestions, and technical support;

All members from the ePortfolio team at the International ePortfolio Development Centre at the University of Nottingham, for their help and advice.

Dr Quintin Gee for proofreading this thesis.

Chapter 1 Introduction

This chapter introduces the research background, describes the problems currently being faced and describes the research challenge. It also states the research contribution and methodologies, and outlines the structure of the whole thesis.

This chapter is entirely the researcher's own work, Some sections have been published in conference papers [29, 36] and on the eCert project website [28].

1.1 Research Background

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 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. The students' claimed achievements within ePortfolios need to be verified. Professor Abrami, of the Centre for the Study of Learning and Performance (CSLP) at Concordia University in Montreal, notes that it is difficult to authenticate the evidence in ePortfolios [1].

Whilst paper-based records and documents are gradually digitized, concerns about how such electronic data is stored and transmitted have also increased. The traditional "Fortress" [44, 122] approach security method, which is systems orientated to protect the system against misuse from both outside attackers and uninformed legitimate users, is being challenged. The world within which users operate is changing – there is now a need to deal with peer-to-peer networking, social networking and linked data. In this environment, the prevention of unauthorized modification and loss of records is vital. Such concerns are compounded by the knowledge that institutions that the public ought to be able to depend upon for maintaining the security of documents appear to have inadequate systems in place. In the UK, the government has been responsible for the loss of 10 million personal records that included bank account details [152], and other examples exist of serious breaches of security protocol.

Besides the potential for human error, as noted above, there is also legitimate concern that confidential personal data could be passed to other organisations for financial gain. Without a system of checks in place, there is no guarantee that confidential data will not be abused. In this context, it is understandable that information owners have increasing demands regarding their rights of ownership. As a result, there are now pressing calls for secure and user-centric systems in a wide range of domains, which aim to give owners the opportunity to choose where and how their information is collected and stored.

1.2 Benefits of eCertificate Research

Students build up portfolios of their achievements as they study, which are then presented when they apply for jobs or for further study. The field of eLearning provides technological developments in ePortfolios, which enable greater power and flexibility in displaying achievements; and is being explored as an improvement over paper-based portfolios in the job and course application process. In the UK, a number of projects have been implemented, such as the eP4LL [124] project. Research indicates that such ePortfolios offer a number of advantages over paper-based ones, such as the potential for the inclusion of a rich set of materials, e.g. dynamic art or films that would be impossible to include in a paper-based portfolio.

The government body, the Joint Information Systems Committee (JISC)[3], is funding the project, eCert, to research for a potential solution for secured electronic qualification award certificate (eCertificate) that can be used as standalone or serviced within ePortfolio systems. The aim of the project is to clarify design requirements, propose a solution with a demonstrator that shows how these requirements can be met.

Students would benefit from eCertificate development as such an approach would solve the certification problem, and engender an atmosphere of support and encouragement in terms of maintaining a life-long commitment to personal growth and development.

The eCertificate challenge represents a special instance of a digitally signed eDocument (i.e. one which involves non-static content; requires authentication, lifelong availability, maintains ownership rights, and needs to be transmitted to two or more parties, whether known or not). The eCertificate solution could be applied in other eDocument transmission domains to solve their security and ownership issues.

1.3 The Challenges

Digital signatures are being used in eDocuments to provide authentication, integration, and non-reputation. For example: currently, there are many commercial systems offering eDocument signing services. However, these traditional digital signatures and existing commercial systems are considered insufficiently secure, and do not satisfy the user-centric eCertificate requirements as the eCertificate system presents special challenges:

- The involvement of non-static content - the signing key may not be alone in being compromised, its content, the award qualification, may be withdrawn;

[3] Joint Information Systems Committee (JISC) "*supports United Kingdom post-16 and higher education research by providing leadership in the use of ICT (Information and Communications Technology) in support of learning, teaching, research and administration. JISC is funded by all of the UK post-16 and higher education funding councils*." http://www.jisc.ac.uk/

- Owner control demands – the student, as the owner of the eCertificate, needs to have control over its usage;
- Lifelong availability requirements – verifiable throughout a student's lifetime;

However, at present it appears that the traditional digital signature systems and existing commercial systems provide no method for:

- Checking whether content revocation is in place – only the signing key revocation is checked;
- Independent user-centric control - Third party access control of an eCertificate needs to rely on the issuing institution's or signing service provider's support systems. In this case, a re-sign process will need to take place to generate the distinct access key. However, the owner still has no control over the distributed eCertificates, which in turn, may be passed on without owners' consent.
- Lifelong availability – At present, this relies on the issuing institution's or service provider's willingness to hold the certificate over time or the guarantee that the organisation remains in business.

Evidence in support of these claims is considered and discussed in Chapter 3. Despite significant efforts by industry these problems are still largely unsolved. So the design and development of eCertificate is a contribution with potential for significant impact in a number of domains such as the ones considered in Chapter 7 and 8. The user-centric approach has ensured that barriers to adoption have been removed.

Without an efficient user-centric security control in place, a digitally signed eCertificate would be useless as it still could not be trusted and the owner could not control its confidentiality or guarantee its availability. These issues also affect other digitally signed eDocuments in similar situation, e.g. eContracts with dynamic contents.

The problems that the public are facing need answers. In order to overcome the problems of education certificates and to enable qualification information to be distributed securely, efficiently, and with owners' consent, it is necessary to design an eCertificate system. Figure 1-1 outlines the research background and the challenge diagrammatically.

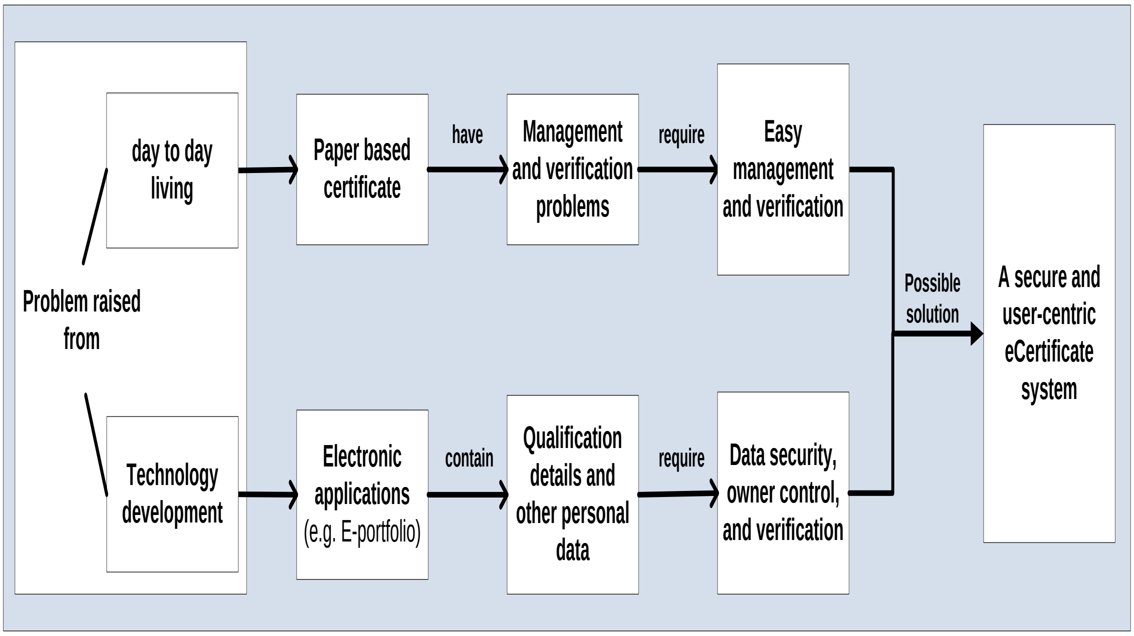

Problem raised from
day to day living
Technology development
Paper based certificate
have
Management and verification problems
require
Easy management and verification
Electronic applications (e.g. E-portfolio)
contain
Qualification details and other personal data
require
Data security, owner control,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

Figure 1-1 Outline of the research background and the challenge, published in [28, 29]

This eCertificate challenge requires the system to handle the certification and verification processes, and meet the lifetime validation requirement, whilst satisfying document ownership rights.

1.4 Hypotheses and Research Methods

The researcher believed that the current technology is ready for the design and implementation of the eCertificate system, so that an eCertificate can be secured and is verifiable lifelong, and the student owner can have control over its use independently from its issuing body. What's more, the concept of the eCertificate solution can be applied to related eDocument transmission and verification domains to solve their security and ownership issues.

Two research methodologies have been selected for this research: the Service Orientated Reference Model (SORM) [173] was employed for the eCertificate system development, to investigate how services fit together to provide the required functionalities. The Delphi method [88] was used for guiding and evaluating the decisions making during the eCertificate system development, alongside the SORM methodology.

1.5 Original Contributions

Through the eCertificate case study, this research has produced results such as:

- the identification and addressing of a particular content validation issue; this has been called the eCertificate square problem in this thesis;
- a new signing method to address owner control requirements, enabling authorized modifications of the access values to a signed eDocument without the need for digital re-signing;
- a new system structure which works with the proposed new signing method. The new system forms a framework resulting in a centralized verification system for secured and owner-controlled distributed data, independent from the issuing bodies to ensure lifelong availability.

This research has also proposed an abstracted eCert protocol, which have been tested through two evaluation studies. This abstracted eCert protocol can be applied across a variety of application domains, not just the ones originally selected. It can also be applied to the “big picture” of secured eDocument transmission and verification, thereby resolving the related security issues with existing eGovernment, and eBusiness systems.

1.6 Thesis Structure

The rest of this thesis is organised in the following way:

Chapter 2 defines the research focus, the research hypothesis, and the methodologies employed.

Following the selection of SORM methodology, the literature review is carried out in Chapter 3, which examines eCertificate-related areas to find out what is being studied in the field.

Domain Research presented in Chapter 4 explores what systems/projects are already available alongside the literature, what can be adapted, and what limitations need to be overcome, in order to make an informed decision to investigate the eCertificate system.

Chapter 5 presents the eCertificate case study. It follows the steps of SORM, describes the use cases, the technical gap, and the outcome of service profiles analysis.

From service profile, design, to system implementation, Chapter 6 presents how the system was developed under the SORM methodology.

Chapter 7 shows the system testing and evaluation using the Delphi methodology.

The proposed eCertificate system is then abstracted as the eCert protocol, and evaluated in Chapter 8 to test the usage of the eCert solution in a wider domain.

The thesis ends with the conclusion in Chapter 9, summarising the research, and proposals for future work.

Chapter 2 Research Hypothesis and Methodology

This chapter describes the research hypotheses and methodologies, indicating the focus of the research and the methods employed. This chapter is entirely the researcher's own work.

2.1 Research Direction

In order to solve the current paper-based certificate management issue, satisfy the requirement of proving the achievements claimed in an ePortfolio, while addressing the increasing issue of privacy within eDocument and answering the calls for enhanced owner control, it is necessary to design a secure eCertificate system that is as valid as the paper-based certificates, and can be verified in a legal context. It needs to be available throughout the student owner's life, be able to be withdrawn, and be used either as a standalone application or serviced within other applications, such as ePortfolios. The students, as the owner of the eCertificate, need to have the ownership right and be able to control its usage. Such an eCertificate also needs to be easy to use and suit users with low IT skill levels while maintaining high security methods to prevent forgery and providing a verification service. We need to secure the eCertificate system, not just the eCertificate alone.

2.2 Research Hypotheses

This research is intended to establish the claim that:

Hypothesis 1: the current technology has the required features that can be used or adapted to support the design and implementation of the eCertificate system, so that an eCertificate can be secured, rendered permanently verifiable and allow the student owner to have control over its use independently from its issuing body.

Hypothesis 2: the concept of the eCertificate solution can be applied to related domains, such as other eDocuments that face similarly complex situations, to solve their security and ownership issues.

2.3 Research Plan

In order to test the hypotheses, the research is planned in three steps: 1) use eCertificate as a case study to research a solution for the problem of eDocument transmitting; 2) design and build a demonstration system to test and evaluate the design and hence test the hypothesis 1 to a satisfactory extent; 3) apply the eCertificate solution to another instance of eDocument transmission in order to test the use of the eCertificate concept in a wider eDocument transmitting domain, and hence test the hypothesis 2 to a satisfactory extent.

2.4 Research Methodology

To make the research process efficient, the principles of research methodology have been studied, and as a result, two research methods have been selected.

2.4.1 What Research Methodology Is

While research is a journey of discovery, research methodology is "*the science of studying how research is done scientifically*". Sridhar [148] describes research methodology as "*a way of systematically solving the research problem by logically adopting various steps*." Saunders and Lewis describe it as "*the theory of how research should be undertaken, including the theoretical and philosophical assumptions upon which research is based and the implications of these for the method or methods adopted*."

Saunders and Lewis summarise research methodology in the following way [135]:

- "*All business and management research projects can be placed on a basic-applied continuum according to their purpose and context*."
- Research projects are "*undertaken for different purposes*", and can be categorized as "*exploratory, descriptive and explanatory*".
- "*The main research strategies are experiment, survey, case study, action research, grounded theory, ethnography and archival research.*"
- Research projects may be "*cross-sectional*" or "*longitudinal*".
- Quantitative and qualitative are used to "*differentiate both data collection techniques and data analysis procedures*".
- "*Using multiple methods can provide better opportunities to answer a research question and to evaluate the extent to which findings may be trusted and inferences made.*"

Adams and Cox [4] have described three evaluation techniques: questionnaires, in-depth interviews, and focus groups. They state that questionnaires are "*usually paper based or delivered online and consist of a set of questions which all participants asked to complete*"; interviews are "*usually conducted on a one-to-one basis ... require a large amount of the investigator's time during the interviews and also for transcribing and coding the data*"; focus groups "*usually consist of one investigator and a number of participants in any one section*." They also point out that the benefit of using questionnaires is that they "*can be delivered to a large number of participants with little effort*", while interviews can be "*flexible and in-depth*", and focus groups "*often result in useful data in a shorter space of time*."

In some research, the combined use of "*quantitative and qualitative data collection techniques and data analysis procedures*" can bring benefits. Morse [134] describes it as "*to obtain different but complementary data on the same topic*." However, it can not be easily applied to all situations, depending on "*what is being studied, how it can be studied and what the goals of the research are*" [5]. Adams, Lunt and Cairns pointed out that "*there are many complex, socially based phenomena in HCI that cannot be easily quantified or experimentally manipulated or, for that matter,* *ethically researched with experiments*,” such that researchers in HCI are “turning to more qualitative methods in order to deliver the research results that HCI needs.” Adams also stated that “*With qualitative research, the emphasis is not on measuring and producing numbers but instead on understanding the qualities of a particular technology and how people use it in their lives, how they think about it and how they feel about it*” [5].

2.4.2 Benefits of Research Methodology

Sridhar [148] summarised the benefit of research methodology as:

- “*Advancement of wealth of human knowledge*”
- “*Tools of the trade to carry out research; provides tools to look at things in life objectively*”
- “*Develops a critical and scientific attitude, disciplined thinking or a ‘bent of mind’ to observe objectively (scientific deduction & inductive thinking); skills of research will pay-off in long term particularly in the ‘age of information’ (or too often of misinformation)*”
- “*Enriches practitioner and his practices; provides chance to study a subject in depth; Enable us to make intelligent decisions; understand the material which no other kind of work can match*”
- “*As consumers of research, output helps to inculcate the ability to evaluate and use results of earlier research with reasonable confidence and take rational decisions*”

2.4.3 The Selected Research Methodologies

A number of appropriate methodologies have been shortlisted. A brief description and comparison of these methodologies is available in Appendix K. According to the earlier findings that multiple methods can “*provide a better view*” into a research topic [135], and since the goal of this research was to understand the issues and find a solution for the problem rather than measuring and benchmarking the proposed system, a software development research methodology, Service Orientated Reference Model (SORM), and a qualitative based research methodology, Delphi, were chosen.

2.4.4 The SORM Methodology

The Service-Oriented Reference Model (SORM) is a “community-driven” methodology for “understanding how services fit together to provide functionality for a particular domain” [174]. It was initially invented to develop the e-learning framework reference model for assessment in 2006.

2.4.4.1 The background

The e-Framework for Education and Research is “*initiative by the UK’s Joint Information Systems Committee (JISC) and Australia’s Department of Education, Science and Training (DEST)*”. It aims to produce an “*evolving and sustainable, open standards based service oriented technical framework to support the education and research communities*” [112]. The e-Framework “*supports a Service Oriented Architecture (SOA) for developing and delivering education, research and administration systems*”, which provide benefits that “*maximise the flexibility and cost effectiveness with which systems can be deployed and enabled to work together at the institutional, national, and international levels*” [112]. A core benefit of SOA is “*interoperability, as service interfaces are described in a standardized manner; providing portability as the service can be consumed or implemented on any platform that supports the required protocols*.” It has been “*the backbone to help build interoperable tools for eLearning,*” [20], such as ePortfolio and eAssessment.

Framework Reference Model for Assessment (FREMA) was a project aiming to provide a structured navigation method for all standards, services and use cases of the assessment domain within the eFramework [173]. To assist the project, SORM methodology was employed to encapsulate the eFramework research process and it has successfully performed the complex and difficult task.

2.4.4.2 The layered SORM methodology

The SORM suits varies domains, and is conceptualised into a number of layers with defined relations between the layers: "*For tightly constrained domains, it may be possible to define a vertical slice through the layers, such that each layer exactly maps onto its vertical neighbours. For broader domains where each layer is smaller in scope but more concrete than the one below it, a Community Reference Model approach is more appropriate*." [173]. Figure 2-1 shows the layers of the SORM and the processes in between.

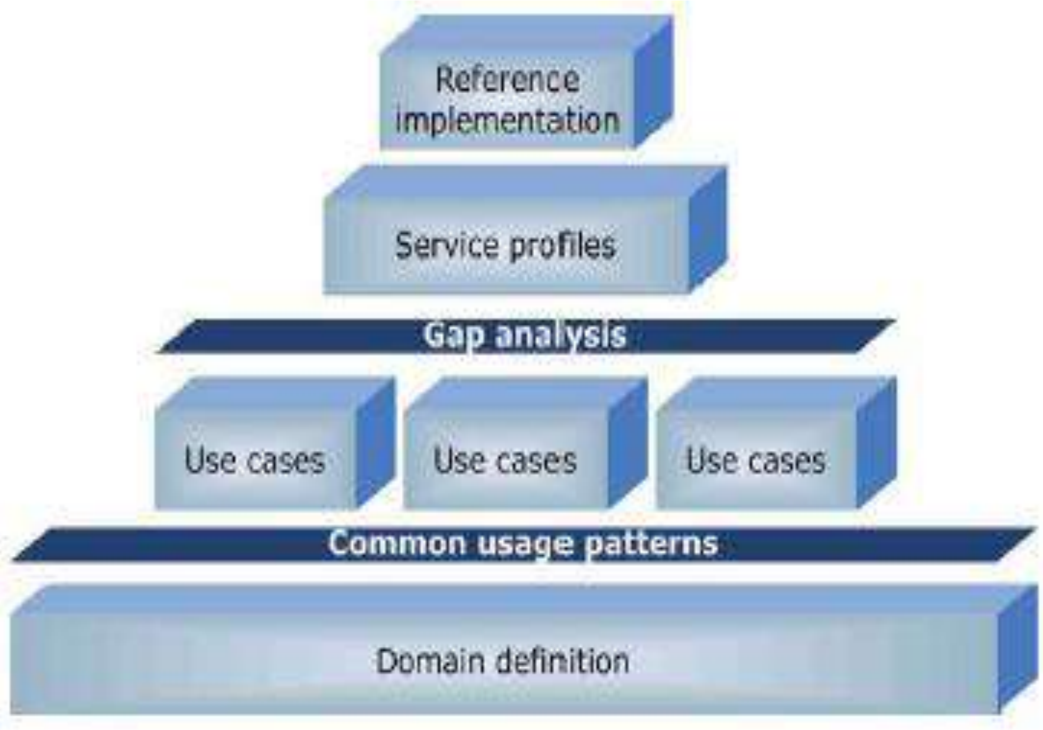


Figure 2-1 The Abstract Layers of a SORM, reprinted from [173]

- The layered model starts from a **Domain Definition**, which provides an overview of the reference model, as it "*contains instances from the ontology of domain resources (such as standards, people, and projects) and also the ontological relationships between them*" [173].

- **Identifying Common Usage Patterns** is the process of "*scoping the domain into a manageable subset*". The patterns should include "*all key activities*" from domain experts, both the "*areas that lie unarguably within the domain*" or "*the reflection of the resources*" [173].
- With the usage patterns defined, they can then be formalised into **Use Cases** to "*formal descriptions of user activity in both diagrammatic and narrative form*" [173].
- A **Gap Analysis** is then performed against the framework to identify if any of the use cases require services "*missing a formal definition*" [173].
- With the result from the Gap Analysis, a series of **Service Profiles** for each required service can be generated. These Service Profiles are "*abstract descriptions of a service that may be fulfilled by several different Service Implementations that potentially expose different concrete interfaces*." They can be collaborated with other services to "*fulfil its own specific use case*" [173].
- **Reference Implementation** is the "*most concrete layer*" of the service profiles, although "*not all services will necessarily be implemented*" while "*some may be wrappers around existing software*." The implementations are not necessary "*as definitive enterprise level pieces of code*", but can be used as "*exemplars that validate the service profiles and demonstrate any interoperability*" [173].

2.4.4.3 Reason for choosing the SORM methodology

The eCertificate research fits well into the e-Framework as it relates to education and many of the eLearning systems; an eCertificate will be the end result of successfully passing an assessment, and it can be used in an ePortfolio. From employing the SORM methodology, we are taking the same SOA approach that supports the education and research communities, which will not only assist the research process, but can also maximise the interoperability between systems and software across the e-Framework.

2.4.5 The Delphi Methodology

The Delphi methodology is a "*structured communication technique that originally developed as a systematic, interactive forecasting method which relies on a panel of experts*" [88].

2.4.5.1 The background

Delphi is widely accepted as a "*forecasting tool*". It has been used successfully in technology forecasting for "*thousands* of studies" and has been applied "*with high accuracy*" in other areas, such as business, economic trends, health and education [88]. The technique has also been adapted for use in "*face-to-face meetings, called mini-Delphi or Estimate-Talk-Estimate (ETE)*", and in web-based experiments, as a "*communication technique for interactive decision-making and e-democracy*" [88].

The principle of Delphi methodology is that "*forecasts (or decisions) from a structured group of individuals are more accurate than those from unstructured groups*" [131]. Such a process "*is effective in allowing a group of individuals, as a whole, to deal with a complex problem*" [88], which has also been referred to as "*collective intelligence*" by Hiltz [78].

Delphi methodology has three main characteristics: "*structuring of information flow*", "*regular feedback*", and "*anonymity of the participants*". These characteristics "*help the participants focus on the issues*", and makes Delphi stand out from other methodologies" [88].

- Structuring of information flow: the experts' initial answers and comments on the questions will be collected, processed, and irrelevant content will be filtered out by the panel director. This not only avoids the negative effects but also "*solves the usual problems of group dynamics*".
- Regular feedback: the participating experts can access others' responses, review and comment on their own forecasts in different stages of the process; this can improve the discussion result.
- Anonymity of participants: the identities of the participants may remain anonymous during the whole process to prevent domination by or from

others, which also "*allows free expression of opinions and encourages open critique*".

The panel director who coordinates the Delphi method, "*also known as a facilitator*", has the responsibility for selecting the panel of experts, setting the questions, collecting and analyzing responses, and identifying the common and conflicting viewpoints.

2.4.5.2 The four phases of Delphi

The method starts by selecting a group of domain experts who hold knowledge on an issue and a set of initial designed questions. The process undergoes "*four distinct phases*" [88].

First phase – exploration: the aim of this phase is to explore the subject by collecting information from the expert panel that they feel "*is pertinent to the issue*".

The second phase – agreement analysis: this phase involves "*the process of reaching an understanding of how the group views the issue," what participants agree and disagree on, what they think is of "importance, desirability, or feasibility*."

These first and second phases may be carried out for two or more rounds. After each round, the experts' forecasts and the reasons that support their forecasts will be summarised, their viewpoints will be identified, filtered, and analyzed. The experts are "*encouraged to revise their earlier answers in light of*" the others' opinions. It is believed that through this process, "*the variety of answers will decrease and tend towards one direction*".

The third phase – further exploration: if there is "*significant disagreement*", then it will be explored to "*bring out the underlying reasons for the differences*" and the possibility of solving them.

The last phase – final evaluation: the process will stop "*after a pre-defined stop criterion*", such as "*number of rounds*", or "*stability of results*". "*All previously gathered information will be analyzed*" and the evaluations will be "*fed back for consideration*".

2.4.5.3 Reasons for choosing the Delphi methodology

Delphi was first developed for the field of science and technology forecasting [40], and later extended to many other areas, including technology in education and policy-making. It has been applied successfully with high accuracy in many cases [14, 77].

The nature of eCertificate research lies in the field of technology and education, and aims to identify the existing issues and technology gaps and find solutions to the problem. This is not easy in a field of rapid change such as technology, where the degree of uncertainty is so great. Delphi would be the right tool to collect the latest opinions from experts in the field, and through the controlled process, help with finding a way towards a final design decision.

Employing Delphi will benefit this research by gaining the latest knowledge of "collective intelligence" and finalising the design decision with the help of the panel experts in a reasonable time.

2.4.6 Applying the Selected Research Methodologies

The comparison demonstrates that for this research, a combination of SORM and Delphi is considered to be most suitable. As multiple methods can provide a better vision of a research topic, employing these two methodologies together would provide a better research outcome. The SORM was selected to investigate the eCertificate framework, and the Delphi research methodology was identified to guide and evaluate the eCertificate system design alongside the SORM methodology.

- From literature review, and domain research, to eCertificate use case, gap analysis, services investigation, and system design and implementation, the research processes of the eCertificate system development were carried out following the SORM methodology.
- In parallel with the SORM methodology, Delphi methodology was employed step-by-step alongside the eCertificate system development. Domain experts' opinions were collected and analysed to guide the system design decisions.

- managers, IT security experts, and exam board officers were selected at national level to represent the eCertificate stakeholders;
- group discussions were employed to investigate the related issues and guide the new system design;
- design adjustments were made according to the outcome at each round.
- At the final round discussion, the developed system was brought back to the selected stakeholders to test whether it met the requirements, and any issues were addressed where required.

2.5 Chapter Summary

In this chapter, the research hypotheses were raised after the research direction was identified. The research methodologies, SORM and Delphi, were selected and a plan of how to apply these methodologies to the eCertificate case study was set up, to be used as a step-by-step guide in the future research, which would lead the researcher to create a design to be implemented and tested both the eCertificate domain and two other related domains.

Chapter 3 Literature Review

The first step of the SORM methodology is Domain Definition. In order to provide an overview of the eCertificate domain, the literature review has looked into eCertificate usage and security related areas, which include certification, ePortfolio, system security, encryption, privacy, and ownership right.

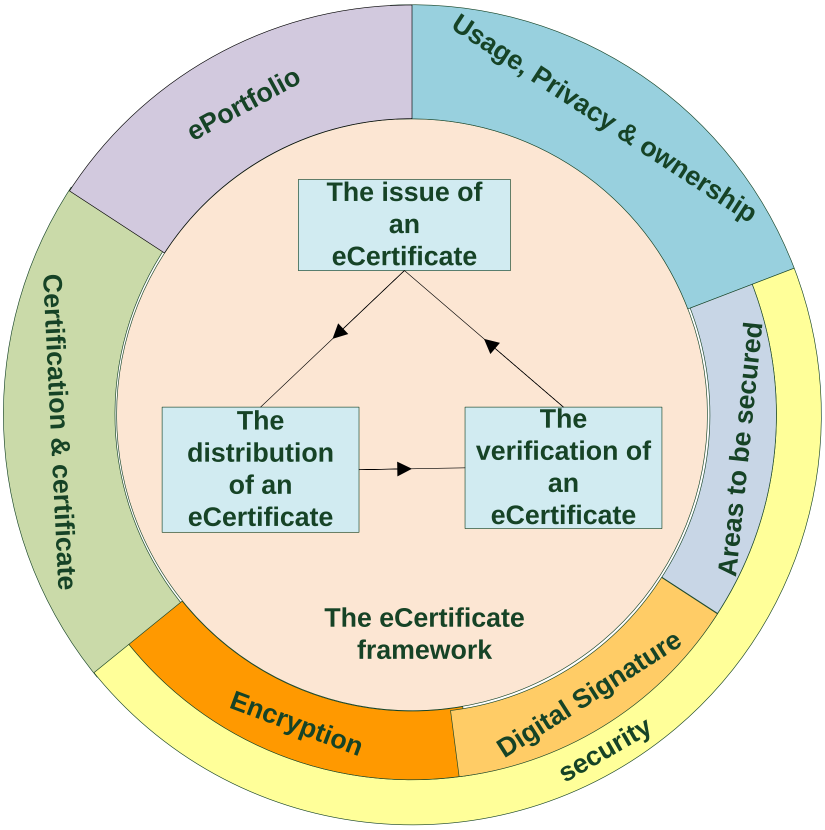

ePortfolio
Usage, Privacy & ownership
Certification & certificate
Areas to be secured
The issue of an eCertificate
The distribution of an eCertificate
The verification of an eCertificate
The eCertificate framework
Encryption
Digital Signature
security

Figure 3-1 Related areas of eCertificate

The relationships between the literature review topics are shown diagrammatically in Figure 3-1.

- An eCertificate is an end product of a successful certification process
- Security control will be the key factor of a successful system
- Its structural design will affect adaptability to other systems, such as ePortfolios, which is one of its main usage areas
- Its social impact, such as privacy and ownership need to be addressed

From Figure 3-1, we may also note that the eCertificate system involves three processes: issue, distribution, and verification. Google Scholar and some online digital libraries, such as ePrint, ACM Digital Library, IEEE Xplore, and WebCat, were used as the web-based tool for the literature search. Relevant key words, such as “certificate and certification process”, “digital signing method”, “ePortfolio systems”, “computer security”, “encryption methods”, and “privacy issues”, were used during the search. Materials were selected based on first scanning of abstracts and conclusions, and then the details of content, where applicable. Recent publications with a high number of citations were chosen over the others.

This chapter summarises the eCertificate related work published in literature. The chapter is expressed in the researcher’s own words.

3.1 EPortfolio

The purpose of this section is to develop a greater understanding of how to explore the domain of eCertificate for ePortfolios.

3.1.1 Definition of ePortfolio

A portfolio is commonly referred to as a large, flat, thin case, usually leather, for carrying collected pieces of creative work, such as loose papers or drawings or maps, to be shown to potential customers or employers. In finance, a portfolio is an appropriate mix of investments held by an institution or a private individual[4]. In terms of educational institutions, a portfolio is "*a collection of evidence that is gathered together to show a person's learning journey over time and to demonstrate their abilities*" [24].

An electronic portfolio is also known as an "ePortfolio", "efolio", "digital portfolio", or "webfolio". Butler [24] defines it as: "*an electronic version of a paper-based portfolio, created in a computer environment, and incorporating not just text, but graphic, audio and video material as well*." Abrami and Barrett [1] define it as: "*a digital container capable of storing visual and auditory content...designed to support a variety of pedagogical processes and assessment purposes*." Challis [27] defines it as a "*selective and structured*" collection of information "*gathered for specific purposes and showing/evidencing one's accomplishments and growth*"; It is "*stored digitally and managed by appropriate software; developed by using appropriate multimedia customarily within a web environment*" and can be "*retrieved from a website, or delivered by CD-ROM or by DVD*".

ePortfolios are a growing area of eLearning research. They provide a useful way for users to "*document their academic achievements*", support applications to employers and/or further education institutions during the transition points of the user's/(owner's) career [71]. It has been "*encouraged, with the intention that such a system should ultimately replace the current paper-based system*". A number of projects have been implemented, such as eP4LL [108], which have led to a reference model for ePortfolios [123].

3.1.2 Types of ePortfolios

There are six major types of ePortfolios catalogued in IMS ePortfolio [79]: "*Assessment ePortfolios, Presentation ePortfolios, Learning ePortfolios, Personal Development ePortfolios, Multiple Owner ePortfolios, and Working ePortfolios*".

[4] http://en.wikipedia.org/wiki/

- Assessment ePortfolios: for demonstrating achievements to "*an authority by relating evidence within the ePortfolio*", and often "*gain score against the initial requirements set by that authority*".

- Presentation ePortfolios: for "*evidence learning or achievement to an audience in a persuasive way*" and are "*often used to demonstrate professional qualifications*."

- Learning ePortfolios: to "*document, guide, and advance learning over time*", often to plan and reflect on learning, and "*diverse learning experiences. Learning ePortfolios are most often developed in formal curricular contexts*".

- Personal development ePortfolios: for personal development planning, could include a learning ePortfolio, "*but goes beyond that, as it is often related to professional development and employment*," and "*also possibly used as a presentation ePortfolio*." It contains "*records of learning, performance, and achievement which can be reflected on, and outcomes of that reflection, including plans for future development*".

- Multiple Owner ePortfolios allow "*more than one individual to participate*". They could be a combination of the portfolio types that mentioned above, but most likely take the form of a Presentation ePortfolio and a Learning ePortfolio. They are also used to "*represent the work and growth of an organization or organizational unit*".

- Working ePortfolios "*often include multiple views*", each view could be an ePortfolio of any type. It is "*the larger archive from which the contents of one or more ePortfolios may be selected. The whole of a working ePortfolio is generally accessible only to its subject, while views are made accessible to other individuals and groups*".

Lorenzo and Ittelson [89] summarized ePortfolios in a slightly differently. They catalogued ePortfolios in three types as: "*for students while studying, for graduates while moving into or through the workforce, and for institutions for program assessment or accreditation purposes*" [89].

- "*for students while studying: Students in college mainly use the ePortfolio for critical reflection and learning purposes*"
- "*for graduates while moving into or through the workforce: For showcasing their qualifications and competencies in job interviews, and promotion*"
- "*for institutions for program assessment or accreditation purposes: for institution-wide reflection, learning and improvement to demonstrate institutional accountability, to make accreditation processes more visible, and to show collective student progress*"

Even though ePortfolios represent a technical change in physical terms, the concept is maintained.

3.1.3 The ePortfolio Reference Models

The UK's Joint Information Systems Committee (JISC) funded projects for ePortfolio reference models. From those, Blowers [20] identified that the EP4LL and RIPPLL projects are theose most related to our interest of portfolio data exchange. They are summarized below.

EP4LL (ePortfolios for Lifelong Learning): The initial aim of the EP4LL project was to "*produce a reference model of an ePortfolio capable of providing and receiving services from other ePortfolios in other episodes of learning*" and "*facilitating admissions and transitions between study and employment at different levels*." It outlined a series of web services for the use case of a student applicant to university [124]. The services would allow an applicant to build an application from an institution template, whilst selecting evidence from their ePortfolio to support it, and to create a submission [124]. It also identified that current ePortfolio interoperability standards, such as IMS ePortfolio, can be a hindrance if too complex [124].

RIPPLL (Regional Interoperability Project on Progression for Lifelong Learning): The project "*established a model of cross-sector collaboration*" utilizing ePortfolios and is currently the closest to a reference implementation, due to its "*symbiotic relationship*" with the ePortfolio reference model [72]. RIPPLL utilized knowledge gained to develop "*practical tools to assist transitions of learning*" within a federation of institutions in the Nottingham area. This allowed ePortfolio data that was created during time at FE colleges to be included and transferred to other institutions [72]. Again to aid feasibility, interoperability was required and the RIPPLL tools are compliant with the UKLeaP XML schema, a UK localised version of the IMS Learner Information Profile (LIP) schema [72, 129]. RIPPLL also tackles 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 another institution's systems [72].

However, although these models define the use cases for the exchange of portfolio data, from an e-certification perspective they are limited, as there is no mechanism to authenticate the veracity of the portfolio data transmitted between institutions. Neither have explicitly described the security issues raised by transmitting data between multiple parties which are not always identifiable.

3.1.4 Benefits of ePortfolios

Based on Challis [27], Abrami and Barrett [1], Strudler and Wetzel [151], and Butler's [24] points of view on the usage of the ePortfolio, and comparing the differences between the ePortfolio and the traditional model, the main benefits made in the literature for ePortfolio are:

- *"efficient storage, easier searching, and simple retrieval, manipulation, refinement and reorganization of records";*
- *"reduced effort and time";*
- *"more comprehensive and rigorous";*
- *"cost-effective distribution";*
- *"instantly accessible, easy to carry and share with peers, supervisors, parents, employers and others";*
- *"allow an organizational structure that is not linear or hierarchical";*

- *“showcase the technological skills of the creator”;*
- *“potential larger audience, by providing access to a global readership if they are based on the web”*
- *“use more extensive material: pictures, sound, animation, graphic design and video”;*
- *“multimedia technology, general literacy, communication and problem solving skills development”;*
- *“personal accomplishment, psychological benefits”;*
- *“engage assessment”;*
- *“allows fast feedback, evidence and reflection of work and learning”;*
- *“privacy protected”;*

3.1.5 Criteria for Successful ePortfolio Adaptation

Ahn [7] believes that “*planning is a key element of success*”. Butler [24] thinks that “*motivation can be encouraged through enabling student decision-making, ensuring students have ownership of their portfolios, and public access to and recognition of students’ work over the web*”. While Klenowski et al. [84] think that “*a portfolio should be a reflective process, through which students construct meaning and understanding out of their learning*”. Strudler and Wetzel [151] have also pointed out that “*the purpose of the portfolio should be clearly connected to the curriculum and goals of the program they are studying*”, and that students should have adequate resources and sufficient access to technology to complete the portfolio. Yancey [175] compiled a series of success factors in the form of questions.

- *“What is/are the purpose/s?”*
- *“How familiar is the portfolio concept? Is the familiarity a plus or a minus?”*
- *“Who wants to create an electronic portfolio, and why?”*

- *“Who wants to read an electronic portfolio, and why?”*
- *“Why electronic? What about electronic is central to the model? And is sufficient infrastructure (resources, knowledge, and commitment) available for the electronic portfolio?”*
- *“What processes are entailed: what resources are presumed?”*
- *“What faculty development component does the model assume or include?”*
- *“What skills will students need to develop?”*
- *“What curricula enhancement does the model assume or include?”*
- *“How will the portfolio be introduced?”*
- *“How will the portfolio be reviewed?”*

3.1.6 Issues in ePortfolios

As ePortfolios would be the main platform where the eCertificate was to be presented, the issues that ePortfolio systems faced might also be expected to have an impact on eCertificate. Therefore, identifying and addressing these related issues in eCertificate design was the key for successful ePortfolio integration.

Many issues surrounding ePortfolios were found during this research; some of them, such as privacy protection, needed to be resolved and successfully implemented before they could be seen as benefits. The main issues identified in the literature were:

- students’ skills/abilities: the students’ technical skill level may affect the creation of their portfolio, “*the danger is that students will end in being assessed more on their technology prowess*” [1].
- Qualification data verification: providing verified access to qualification data was a main issue. Projects working on this area, such as the LIPID project, which “*investigated the use of a middleware solution to provide verified qualifications data from an MIS system (student record system) into a student’s ePortfolio*.” [67]

- work verification: it is "*very difficult to authenticate the evidence in ePortfolio – is it really the student's own work*" [1].

- Access rights and system authentication: the issue centred on the questions of who would have access to the ePortfolios, and how their identities could be authenticated. Studies on the Shibboleth-based authentication system to explored the potential solution.

- Interoperability and data transfer: middleware and standards needed to be developed to enable transfer of data between incompatible systems. Many projects have investigated this area, that "*worked on the standards involved in data transfer, and with JISC-CETIS are taking this work forward through the Portfolio SIG,*" such as IMS LIP, HR-XML, UKLeaP, LEAP 2.0, IMS ePortfolio. Projects like SHEEL have "*developed a technical middleware solution called ioNode which enable the transfer of student data in a LIP compliant way"* [67].

- Legal issues: there are legal issues invoked in ePortfolios, such as data protection, copyright, Intellectual Property Rights (IPR), ownership and stewardship. "*There were projects running for the last 2 years on exploring the legal issues surrounding the lifelong learner record and ePortfolios. The study has written a number of FAQs and reports around the legal issues and accessibility …and guidance have been produced.*" For example, the EPICS project produced a toolkit for projects, which "*helps to think through the main issues in planning, implementing and planning an ePortfolio project*" [67].

- Connection speed and data storage capacity were also mentioned as issues from institutions in the literature.

3.1.7 Barriers to Implementation

Grey [67] pointed out that it can be difficult to engage learners in planning and reflection, since students often need to feel the potential benefits for their investment. At the same time, a number of barriers to the implementation were summarized by Butler [24] from the issues raised in the literature [25, 151]:

- "*The need for adequate hardware and software";*
- *"The accessibility of that hardware and software";*
- *"Lack of technology skills amongst students and staff";*
- *"Technical problems with the equipment or electronic portfolio system";*
- *"The need for support when problems are encountered";*
- *"Maintenance of the hardware";*
- *"Adequate storage space and server reliability";*
- *"Demands on staff time";*
- *"How to use students' time efficiently";*
- *"How to overcome issues of ownership and intellectual property";*
- *"Problems with security and privacy of data";*
- *"Lack of features or of control over those features";*
- *"The need for access and permission controls";*
- *"How to transport electronic portfolios into new systems as students move on"; and*
- *"The need for common standards between different electronic portfolio systems.*"

3.1.8 Discussion

From the research results, there are six types of ePortfolios. One that most relates to the eCertificate is the presentation ePortfolio, 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.

After reviewing the ePortfolio research domain, it is apparent that concerns have been raised regarding the security aspects of the ePortfolio data transitional processes. The eP4LL (EPortfolios for Lifelong Learning) project developed a reference model for ePortfolios for the eFramework. The RIPPLL (Regional Interoperability Project on Progression for Lifelong Learning) has tackled the authentication issue between institutions it links to 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. However, although the eP4LL models define the use cases for the exchange of portfolio data, they did not address 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 ePortfolio data transmitted between institutions in RIPPLL. Rees Jones, an eP4LL project member, admitted "*Security and Trust: the* (ePortfolio) *Reference Model sidestepped this key issue*" [125]. Even though the issues of work authentication, qualification data verification, access rights and system authentication were mentioned in the literature, either there is little information since they are still under development, or these are simply referred to as 'future development'. One of the suggested methods in the literature was through referees and digital signing for their references [159], but this method is clearly not secure enough. Referees can only provide opinions on how they think you are as a person for the period that they know you; they cannot prove your qualifications and works, especially the ones that you obtained before they knew you.

ePortfolio would be the main platform where eCertificates are presented, therefore, besides adaptation that ensures the eCertificates could be recognised by various ePortfolio systems, verifiable qualification awards with secured supported evidence (involving various file types) would be the main requirement for eCertificates to be presented in ePortfolio systems.

Lots of the issues that the ePortfolio face, also apply to the eCertificate system, such as qualification data verification, access rights, system authentication, data interoperability and transfer, data protection, and copyright. Of all the barriers that the ePortfolio faces, users' lack of technology skills would be the main one to affect the eCertificate. If the eCertificate system required digital signing from end users (very likely), then the students need to have the knowledge of how to generate and use the key pairs. This is considered as a big task for most students as it possibly requires degree level computing skills. To overcome this, the eCertificate system might need to develop a sub-system to help with this.

3.2 Certification and Certificates

A certificate is the end product of a successful certification process. Therefore, it is necessary to understand the domain of certification in order to determine an appropriate structure for the eCertificate system.

3.2.1 Definition of Certification

Certification is defined as an "*independent third party confirmation that a product, system, service or installer meets, and continues to meet the appropriate standard*" [23]. It can be summarized into three catalogues:

- professional certification: "*a person is certified as being able to competently complete a job or task, usually by the passing of an examination*";
- product certification: "*processes intended to determine if a product meets minimum standards, similar to quality assurance*";
- cyber security certification: "*usually referred to as accreditation, and is also referred as eCertification*", such as "*organizational certification and digital signatures*"

Certification is used in all areas around us, such as accountancy, business, computer technology, economic development, as well as the health and education sectors. For example, in accountancy and finance, qualified accountants are the experts who have successfully passed their certification process, working in public practices, private corporations, the financial industry and government bodies [59].

3.2.2 Certification Processes

Anderson and Fuloria [10] have described the processes, the causes of failure, and the need for success for evaluating and certifying products and systems in the domain of information security. They claimed that certification is "*often used where a third party is expected to rely on the protection provided by the evaluated product*". Evaluation, "*means having a system closely examined by engineers at the National Computer Security Center*," as part of the product certification process, which can go wrong in nine ways, such as inadequate testing criteria, inappropriate protection profile, framework abuse, and target scope which is either too narrow or ambiguous. They stated that, for proper product certification, "*the vendor would have had to file the evaluation report with GCHQ, which would have published it*." However, the Common Criteria for Information Technology Security Evaluation that "*permit systems to be evaluated against a protection profile*," are not "*well matched to the needs of the control systems world*," and suggested that a certification scheme could do better by adding "*usability testing to its evaluation process*" and should "*take the whole product lifecycle into account*."

The attention of research on the certification process was drawn onto the catalogue of professional certification, since it is the one that directly relates to the eCertificate of qualification.

According to the examples of the certification process in the IT industry from Microsoft [100] and Novell [109], the process for achieving their professional certification consists of four steps.

- Search and choose a certification exam from the variety on offer;
- Choose a preferred study method to prepare for the exam. This can be either Instructor-led Training (attend classes for interactive training), Self-study Training (buy a kit; this is a self-study cost-effective training option, for people "*with busy schedules requiring flexibility*"), or Technical Skills Assessment (TSA) to "*evaluate your current level of knowledge*";

- Register for an exam and take the test in order to be certified. There may be an option for the test method, such as practical tests, which "*requires completing technical scenarios and applying knowledge in a real-world setting; standard tests, which consist of computer-based point-and-click, matching, fill-in-the-blank and multiple-choice questions*".
- Award the certificate when the test is passed successfully.

3.2.3 Benefits of Certification

Earning professional certification not only validates your expertise, but also "*demonstrates your skills and capabilities to current and future employers and peers*". Microsoft summarized the benefit as: "*validates your hands-on experience, shows off your skills and expertise; matches your current or desired job role with an existing or evolving technology; makes connections around the world*" [102]

3.2.4 Issues Related to Certification

In theory, a qualified person who has successfully passed the certification process should be better for the job than an unqualified person, but this is not always true. ISO 9000 certification is "*one of the most popular quality assurance systems in the world*". A quality/operations management study which tested "*the strength of the relationship between ISO 9000 certification and organizational performance in the presence and absence of a total quality management (TQM) environment*" [156] indicated that ISO 9000 certification "*is not shown to have a significantly positive effect on organizational performance in the presence or absence of a TQM environment. This supports the view that on average ISO 9000 certification has little or no explanatory power of organizational performance*".

Other drawbacks included the students' stress on their exam experience, the need to withdraw mis-issued certificates (e.g. plagiarism was found after the certificate has been issued), and the time limitation of some certificates (e.g. a 3 year First Aid Certificate). In the latter two cases, certificate revocation or recertification is required.

Shore and Scheiber [144] stated that "*as the certifying boards become established ... find it desirable to issue certificates that are valid for a stated period*".

3.2.5 Types of eCertificates

A certificate is commonly known as a confirmation and proof document that a person has passed a specific test or study. Certificates in different domains have different levels and also vary between countries. However, the term eCertificate could be referred to in many other domains besides qualification award certificates.

3.2.5.1 eCertificate as e-voucher and e-currency in online marketing

In online marketing, an e-voucher or e-currency is also called an eCertificate. It refers to an online gift card that is equivalent to the plastic gift card in the physical world. It is defined as: "*a powerful tool to help you combine the effectiveness of face-to-face sales with the broad based reach of the online marketing…single-use special offer certificate that you define and customize.*" [42]. It integrates traditional sales methods with the powerful online payment process. It can be used anywhere at any time, provided you have network access.

For example, the DigiProofs eCertificate [42], offers a system for professional photographers to provide their clients with the ability to view proofs online. With the use of the eCertificate process, photographers are able to pre-generate and distribute the eCertificate codes embedded in their order forms. Once customers send in payment with the order forms, the photographer activates the associated eCertificate codes online. Customers are then able to view and select the image(s) of their choice, and redeem the prepaid package.

By using an eCertificate approach with its online payment system, companies can increase viewing exposure, maximize orders, and bring in add-on sales while simplifying manual payment processes.

3.2.5.2 eCertificate as an e-card and printable certificate templates

Online printable certificate templates and e-cards that have certificates as their topic are also called eCertificates. There are plenty of free online applications that provide such services to help users create their own eCertificates, such as SmartDraw [145] and activ8 [3]. These systems provide a choice of certificate design templates, and take a name and a message as input (which varies according to the application), and then produces the required personal eCertificate. By using this type of software, a professional certificate can easily be achieved. However, there is no control on security, therefore anyone can create such eCertificates with their preferred qualifications.

3.2.5.3 eCertificate as Public key certificate in system authentication

In computer security and cryptography, eCertificates refer to digital certificates, also known as an identity certificates or a public key certificate. It is "*an attachment to an electronic message used for security purposes*". It is "*an electronic credit card that establishes credentials when doing business or other transactions on the Web*" [139]. FDA ESG describes public key certificate as *"an electronic document which conforms to the International Telecommunications Union's X.509 specification*" [54]. A public key certificate typically contains the following attributes [139]:

- *"The owner's public key"*
- *"The owner's name, which can refer to a person, a computer or an organization"*
- *"The expiration date of the public key"*
- *"The location (URL) of the issuer (the CA that issued the Digital Certificate)"*
- *"Serial number of the Digital Certificate"*
- *"The digital signature of the certificate, produced by the issuer's (the CA's) private key"*

VeriSign [165] introduced the concept of classes of public key certificate. The classes are differentiated by the level of confidence that can be placed in the certificate based on knowledge of the process used to verify the owner's identity.

- *"Class 1 for individuals, intended for email"*
- *"Class 2 for organizations, for which proof of identity is required"*
- *"Class 3 for servers and software signing, for which independent verification and checking of identity and authority is done by the issuing certificate authority"*
- *"Class 4 for online business transactions between companies"*
- *"Class 5 for private organizations or governmental security*"

The "*most common use of public key certificates is for HTTPS-based web sites*", which belong to class 3. With an eCertificate in place, a Web browser will validate whether an SSL based Web server is authentic, in other words, if it has been attacked or if "*the web site is who it claims to be*". This means that the user can "*feel secure that their interaction with the Web site has no eavesdroppers and that the web site is who it claims to be*".

Public key certificates can be structured. For a hierarchy of structured certificates that are used within a company, the only need is to trust the top level. However, the "Internet is a large federation of networks for inter-company, inter-organizational, and international communication," which is governed by its members, "a board called the Internet Society"; "there really is no "top" for the Internet". Therefore, there are many root CAs "largely structured around national boundaries" [117].

3.2.5.4 eCertificates as qualification award certificate is new in research

There was no information regarding eCertificates as qualification award certificates in the literature when this research started in 2007. This indicated that eCertificates was a new field in research. This was true not only across UK, but also worldwide.

- In 2009, after two years into this research with the eCertificate system design proposed and published, the UK government funded JISC called for a research project to investigate such an eCertificate system. As a result of successfully wining the bid, this research had been run as the eCert project since 2010 to develop a demo system to prove the proposed design from the technical level [28].
- Also in 2009, the Department of Education, Employment and Workplace Relations of the Australian government established the Australian Flexible Learning Framework, and set up the eWork project to "investigate existing learner information verification services and systems" to "identify the verification needs of third parties" [92] [93]

3.2.6 Fake Certificates

There are lots of fake certificates abound. The phase "create fake certificate" was entered in Google UK search in March 2008, and returned 240 000 results of fake certificate services and stories. The quality of the fake certificates varies. The "Easy Certificate Software"[5] provides "*Great-looking Certificates in minutes*"; the "Fake Certificate Factory"[6] offers "*Replacement University Certificate British designed professional style*"; while the "Diploma Centre"[7] stated that they could create authentic fake university diplomas, such that their fake diplomas would pass any quality check.

3.2.7 File Structure and Format of an eCertificate

The eCertificate file structure and format were the main investigation points in eCertificate system design as they affect the interoperability of such an eDocument within other systems.

While the main content of an eCertificate could be mirrored from the paper-based certificate, the digital signature scheme [128] also provided information that a digitally

[5] http://www.SmartDraw.com

[6] http://www.DiplomasandTranscripts.co.uk

[7] http://www.nd-center.com/

signed eDocument file would contain the digital signature and the public key certificate with the signed eDocument. Europass [53] provides an example of a transcript file that a qualification certificate could bind with. Further, many organisations require additional evidence to support online qualification claims, e.g. examples of work achieved. However, there is no correct answer or guideline found in the literature for what an eCertificate file should contain.

Simple Procedures Online for Cross-border Services project (SPOCS) [147] has proposed an eDocument structure, which answers the needs of the EU Directive 2006/123/EU. Its structure design consists three layers: 1. the payload layer, to handle the eDocument which comes with various file formats and the official signatures; 2. the metadata layer, to provide a minimum set of semantic information about the document; 3. The optional common authentication layer, to handle the authentication and additional signatures. It has also introduced a new concept: the Omnifarious Container for eDocuments (OCD), which is "*an extension of the Virtual Company Dossier concept that has been introduced by the European Public Procurement on Live Project (PEPPOL)*" [115]. The container "*is a physical object, e.g. a PDF or ZIP*," and "*holds the capability to carry inside any electronic documents*." The idea of the OCD was interesting and could be applied to the eCertificate study, as the eCertificate would be composed of various files, in different formats, with multiple purposes

3.2.8 Discussion

From the research results, the certification process for an academic achievement involves the processes of registration and examination, and can be paper-based, computerized, or practical. A certificate is considered as a result of a successful certification process, whether this process is computerized or not. Therefore, an eCertificate should also be a result of a successful certification process, whether this process is carried out through eCertification or not. In other words, eCertificates should be a digital form of certificate that certify facts in exactly the same way as a paper-based certificate does; it is not for eCertification only!

The drawbacks of this certification study highlight that the certificates sometimes come with time limitations, such that "*re-certification is required*" [144], together with the fact that there are many fake certificates around, and mis-issued certificates exist widely (e.g. as in the case of widespread plagiarism). System support for validation and revocation is therefore mandatory.

The search for eCertificates in the literature has retrieved considerable material about public key certification, which is related, but has different concepts. A public key certificate binds a public key to an identity. When used as an attachment to a digital signature, a valid public key certificate can verify that the key used to sign an electronic document or message belongs to the specified individual or organisation. However, the eCertificate that is referred to in this research is a digital form of the traditional paper-based certificate, especially those related to educational achievements, and can be used within eLearning and ePortfolios. It is a “paperless reward certificate,” a kind of digital qualification certification. It is the electronic qualification information that is associated with individuals – the electronic document itself. It is not a digital signature or any other kinds of authentication alone. According to this idea, an eCertificate can involve public key certificate in its signing process. These two terms are analyzed and compared in Table 3-1.

Table 3-1 eCertificate VS public key certificate, published in [30]

	public key certificate	**eCertificate**
Issued by	• a CA	• an exam board
Purpose	• Verify whether who you are and what you have are true	• State who has achieved what
Usage	• Usually used within a selected environment or group of organizations	• Can be used anywhere in the world
Verification of who you are	• Identify the person from outside the system	• The person is an "insider", the institution should have had the identification when he/she enrolled for a course.
Verification of what you have	• Verify materials that are from anywhere outside the system • materials are usually paper based • user needs to provide all the materials for proof	• Exam results are in the exam board's own database system • No proof is required from the student for the achievement.
Trust	• Anyone can be a CA, need to trace and find a CA that you trust, this may invoke many level of CAs	• A CA may be invoked to provide an eCertificate of authentication for an eCertificate of qualification. The CA is for exam boards, aim to certify that they are official, recognized organizations, ideally the "Ministry of Education"

In order to issue an eCertificate, the system will need to have access to the personal data as well as the qualification record, to identify the person who it is being issued to, and to verify that they have passed the relevant exams. These data and records are all required in digital form. This is unlike the certification process, where data and records do not have to be computerized. Therefore, this will be the barrier for the use of eCertificates for some certification organizations, if they don't have a computerized system for their records. Even though this is unlikely to be the case, it cannot be assumed.

The idea of the OCD could be applied to the eCertificate design to manage the various files, different formats and multiple purposes that an eCertificate file may involve. However, it does not seem to address the security issue that appears in the eCertificate case, but this can be investigated further in the design stage.

3.3 Security

Security control will be a key factor of a successful system. The purpose of this section is to find out what areas of an eCertificate system need to be secured.

3.3.1 Definition of Security

Security is defined as the "*condition of being protected against danger or loss. In the general, it is a concept similar to safety*" with "*an added emphasis on being protected from dangers that originate from outside*", that "*something not only is secure but that it has been secured*". Security can mean traditional physical security, IT security, or the combination of the both. There are a wide range of issues involved in IT security alone. Federal Standard 1037C defines security as "*1. A condition that results from the establishment and maintenance of protective measures that ensures a state of inviolability from hostile acts or influences. 2. With respect to classified matter, the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security. 3. Measures taken by a military unit, an activity or installation to protect itself against all acts designed to, or which may, impair its effectiveness.*" [55].

3.3.2 The Goals of Computer Security

To build a secure computing system, we also need to find the right balance among the three goals: confidentiality, integrity and availability (also known as the CIA Triad).

Confidentiality is also called secrecy or privacy. It ensures that "*computer-related assets are accessed only by authorized parties*". Integrity means that "*assets can be modified*" only when they are under authorized control of "*who or what can access which resources and in what ways*". Availability means that "*assets can be accessed to those authorized at appropriate times*". It applies to both data and services [117].

Their relationships can be summarized as: protection of confidentiality can restrict availability and affect integrity. Enhanced integrity will reduce confidentiality and availability. Wide availability will put integrity and confidentiality at risk.

3.3.3 Types of Security

In order to further understand how security controls apply to data, programs, the systems, the communications links, the devices, the environment, and the personnel, the following topics were reviewed: data security, database security, information security, computing security, program/application security, network security, and human controls in security.

- Data Security:
  - It ensures that data "*is kept safe from corruption and that access to it is suitably controlled. Thus data security helps to ensure privacy. It also helps in protecting personal data*".
  - The ways that we secure our data is changing. Ablisser et al. describe that "*in the old days, data security and privacy were easily provided by storage in a locked box or file cabinet. Conversion of such records into digital data in databases on local and wide area networks markedly increases the provider's exposure to liabilities*" [9].

- Data security is also there to ensure individuals are treated fairly. In the UK, the Data Protection Act [162] "*is used to ensure that personal data is accessible to those whom it concerns, and provides redress to individuals if there are inaccuracies. It states that only individuals and companies with legitimate and lawful reasons can process personal information and cannot be shared*".

- The International Standard ISO/IEC 17799 covers data security [120], "*is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices ... One of its cardinal principles is that all stored information/data, should be owned so that it is clear whose responsibility it is to protect and control access to that data*".

- Encryption is one of the effective ways to secure data. The most common cryptosystems are DES, AES, and RSA. The applications of cryptography include hash functions, key exchange protocols, digital signatures, and certificates [117].

- Database Security:

  - Protecting data is the heart of many secure systems. In many cases, this relies on the database management system (DBMS). The requirements of database control include "*physical database integrity, logical database integrity, element integrity, audit ability, access control, user authentication, and availability*" [117].

  - Databases may contain sensitive data, and these sensitive data may also be subject to different levels of degree which could challenge access control.

  - There are five main approaches for ensuring confidentiality in multilevel secure databases: integrity lock, trusted front end, commutative filters, distributed databases, and restricted views.

- Information Security:

- Information security is defined as "*protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction*" [57]. The three components: confidentiality, integrity and availability are "*the core principles of information security*". Information Systems can be categorized into three sections: hardware, software and communications, and three levels or layers: physical, personal and organizational.

- Many organizations including governments, military, and business companies, collect confidential information about their employees, customers, and products, which is then "*processed and stored on computers, and transmitted across networks*". While the information satisfies the organizations' needs, the organizations become exposed to information leaks, unauthorised access and abuse of their data. Protecting confidential information is now a legal requirement in many domains. In some cases, "*information security has a significant effect on privacy, which is also viewed very differently in different cultures*".

- In principle, information security includes system authentication; non-repudiation; risk management; administrative, logical and physical controls; information classification; access control, and cryptography.

- Program/application security:

  - Application security is "*the use of software, hardware, and procedural methods to protect applications from external threats. Security measures built into applications and a sound application security routine minimize the likelihood that hackers will be able to manipulate applications and access, steal, modify, or delete sensitive data*" [155].

  - Yoder and Barcalow claimed that "*the goal of application security is to keep unwanted perpetrators from gaining access to application areas where they can find confidential information or can corrupt data. … making an application secure is much harder than just adding a password protected login screen*". [177]

- Computer security:
  - Pfleeger [117] has catalogued the security flaws in computing development into two general classes: one is compromise or change data, and the other one is affect computer service. Pfleeger has also stated three controls on these activities: "*development controls, operating system controls, and administrative controls*". The "*development controls limit software development activities*"; the operation system provides controls to limit "*access to computing system objects*", while the "*administrative controls limit the kinds of actions people can take*".
- Network security:
  - Network security consists of an "*underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access and the effectiveness (or lack) of these measures combined together*".[94]
  - Network assets include the network infrastructure, applications programs, and data. The strongest network controls are solid authentication, access control, and encryption. There are three controls that are specific to networks: firewalls, intrusion detection system, and secure e-mail. Wesinger claimed that firewalls "*provide enhanced network security and user transparency*" [170]. Network security can be assessed: e.g. Gleichauf has proposed a method and system for "*adaptive network security using a network vulnerability assessment*" [64]; Boyle has proposed an "*apparatus and method for providing multi-level security for communication among computers and terminals on a network*" [22]; and Hershey has proposed a system and method "*using a parallel finite state machine adaptive active monitor and responder*" [75]
- Human controls in security
  - Most of the computer-based security breaches are "*caused by either human or environmental factors*". This can be "*the administration of security*" (e.g. the security planning and risk analysis), the economics of cyber security

(e.g. the cost and benefit analysis of spending in security), the ownership and usage of the collected data, and the law and ethics that control malicious behaviour.[127]

3.3.4 Security Components and Assurance

Security has three components: requirements, policy, and mechanisms. "*Requirements define security goals. Policy defines the meaning of security. Mechanisms enforce policy". "These components exist in all manifestations of security"* [18].

Lee [86] referred to the security policy as "*a statement of intent about the required control over access to data*". He has also summarized it into three types that are "*generally used in secure computer systems*": confidentiality policy, integrity policy, and availability policy.

Security assurance is used for "*measuring how well requirements conform to needs, policy conforms to requirements, and mechanisms implement the policy*".[83]

3.3.5 Security Problem

To build a secure computing system, we need to find out what threats it faces, what vulnerabilities it has, and what controls it needs.

Pfleeger [117] defines a threat to a computing system as "*a set of circumstances that has the potential to cause loss or harm*"; a vulnerability as "*a weakness in the security system*"; and control as "*an action, device, procedure, or technique that removes or reduces a vulnerability, and used as a protective measure*". The relationships of these three terms are described in his book Security in Computing as: "*A threat is blocked by control of vulnerability*". Pfleeger [117] also catalogued the threats to a computing system in four main attacks: interruption, interception, modification, and fabrication; he stated that the vulnerabilities resources/components of a computing system that "*subject to attacks are hardware, software, and data*"; and he pointed out that controls can be applied to "*data, programs, the systems, the physical devices, the communications links, the environment, and the personnel*".

3.3.6 Issues in Security Implementation

Acquisti and Grossklags have well described our system users that "*consumers often lack enough information to make privacy-sensitive decisions and, even with sufficient information, are likely to trade off long-term privacy for short-term benefits*"[2]. Martinovic and Ralevich agree with the view, and said that "*individuals are often willing to trade privacy for convenience or bargain the release of personal information in exchange for relatively small rewards and are reluctant to adopt privacy technologies*" [96]. Adams and Sasse commented on password security [6] that "*because security mechanisms are designed, implemented, and breached by people, human factors should be considered in their design*".

Martinovic and Ralevich pointed out that "*one way of protecting privacy is reduction of stored sensitive information to the necessary minimum and raising awareness of threat of identity theft*"; and security "*has to be built-in instead of being added-on*", so that the system can avoid user flaws and "*does not require from users to gain knowledge and understanding of what needs to be done in order to further protect their privacy, prevent unauthorised access, or maintain data confidentiality*" [96].

3.3.7 Discussion

One of the purposes of this section is to find out what kinds of securities will be required by eCertificates, but there is no clear answer. The catalogue of security topics is very big and very confused: many of them overlap, and are catalogued in different places at the same time. Different people have different views of grouping them. Terms such as data security and information security are "*frequently used interchangeably; they are interrelated and share the common goals of protecting the confidentiality, integrity and availability of information*" [153]. Their differences "*lie primarily in the approach to the subject, the methodologies used, and the areas of concentration*" [85].

To secure a computer-based system, there is a 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. There is also a need to determine the right balance between the three goals: confidentiality, integrity and availability. In the case of eCertificates, there is a need to consider all these areas in our design, and find the right balance among the goals, to minimise stored data, and to build-in system security support functions so that the system is user friendly while maintaining a high level of security.

From the understanding of security at this research stage, the eCertificate system involved data security, database security, information security, program security, network security, and human controls in security.

Any issues in computing security, such as hardware, operating systems, and firewalls, were considered as not directly related to an eCertificate system, and therefore were ignored in further research of the eCertificate framework.

The literature review has just scratched the surface of security, in order to have an overview of the security design for the eCertificate system. The technical part of security methods research was carried out alongside the project.

3.4 Encryption and the Digital Signature Application

Encryption is a technique to address the block, intercept, modify, and fabricate attacks during a message transmission. Pfleeger described it as "*probably the most fundamental building block of secure computing, it is a means of maintaining secure data in a secure environment*" [117].

Since encryption is the method for security, eDocument related encryption applications were investigated for the purpose of eCertificate security, such as water marking and digital signature.

Water marking is one of the methods used in protecting digital data from unauthorized copying. "*By embedding a cryptographic string, or water mark, a legitimate author can demonstrate the origin of the file*" [117]. However, although water marking can protect unauthorized copying and indicate who the issuer is, for use in our eCertificate case, it could not prove that the issuer was an authorized educational body.

Digital signature, on the other hand, turned out to be the most suitable for an eCertificate system as it can not only detect unauthorized modification, but also addresses the trust issues by providing the chain of authorities.

3.4.1 Definition of Encryption

Pfleeger and Pfleeger defined encryption as "*the process of encoding a message so that its meaning is not obvious*", while decryption is "*the reverse process, transforming an encrypted message back into its normal, original form*" [117].

Encryption can be symmetric (encryption and decryption keys are the same) or asymmetric (encryption and decryption keys come in pairs, so that a message encrypted with the encryption key can only be decrypted by the corresponding decryption key). Both of the encryption systems provide authentication, proof that a message received was sent by the declared sender while the keys have not been compromised.

3.4.2 Symmetric Cryptosystems

The most widely used symmetric (Private Key) cryptosystems today are Data Encryption Standard (DES) and Advanced Encryption Standard (AES).

3.4.2.1 Data Encryption Standard

DES is an encryption algorithm, published as a National Bureau of Standards in 1977. Pfleeger and Pfleeger describe it as a "*careful and complex combination of two fundamental building blocks of encryption: substitution and transposition*" [117]

DES uses a 56-bit key size, which, according to Johnson [81], was a compromise result between 64 and 48 bits by the National Security Agency (NSA) and International Business Machines Corporation (IBM). Stallings [149] claimed that the reason for reducing the key size was to fit on a single chip. However, rapidly increasing availability of computational power, which made many attacks, such as the brute force, a possibility, the 56-bit key size was considered as too small and insecure for many applications. A classic example is a DES key that was broken in 22 hours and 15 minutes, which was a result of a public collaboration by distributed.net and the Electronic Frontier Foundation in January 1999.

Double DES and Triple DES was also developed to enhance the security of DES. Triple DES has been approved by NIST for sensitive government information up to the end of 2030 [104, 107], and according to Microsoft TechNet product documentation [101, 107], “Microsoft Outlook 2007, Microsoft OneNote, and Microsoft System Center Configuration Manager 2012 are using Triple DES for password control”. However, as there are some analytical results that show the “theoretical weaknesses in the cipher”, DES has been superseded, and the Advance Encryption Standard (AES) has been developed to adjust the security needs.

3.4.2.2 Advanced Encryption Standard

As announced by NIST, the AES was established in 2001, originally called Rijndael [106]. Westlund stated in a NIST report that AES was going to supersede DES in 2002 [172]. According to Schneier et al., AES is based on “the design principle of substitution-permutation network”, and is considered as “fast in both software and hardware” [138]. AES is a “variant of the original Rijndael, which has a restricted block size of 128 bits”, and is described in Kelsey et al.’s paper as having “10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys” [56]. After a 5-year long standardization and evaluation process, the U.S. government announced in June 2003 that the “AES could be used to protect top secret information” [74].

The first successful attack against the full AES was published in 2011, named Key-recovery attacks [16, 21]. Before this, there had been many other attacks targeted at the AES, such as the XSL attack [137], the related-key attack [17], and known-key distinguishing attack [62]. However, they are either theory only or just work for specific key lengths but not the full AES.

There are other types of attack also affecting the security of the system that the AES employed, such as the cache-timing attack announced by Bernstein in 2005 [15] and the “near real time” secret key recovery published by Bangerter et al. in 2010. These “side-channel attacks” do not target the “underlying cipher” but the implementation of the cipher on system, which leads to the data leak [13].

3.4.3 Asymmetric Cryptosystems

Asymmetric Cryptosystems, also called Public Key Cryptosystems, are the most common. The most widely used asymmetric cryptosystems today are RSA and DSA.

3.4.3.1 Rivest-Shamir- Adelman Algorithm

RSA is named for its inventors Rivest, Shamir, and Adelman in 1978. The RSA algorithm is “*similar to the Merkle-Hellman method, … finding terms that add to a particular sum or multiple to a particular product*”; it is based on the “*underlying problem of factoring large numbers*” [117].

Pfleeger and Pfleeger’s described it in [117] the RSA algorithm uses two keys: the encryption key *e* and the decryption key *d*. The key generation starts from a selection of two prime numbers *p* and *q*, which should be quite large, “*typically, p and q are nearly 100 digits each*”; *n* is a product of *p* and *q*, in this case, it could be around 200 digits long, which is about 512 bits; “*depending on the application, 768, 1024, or more bits may be more appropriate.*”; A relatively large integer *e* is next to be chosen, such that “*e is relatively prime to (p-1)*(q-1)*”, and then *d* is selected as “$e*d = 1 \bmod (p-1)*(q-1)$”; “*A plaintext message P is encrypted to ciphertext C by* $C = P^e \bmod n$*; the plaintext is recovered by* $P = C^d \bmod n$”, where “$P = C^d \bmod n = (P^d)^e \bmod n = (P^e)^d \bmod n$”.

Ireland has pointed out that one of the weaknesses of RSA is when the same key is used for encryption and signing: “Given that the underlying mathematics is the same for encryption and signing, only in reverse, if an attacker can convince a key holder to sign an unformatted encrypted message using the same key then she gets the original” [80].

The inventors, Rivest, Shamir, and Adelman, explained that the operation of the RSA starts from creating and publishing the public key while keeping the private key secret. They claimed that "*anyone who has the public key can encrypt a message, but if the public key is large enough, only someone with the private key can feasibly decode the message"* [128].

There are attacks against plain RSA, such as the chosen plaintext attack and the chosen-ciphertext attack. Ciphertexts can be easily decrypted if the "low encryption exponents (e.g., $e = 3$) and small values of the *m*, (i.e. $m < n^{1/e}$)" were chosen [39, 73].

While the underlying RSA computations are always the same, some advanced schemes have been developed with variants on how they can be used inside an encryption. One such is the Padding scheme, which has been designed to increase the security by "embedding some form of structure into the value *m* before encrypting". The PKCS#1 is the standard "designed to securely pad messages prior to RSA encryption [82].

3.4.3.2 EI Gamal and Digital Signature Algorithms

Besides the well known RSA, EI Gamal devised another public key algorithm in 1984. This algorithm *"is not widely used directly, but it is of considerable importance in the U.S. Digital Signature Standard (DSS) of the NIST*" [117].

Pfleeger and Pfleeger described this: The EI Gamal algorithm [47] key generation starts from a selection of a prime number *p* and two integers, *a* and *x,* such that "*$a < p$ and calculate $y = a^x \bmod p$*"; also the prime *p* "*should be chosen so that (p - 1) has a large prime factor q*". When signing a message *m,* a random integer k will be chosen, where the k need to be not been used before, satisfying $0 < k < p – 1$, and is relatively prime to $(p - 1)$. The message signature (*r* and *s*) is then computed through $r = a^k \bmod p$ and $s = k^{-1} (m - xr) \bmod (p - 1)$, where "*$k^{-1}$ is the multiplicative inverse of k mod (p - 1), so that $k * k^{-1} = 1 \bmod (p - 1)$*". When verifying a message, the public key *y* will be used to "*compute $y^r r^s \bmod p$ and determine that it is equivalent to $a^m \bmod p$*" [117].

The Digital Signature Algorithm (DSA) is also referred to as the Digital Signature Standard (DSS). It was proposed by the NIST in August 1991, specified in FIPS 186 [45], with the latest version of FIPS 186-3 in 2009 [46]. DSA is "*the EI Gamal Algorithm with a few restrictions*", such as [117]

- "*The size of p is specificallyfixed at 2^{512} <p < 2^{512}"* which makes the p at about 170 decimal digits long;
- "*q, the large prime factor of (p – 1) is chosen so that 2159 < q < 2160*";
- Use of a hash value, *H(m)*, instead of the full message text *m*
- "*the computations of r and s are taken mod q*"

Pomin and Stern [118] clearly state that RSA and DSA are "*two completely different algorithms, RSA keys can go up to 4096 bits, where DSA has to be exactly 1024 bits*".

DSA is "faster for signature generation but slower for validation", but when used for encryption, DSA is "slower when encrypting but faster when decrypting". Security of DSA and RSA are considered equivalent when compared with equal key length. According to Schneier [136], "*both DSA and RSA with the same length keys are just about identical in difficulty to crack.*"

3.4.4 Symmetric vs Asymmetric

Although the symmetric encryption can provide a "*two-way channel*" between two users with only one shared secret key, there are three main issues found in the literature of employing a symmetric key system, which are in the areas of key compromise, distribution, and management. Pfleeger and Pfleeger summarised them in their book [117] as:

- Once a key is compromised, all the encrypted information under them can be revealed. To avoid this, keys need to be changed frequently so that "a compromised key will reveal only a limited amount of information"

- Key distribution is a problem, and it requires handling by hand or using methods such as 2-piece key distribution.

- Key management is the biggest problem: "*the number of keys needed increases at a rate proportional to the square of the number of users*", in which "*n users who want to communicate in pairs need n*(n-1)/2 keys*". It is most suitable for a small group of people exchanging secret information directly; methods such as “*clearing house*” or “*forwarding office*” would be required when a wide network exchanging is involved.

On the other hand, the asymmetric system which uses a public key and a private key, only requires one key pair per user. However, to perform a public key encryption can take 10,000 times longer than a symmetric encryption because “*the underlying modular exponentiation depends on multiplication and division, ... is reserved for specialised, infrequent uses, where slow operation is not a continuing problem*” [117]These two systems are compared in Table 3-2.

Table 3-2 Comparing Secret Key and Public Key Encryption, reprint from [117]

	Secret Key (Symmetric)	**Public Key (Asymmetric)**
Number of keys	1	2
Protection of key	Must be kept secret	One key must be kept secret; the other can be freely exposed
Best uses	Cryptographic workhorse; secrecy and integrity of data – single characters to blocks of data, messages, files	Key exchange, authentication
Key distribution	Must be out-of-band	Public key can be used to distribute other keys
Speed	Fast	Slow; typically, 10,000 times slower than secret key

3.4.5 Definition of Digital Signature

Pfleeger and Pfleeger described digital signature as “*a protocol that produces the same effect as a real signature: it is a mark that only the sender can make, but other people can easily recognize as belonging to the sender*”; they defined it as “*a mathematical scheme for demonstrating the authenticity of a digital message or document*”; “*it is a sequence of bits applied with public key cryptography, so that many* *people using a public key can verify the authenticity of bits, but only one person using the corresponding private key could have created them*” [117]

3.4.6 The Trust in Digital Signature

The word “trust” has been used in security. Pfleeger and Pfleeger stated [117] that “*security professionals prefer to speak of trusted instead of secure operating system*”. They also pointed out that “*trust is perceived by the system's receiver or user, not by its developer, designer, or manufacturers*”, and “*there can be degrees of trust*”. They describe a trusted system as “*a system that employs sufficient hardware and software integrity measures to allow its use for processing sensitive information*”.

For a successful online communication or transmission, the parties involved need to “*establish trust without having met*” through a “*common respected individual*” [117]. To increase security and establish the trust, digital signature makes use of Hashing and Public Key Infrastructure (PKI).

3.4.7 Hash in Digital Signature

Hashing is one of the encryption applications. The most widely used hash functions include MD4, MD5, and SHA/SHS. In cryptography, a hash is also called “checksum or message digest”. It is a one-way function for which the encryption is easy to compute, but the inverse decryption is much more difficult.

A one-way hash function can be used to “seal” a file, so that “*any change to even a single bit will alter the checksum result*”. This is “*similar to the use of wax seals on leathers in medieval days*” [117]. When a hash is used in the digital signing process, a message is not signed directly, but rather first hashed to produce a constant size digest, and then the digest is signed instead of the message. When the checksum value is stored with the file, and if the computed checksum value matches the stored value on access, it is “*likely that the file has not been changed*” [117]. This hash-then-sign method increases system security, and can guard against attacks such as the chosen-message attack [91].

3.4.8 Public Key Infrastructure

Toorani defined public-key infrastructure (PKI) as "*a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates*" [158]. Pfleeger and Pfleeger defined PKI as "*a process created to enable users to implement public key cryptography, usually in a large setting*". He also noted that PKI offers users a set of identification and access control services, including: creating certificates associating user's identity and the public key; signing certificates; confirm/deny if a certificate is valid; invalidate certificates if withdrawn or if signing key has been exposed [117]

PKI consists of the following main components [8, 99, 158, 164, 176]:

- Registration Authority (RA): an agency who verifies public keys and the identities of their holders before binding, ensuring the keys meet the international standard
- Certification Authority (CA): binds public key to the identities of their holders, responsible for issuing and revoking of Public key certificates
- Validation Authority (VA): an agency that provides information on behalf of the CA
- Public key certificate: a document that is signed by a certificate authority (CA), certifying the accuracy of the binding of a public key and its owner's identity (also reviewed in the Certificate section)
- Certificate Repository (CR): stores Public key certificates and Certification Revocation Lists (CRLs)
- Central Directory: a secure location for store and index keys

The principle of PKI outlined in literature [158, 160, 164, 166] is:

1. A user applies for a certificate with his public key at RA;
2. RA verifies and confirms the user's identity to the CA;
3. CA signs the public key certificate with CA's private key and issues the certificate to the user;
4. CA also sends information about issued certificates to VA;

5. The user can now sign eDocuments with his private key and attach the Public Key Certificate to the eDocument;
6. The integrity of the eDocument can then be verified on access and the user's identity can be checked by the VA on behalf of the CA.

PKI provides a hierarchy trust structure [117]: through PKI, a chain of CAs can be traced to find a trusted note from the signer's public key certificate, such that not only can the signer be tracked down, but also the CA, and the CA's CAs, all the way to the root CA. Yeun [176] comments on PKI in his paper as "*trusted services that enables the secure transfer of information and supports a wide variety of E-Commerce applications*". He also pointed out that a properly implemented PKI can provide "*Confidentiality: communications between two parties remain secret; Integrity: no unauthorized modification of information between two parties; Authentication: the process of reliably determining the identity of a communication party; and Non-repudiation: impossible for communicating parties to falsely deny*." [176]

3.4.9 Digital Signature Theory

The core of the PKI is the digital signature, which employs asymmetric cryptography and "consists of three algorithms: key generation algorithm, signing algorithm, and signature verifying algorithm". Rivest, Shamir, and Adelman, the RSA inventors, describe the signing algorithm of a digital signature as "*A message is encrypted by representing it as a number M, raising M to a publicly specified power e, and then taking the remainder when the result is divided by the publicly specified product, n, of two large secret prime numbers p and q*" and the verification algorithm as "*secret power d is used, where e d ≡1 (mod (p - 1) _ (q - 1))*." They also stated that "*the security of the system rests in part on the difficulty of factoring the published divisor, n*" [128].

Pfleeger and Pfleeger pointed out that a digital signature must meet two primary conditions: "*unforgettable*" and "*authentic*," such that only person P can sign message M, and produce a signature of S(P,M). It is "*impossible for anyone else to produce the (M, S(P,M)),*" and such a signature can be checked on receive [117]. They also mentioned that a digital signature has two properties: "*not alterable*" and "*not* *reusable*", such that the message M will not be reused or modified without notice on receive [117]. A valid digital signature provides authentication, integrity, and non-repudiation, such that it gives the receiver reason to believe that the message was sent by the signer, it has not been modified without authorization, and at the same time, the signer can not deny he/she signed the message.

In practice, an eDocument will first be hashed; the hashed value (message digest) will then be encrypted using the signing algorithm with the issuer's private key; the result of the encrypted hash is the new called the digital signature of the message, which can be attached in the eDocument along with the Public key certificate before distribution. On receipt, the eDocument will first be hashed again; and the digital signature (the encrypted hash) will be decrypted using the verification algorithm with the user's public key; if these two hash values matched, then the received message is considered as valid, it has not been modified since it is signed and it is from the claimed public key's owner.

Another verification process is checking the revocation status/validity of the public key certificate. This can be done by checking the CA's certificate revocation list (CRL). X509 is a standard for a PKI, specifies the standard formats for public key certificates and CRL.

3.4.10 Security Issues in Digital Signature

Security assurance of digital signature has been published in the literature [82, 91, 117], that includes these characteristics.

1. Quality algorithms: Some simple public-key algorithms with small chosen prime numbers are known to be insecure, and are easily attacked
2. Quality implementations: a good algorithm with no implementation mistakes form the base of the security design
3. Secret private key: The private key must remain private at all times
4. Ensure trust: The public key certificate must be verifiable and the CAs can be traced
5. Correct procedure: Users must carry out the process properly.

Many attacks target the digital signature, such as key-only existential forgery attack [95] and chosen-message attack [91]. Goldwasser, Micali, and Rivest studied some of these attacks and published the attack results in the SIAM Journal on Computing [65].

The review of digital signature has been focused on the security holes that may have a special impact on eCertificates. As a result, two main issues raised in the literature have been identified; however, one of the main eCertificate security concerns: the content status validation of a digitally signed eDocument, has not been mentioned in literature. These three issues are detailed below.

3.4.10.1 Issue 1 - public key certificate status validation

Certificate Revocation List (CRL) is a list of the issued public key certificates that need to be revoked. The reasons for the revocation can vary, but according to the revocation reason code specified in RFC 5280 [105], it is categorized as: "*unspecified; keyCompromise; cACompromise; affiliationChanged; superseded; cessationOfOperation; certificateHold; removeFromCRL; privilegeWithdrawn; and aACompromise*."

When accessing a digitally signed eDocument, the system will automatically verify the integrity of the document by comparing the eDocument's hash value against the decrypted signature hash value. The reviewer will be informed if the signature is invalid (the two hash values do not match) [82, 91]. However, not all systems will automatically check the status of the signature's signing key (the public key certificate) against the CRL. Some of them require the reviewer to manually open up the public key certificate to check the status when concerned, while some of them require the receiver to configure the system to enable the function.

In practice, a message may be displayed with a valid signature: "This document and all items contained in the document file are signed. All signatures are valid. Click here to view the signer's identity." Pronichkin commented that "*CRL checking takes place on a per application basis, ... Some applications make verification failures visible to the user while other applications stay silent and suppress such messages*"

[119]. This is a known security hole; it can lead to documents signed by a revoked key being accepted, if this part of the verification process has been skipped.

3.4.10.2 Issue 2 – eDocument content validation

The simplest form of signing is called Comprehensive Signing, where one or multiple signatures is used to sign all the content in a single document with no reference to external content. In addition, the eDocument contents have also been categorized into four additional groups according to their different signing situations. These four groups are: Unsigned content, Signed content groups, Externally referenced content, and Dynamic content [41]. Signing for contents that fall into any of these four categories will invalidate the trust and should be avoided. "*From a signature-trust standpoint, content that can be dynamically added, removed or altered is by its very nature unsignable*." When the situation is unavoidable, clear notifications should be provided [41].

- For a document with pages/parts left unsigned or added later as unsigned parts, a verification result message should be displayed clearly to inform users of the unsigned but associated content.
- For a document with different signed content groups, a verification result message should be displayed clearly to inform users that signatures that relate to different content groups are independent.
- For a document with externally referenced content, a verification result message should be displayed clearly to enable the user to understand the situations and identify the unsigned external materials.
- For a document with dynamic content, such as inserted variable texts or results of running macros, a verification result message should be displayed clearly and accurately to enable the user to understand the situations and identify the unsigned dynamic materials.

Signing contents can also present in various content types, such as text documents, media files, and programme code. To accompany the various content types and signing categories, a digital signature with XML syntax has been defined, which can be used for signing data resources of any type and is most suitable for signing

XML documents [103, 167]. Three signing methods have been defined: detached signature can be used for signing externally referenced resources; enveloped signature can be used for signing part of the document; enveloping signature can be used to sign a whole document and wrap the signed content within itself. This XML signature has the advantage over other forms of digital signatures, such as Pretty Good Privacy (PGP) [180] as it operates on XML Info set rather than binary data. This allows various ways of binding the signature and the signed content [103, 141].

However, although the XML signature provides helpful signing methods, it still does not solve the security issue when unsigned content is involved. This needs to be addressed when designing the eCertificate system.

3.4.10.3 Issue 3 – eDocument status validation

After a long search in the literature, information was found about revoking a digitally signed eDocument and was all about the signing key being compromised. No information was found about revoking a signed document due to a changed situation so that the signed content is no longer true. This is similar to the unsignable dynamic content that also involves some changes after signing, but the difference in this is the document can just be a simple static file and perfectly signable. Taking the eCertificate as an example, it could be a simple text file when it is signed, but what happens if fake evidence, or copied work, or cheating, has been found after the certificate has been miss-issued?, How can the eCertificate be revoked due to this changed situation but where the key has not been compromised? For the eCertificate, the public key certificate must be checked against the certificate revocation list (CRL) and also whether the content of the eCertificate, the qualification award certificate, has been withdrawn. Thus the issues faced are of having two types of certificates to be verified: one well-documented and supported, and the other with no information at all. It might be called the (eCertificate)^2 issue!

3.4.11 Discussion

Encryption, as the security method, has been reviewed. Both Symmetric and Asymmetric encryption methods have their pros and cons. A combination of the asymmetric encryption application (digital signature) and the symmetric encryption application (hash function) has turned out to be the favourite for securing an eCertificate. With the support of PKI, these could well provide the eCertificate system with confidentiality, integrity, and non-repudiation.

However, three issues relevant to eCertificate have been identified: public key certificate status validation, eDocument content validation, and eDocument status validation. Unlike the first two known issues, the third, eDocument status validation, is unique for the case of an eCertificate, although it is not mentioned in the literature. All three issues need to be addressed when designing the eCertificate system in order to provide the confidentiality, integrity, and non-repudiation throughout the eCertificate lifecycle (issue, distribute, and review).

3.5 Privacy and ownership

With technology developing rapidly, and information gathering and sharing become much easier, the privacy and ownership issues of the eCertificate have also increased.

3.5.1 Privacy Rights

Privacy, is generally understood and has remain unnoticed or unidentified by the public, as "*an Aspect of Human Dignity*" [19], and has been studied for decades. Cohen described privacy is "*anything but old-fashioned, … an indispensable structural feature of liberal democratic political systems … is foundational to the capacity for critical self-reflection and informed citizenship, … is also foundational to the capacity for innovation*" [38]

Cavoukian thinks that identity and privacy are "*closely related*", when a person's identity is unknown, he/she "*tend to have more privacy*". He has also used paying for a coffee as an example. If you pay cash, your identity is of an "*anonymous consumer*"; if you pay "with an pre-paid coffee card", your identity becomes "*a loyal patron*"; but when information such as your name, address, and the coffee purchases history are linked to the pre-paid card, your identity becomes "*identifiable individual*". Cavoukian also stated that "*information that can be linked to an identifiable individual is considered to be personal information*".[26]

The definitions of privacy are different in different countries, it is "*a sensitive prone to different interpretations which are largely politically and culturally determined*" [96]. Dragana and Victor have also stated that privacy protection in the USA is "*primarily motivated by the protection of liberty*," and in the EU is "*mainly the protection of one's dignity*," while those in Canada "*occupy the middle ground*."

Many countries have their own laws to protect privacy in different domains. For example, the USA has the Family Education Right and Privacy Act (FERPA) that requires education institutions to provide access to student record-related information to students and parents, including an access history of where, when, and by whom the record was accessed [110]. Canada has the Personal Information Protection and Electronic Documents Act (PIPEDA) that defines in detail what personal information is [12]; in Europe, the EU Data Protection Directive 1995 has set "the minimum standards for national privacy laws" and "defines personal data as any information related to an identified or identifiable person", either directly or indirectly [50]. However, there are many perfectly legal daily transfers in the USA and many other countries are in fact illegal under the EU regulations. In UK, the UK Data Protection Act 1998 has eight principles of data protection, and requires that all personal data processes must comply these principles [162]

In 1890, Warren & Brandeis pointed out that privacy is the "*right to be let alone*" [168]. Lessig believes that "*individuals should be able to control information about themselves*" and "privacy breaches online" could be "regulated through code and law" [87]. Alan believes that privacy rights can protect democratic processes but may limit government surveillance [171], while Etzioni believes that "privacy is merely one good among many others" and "privacy laws only increase government surveillance" [48, 49]. Regan believes that "individual concepts of privacy have failed philosophically and in policy", and she aims to strengthen privacy claims in policy-making [126]. Shade argues that "the human right to privacy is necessary for meaningful democratic participation, and ensures human dignity and autonomy" [142].

Privacy laws exist that concern the protection and preservation of privacy rights of individuals. The United Nations Declaration of Human Rights states that: "*Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers*" [163].

3.5.2 Privacy issues in Technology

As technology is being developed rapidly, the way in which privacy is protected and violated is also changing. The increased ability to share and gather information, such as peer-to-peer networking and data mining, also challenge our computer systems as they lead to new ways that privacy can be breached, and users have little or no control of the information about themselves that others may have, hold or access.

Use of the Internet led to data that could be stored permanently without our notice. Jeffrey stated that the web means the end of forgetting "*where every online photo, status update, Twitter post and blog entry by and about us can be stored forever*" [130]. Studies indicated that "75 percent of U.S. recruiters rejected candidates" based on their "internet profile", such as information gathered through search engines, personal web sites and blogs, Twitter, and Facebook [130]. Andrew, the Co-founder of Intel Corporation commented that "*Privacy is one of the biggest problems in this new electronic age. At the heart of the Internet culture is a force that wants to find out everything about you. And once it has found out everything about you and two hundred million others, that's a very valuable asset, and people will be tempted to trade and do commerce with that asset. This wasn't the information that people were thinking of when they called this the information age*" [70].

Furthermore, the web has become a social tool. While personalization technologies offer the power to enhance user online experience, many application are using networked user information to improve their user profile, which "*has the potential to amplify and complicate the Internet's inherent privacy risk and concerns*" [157].

Dragana and Victor state that “Privacy issues in education systems is important to investigate and complex to achieve, … as it become easier to collect and store personal records, we believe that privacy issues need to be addressed holistically”. They have also pointed out that “regardless of the way in which the information is collected, it most likely gets stored electronically in the form of database records. Security protection and proper maintenance, combined with access and retrieval protocols and policies, are expected to be put in place to maintain compliance with relevant privacy legislation and policies”. [96]

3.5.3 Ownership Rights

The term ownership is very broad and complex, it could be private, collective, cooperative, or common, could refer to objects, land, or intellectual property, and it can be gained or lost in many ways, such as buying and selling, exchange, or as a gift.

In The cost and benefits of ownership [69], Grossman and Hart defined two rights: specific rights and residual rights. They stated that ownership is the purchase of the residual rights, such that “*When residual rights are purchased by one party, they are lost by a second party, and this inevitably creates distortions. Firm 1 purchases firm 2 when firm 1’s control increases the productivity of its management more than the loss of control decreases the productivity of firm 2’s management*”. They also claimed that they “*do not distinguish between ownership and control and virtually define ownership as the power to exercise control*”.

3.5.4 Ownership Issues in Technology

Information ownership refers to “*both the possession of and responsibility for information, … implies power as well as control*”, these include “*the ability to access, create, modify, package, derive benefit from, sell or remove data*”, and the right to “*assign these access privileges to others*” [90]. It is “easily and frequently confused due to the lack of standardized definitions”, and is “*frequently assigned in organizations without regard to who created the information or where it originated*” [150].

In the world of computing, discussions and arguments regarding intellectual property aboud. For many years, this topic has also varied widely across countries and across cultures. Commonly, the person "*who creates, or initiates the creation or storage of the information*" is considered as the initial owner, and has the responsibility of safeguards while ensuring that the information "*continues to be classified appropriately" [140]*. Adam stated that "*one of the sacred laws of justice was to guard a person's property and possessions*" [146]. However, as Tsahuridu said, "*parting ways and deciding who keeps the material created during the relationship can be a tricky business*" [161]. Aristotle pointed out two main issues: "how to allocate property between what is private and common and how to allocate the private property within society" [97].

Stevens believes that "as long as the ownership of the information asset is established, the owner has responsibility and authority to perform ownership duties, and accountability is enforced" [150].

In military cyber information flows, "*the relationship between the information producer, information owner, and information consumer do not adhere to the traditional definition*", but their "*clearly defined roles of consumption and ownership become relative to need and to the contextual value within an organization*" [68]. Webb believes that the ownership of media may "*even extend to the documents or media in which the secrets are disclosed such that the owner controls not only the underlying intellectual property rights but also the physical embodiment of such rights whether in the form of a document or a tape or disk. This allows the owner to call in such documents or other media when the relationship which was the occasion for disclosure terminates*" [169]

3.5.5 Calls for a User-Centric Data Model

With the use of Cavoukian's technical terms of "user-centric", "enterprise", and "federated" [26], Dragana and Victor categorise the current models for organizing personal information as Clustered, Centralised, and Mixed. They define Clustered as a user-centric model, where "there is no central repository of personal data and every person has some control over his/her personal data in terms of accuracy and further dissemination”; Centralised is an enterprise model, where “there is a centralised repository of personal data with role-based control over accessibility to data”; and Mixed is a federated model, which lies between the other two [96].

Graham, presented his opinion at a conference that our data should be accessible to us “through any channel, on any device, at any time”; we should have the right “to store, update and manage, … to have authenticated, verified and certified, … to share, sell and track, … under our control, with our consent, for our benefit”, and on the terms of “Secure, Convenient, and Valuable” [133].

Although lots of systems that we currently use are presented as enterprise models, calls for a user-centric model have rapidly increased in the past few years as it “better facilitates privacy protection” [96]. Many systems have or are planning to re-examine their design to meet the increasing demand of “privacy and personal data protection”, while enabling “individuals owning and controlling their personal data and information” [96]

3.5.6 Discussion

According to the definition that ownership can be gained through gift, students can gain ownership of their eCertificate when being awarded, no matter how many other parties also have ownership during the creation process.

As technology continues to develop, information gathering and sharing are much easier than ever before. As a result, privacy and ownership issues have also increased rapidly.

In literature, discussions around privacy and ownership are mainly about the stored data, but not much about the distributed data, especially how to protect privacy and ownership of the distributed data from unauthorized further forwarding and accessing. This could be the main task for the case of eCertificate as the distributed eCertificates are very likely to be passed or collected by unauthorized parties, such as recruitment agencies, without owners’ consent.

There have been many calls for a user-centric data model found in literature which aims to give the information owner full control of their data, that includes storage, updating, sharing, tracking, and who can access and for how long. These qualities should also be integral when designing the eCertificate, in order to develop a user-centric eCertificate system.

3.6 Chapter Summary

eCertificates represent a typical case of eDocument that contains dynamic content and needs to be transferred to multiple parties. The literature was reviewed about what an eCertificate should consist of and how to secure such a distributed eDocument. The result indicated that:

- Certificates require support for verification, revocation and time limit re-certification processes. The eCertificate, as an electronic qualification award certificate, is still a new field in literature: beyond the paper-based certificate elements, there is no clear indication of what an eCertificate should include or what format it should be. However, the SPOCS project has proposed an eDocument structure, and its OCD concept could be used for eCertificate file structure design.
- ePortfolios, as the main usage of eCertificate, lack security control. They require verifiable data with supported evidence; and eCertificate, when being used within other systems, such as ePortfolios, need to be verifiable, compactable and recognisable. Some of the barriers that ePortfolios face, such as users with low IT skills, will also apply to eCertificate.
- Security involves many areas. Merely securing an issued eCertificate would be insufficient to prevent it being hacked, faked, or modified in many areas: such as the database, the application, the software, or the network. The whole lifecycle of the eCertificate system needs to be secured, from its creation, distribution, to verification processes, from its front-end application, distribution paths, to the back-end database and the human controls. The right balance between confidentiality, integrity and

availability, needs to be determined to ensure the eCertificate is user friendly while maintaining a high level of security.

- Both Symmetric and Asymmetric encryption methods have their pros and cons. A combination of digital signature and hash function appear to provide an optional means of securing an eCertificate; with the support of PKI, these could well provide the eCertificate system with confidentiality, integrity, and non-repudiation.
- Many issues exist in the field of encryption and the digital signing application. Among them, the public key certificate status validation issue and the eDocument content validation issue, will directly affect the security of eCertificate system. A new issue, eDocument status validation, which is key to the eCertificate case, has not been mentioned in literature. All three issues needed to be addressed in the eCertificate design in order to provide a secure eCertificate system.
- Acts and policies exist for different domains and cultures to address the information privacy and ownership issues. However, the world of security in computing is changing, such that the ways in which privacy and ownership are protected and violated are also changing: from the systems orientated “Fortress Approach” to the needs of securing our privacy and ownership in peer-to-peer networking, social networking and link data environment. Currently, users still have little or no control of their data, or how people may have, hold or access to their data. As a result, the demand for a user-centric system is increasing rapidly, with a call to give users back control of their own data.

Chapter 4 Domain Research

Before considering a new eCertificate system, it is important to find out, besides the literature, what systems and information are already available, what can be adapted, and what limitations exist that need to be overcome. These, together with the literature review, will provide an informed background of what is required in the investigation of the new eCertificate system.

Domain research was carried out, which has been focused on related previous works, existing systems, and domain experts' opinions.

This chapter summarises the related work in the eCertificate domain. It is expressed in the researcher's own words. It has been published in conference papers [34, 35] and in the eCert project website[28].

4.1 Previous Work: The eCert-GDP2008 Project

A project entitled "eCert-GDP2008" [132] was run in the school of Electronics and Computer Science, at the University of Southampton, to explore the issues of on-line authentication of awards, and produced an award verification demonstrator.

4.1.1 The Demonstrator and the Development Group

The eCert-GDP2008 project explored the issues of three-party authentication and demonstrated how to best approach the process of validating students' claimed awards in such an environment.

The demonstrator was developed by a group of four MSc Computer Science students. This was the end product of the group development project (GDP) within their degree study. EdExcel, a UK national certifying authority, was also involved in working with the project team to explore and create a potential model and proof-of-concept system.

4.1.2 The Design

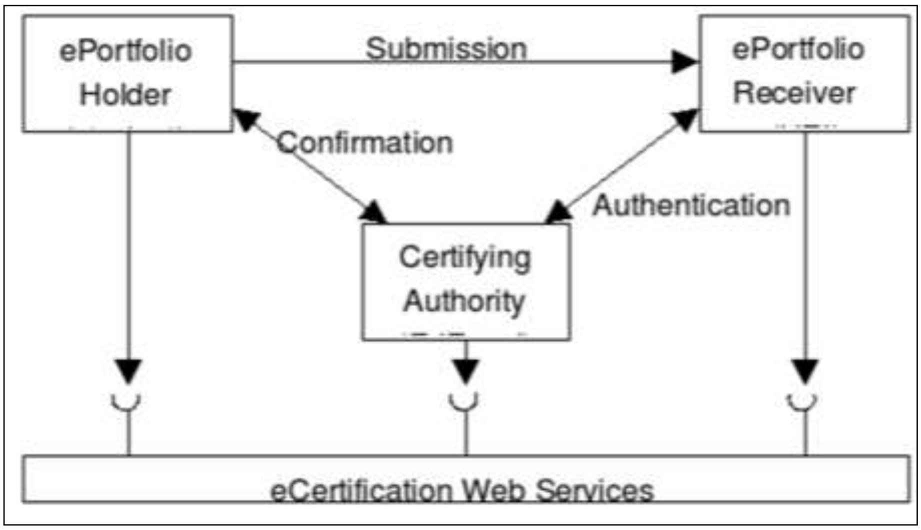


Figure 4-1 Original design for eCert-GDP2008 project, published in[34]

The eCert-GDP2008 project raised interesting points. In particular, many conventional security scenarios assume two stakeholder transactions, with any third party involved being an attacker. In e-certification, three parties are involved in the transaction; any external attacker becomes a fourth party. The system not only dealt with access to resources with the attendant issues of Authorization, but also with verification of the information provided. Figure 4-1 shows its original design, Figure 4-2 indicates the important interactions within the system.

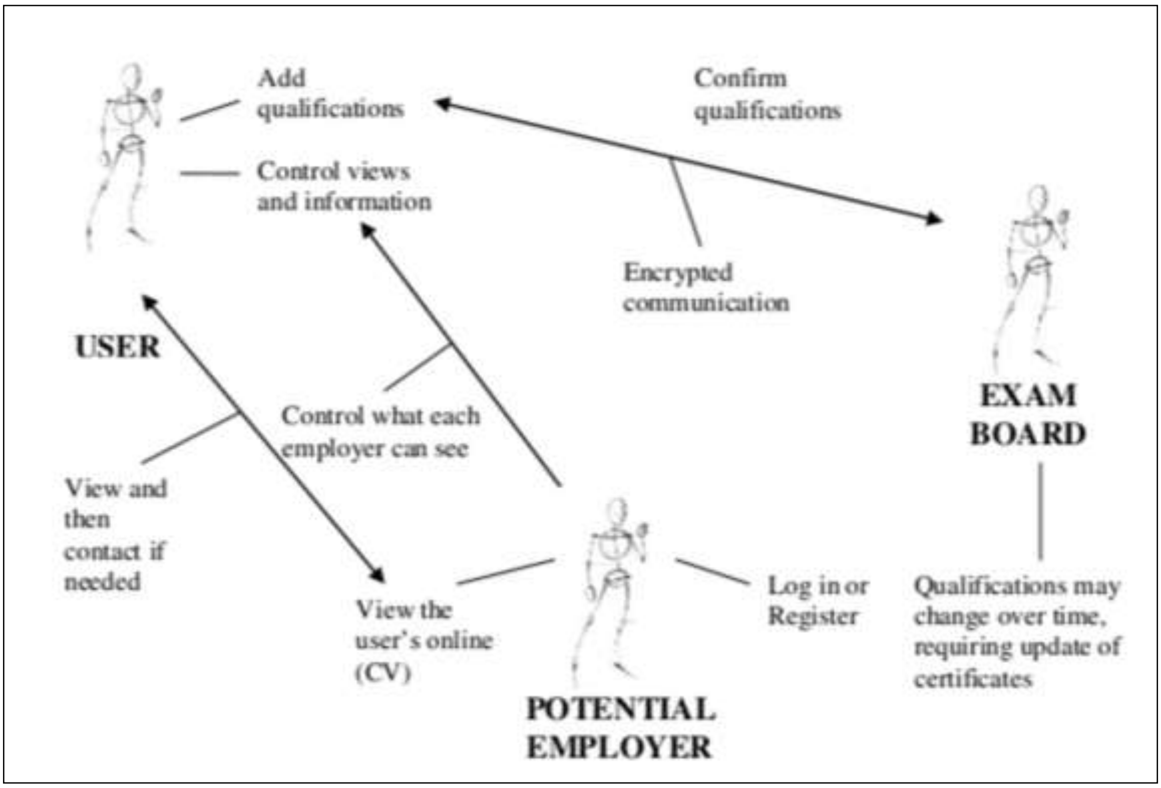

Add qualifications
Confirm qualifications
Control views and information
Encrypted communication
USER
EXAM BOARD
Control what each employer can see
View and then contact if needed
View the user's online (CV)
Log in or Register
Qualifications may change over time, requiring update of certificates
POTENTIAL EMPLOYER

Figure 4-2 The interactions within the system, published in [34, 35]

4.1.3 The Security Model

The group made some security policy decisions. These not only concern who can see what and when, but also the value of the data. For example, one might decide that information about qualifications is less valuable than banking details, so the level of security could be lower if it aids usability of the system. In contrast, one might decide that the level of security should be higher to prevent identity theft, for example.

The security policy decisions adopted were:

- The data is to be regarded as important and therefore should be properly secured
- There should be minimal transfer of data
- It should not be possible to browse the data; all queries should be of the format, <claimed award> and the response, <true/false>

- The award holder (student) should determine who may see their award details

These decisions introduced novel design criteria. The basic concept was that there would be a Certification Server – the Certifying Authority in the original design. This provides a service to the ePortfolio Holder (student) who can build up a set of ePortfolio certificates, each one tailored for a specific ePortfolio Reviewer (e.g. employer). Because of design policy 3 above, it is not possible for the student to browse their awards and select from a list. Instead they have to be entered individually. Although this could be annoying for the student, it prevents attackers from intercepting the communication and obtaining all the student's qualifications in one go. Similarly, it prevents the employer from taking the student's details and making a general enquiry to see what information about awards has been withheld.

As the student builds up their award profile, the Certification Server contacts the Awarding body (e.g. EdExcel in our case, but as many awarding bodies as possible ought to be part of a full scheme). This is done on an "is this true" basis, with a true or false answer being returned as in design policy 3 above. The student's profile then builds up with a series of certified claims, and hopefully none denied! It is also likely that there may be some unverifiable claims (e.g. an award from a body that is not part of the scheme). In practice, it was found that a fourth possibility was "pending" – i.e. it should be possible to verify the claim, but for some reason the Certifying Body has not yet responded, possibly as a result of their server being offline. The final step in building up their profile is for the student to select which awards they want to present to a given employer, which is done via a tick box grid.

Having built up an award profile for a particular employer, the student is now given a code by the Certification Server. This code is then sent to the employer, who can use this to log in to the Certification Server to see the student's award profile. The web page that they see gives a "stamp" indicating the status of the claim.

4.1.4 Advantages

All communications are encrypted and digitally signed so the source can be verified. This entails the use of both public and private key encryption.

The benefit of this approach is that all original data remains with the Certifying Authorities. The Certifying Sever simply communicates with these authorities to confirm or deny claims, and no data is passed on from this point – all communications involve the Server.

4.1.5 Limitations

The purpose of this project was to investigate the issues involved in setting up an e-Certification system, particularly from the security point of view. In order to make it realisable within a realistic timeframe, the scope was limited, and focused particularly on the delivery end, linking to the ePortfolio holder and the ePortfolio reviewer.

The project explored security issues, particularly in the client-facing side of the process. The issues of scalability and the need to communicate with multiple awarding body servers were not considered.

4.2 Existing Systems

Some existing systems are relevant to the validation of qualification records or certificates. Typical examples have been selected and are examined here.

4.2.1 The Europass

The European Community provides Europass Certificate Supplements and Diploma Supplements [51], which are facsimiles of award certificates and information about the qualifications.

All information below about Europass has been sourced from the Europass website[8]

[8] http://europass.cedefop.europa.eu/europass/home/hornav/Introduction.csp

4.2.1.1 The service and its organization

Europass was established in 2004, with the aim of "facilitating the mobility of European learners and workers by making their skills and qualifications more easily understood in Europe" [51]. Besides the online CV, Europass offers four document services: "Europass Language Passport; Europass Mobility; Europass Diploma Supplement; and Europass Certificate Supplement".

4.2.1.2 The Europass Certificate Supplement

A Europass Certificate Supplement is "made available to individuals who hold a further education and training award certificate by the body that issued the award certificate". It aims to make the award certificate "more easily understood by employers or institutions outside the issuing country". It provides additional information to the award certificate. This includes [51]:

- *"the awarding status of the body that issued the award*
- *the skills and competences acquired by ALL holders of the award*
- *the level of the award in the national awarding system*
- *the typical entry requirements to programmes that lead to the award*
- *the typical employment or learning opportunities that are accessible to holders of the award"*

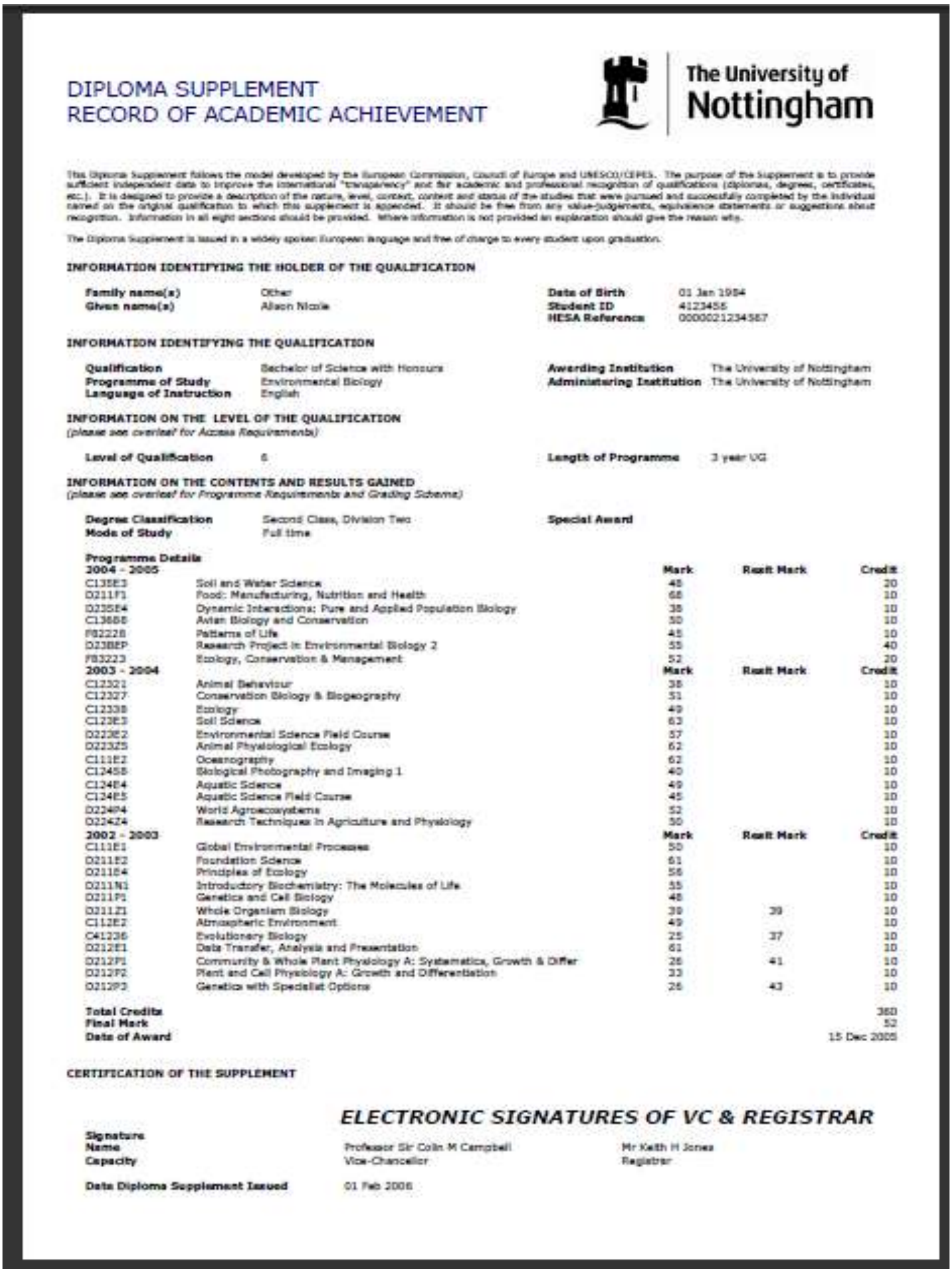
4.2.1.3 The Europass Diploma Supplement

A Europass Diploma Supplement is "issued to graduates of higher education institutions along with their degree or diploma. It helps to ensure that higher education qualifications are more easily understood, especially outside the country where they were awarded". [51]

The Europass Diploma Supplement was developed by the European Commission, Council of Europe and UNESCO/CEPES. It aims to provide "*sufficient independent data to improve the international 'transparency' and fair academic and professional* *recognition of qualifications (diplomas, degrees, certificates, etc.)*" It is designed to "*provide a description of the nature, level, context, content and status of the studies that were pursued and successfully completed by the individual named on the original qualification"* [9] to which the supplement is appended. Figure 4-3 shows a screenshot of part of a Europass Diploma Supplement example. [51]

The Diploma Supplement "is issued in a widely-spoken European language and free of charge to every student upon graduation" [51].

[9] http://www.uknec.org.uk/index.asp?page=9



DIPLOMA SUPPLEMENT
RECORD OF ACADEMIC ACHIEVEMENT

The University of Nottingham

This Diploma Supplement follows the model developed by the European Commission, Council of Europe and UNESCO/CEPES. The purpose of the Supplement is to provide sufficient independent data to improve the international "transparency" and fair academic and professional recognition of qualifications (diplomas, degrees, certificates, etc.). It is designed to provide a description of the nature, level, context, content and status of the studies that were pursued and successfully completed by the individual named on the original qualification to which this supplement is appended. It should be free from any value-judgements, equivalence statements or suggestions about recognition. Information in all eight sections should be provided. Where information is not provided an explanation should give the reason why.

The Diploma Supplement is issued in a widely spoken European language and free of charge to every student upon graduation.

INFORMATION IDENTIFYING THE HOLDER OF THE QUALIFICATION

Family name(s)	Other	**Date of Birth**	01 Jan 1984
Given name(s)	Alison Nicole	**Student ID**	4123456
		HESA Reference	0000021234567

INFORMATION IDENTIFYING THE QUALIFICATION

Qualification	Bachelor of Science with Honours	**Awarding Institution**	The University of Nottingham
Programme of Study	Environmental Biology	**Administering Institution**	The University of Nottingham
Language of Instruction	English		

INFORMATION ON THE LEVEL OF THE QUALIFICATION
(please see overleaf for Access Requirements)

Level of Qualification	6	**Length of Programme**	3 year UG

INFORMATION ON THE CONTENTS AND RESULTS GAINED
(please see overleaf for Programme Requirements and Grading Scheme)

Degree Classification	Second Class, Division Two	**Special Award**	
Mode of Study	Full time		

Programme Details

2004 - 2005		**Mark**	**Resit Mark**	**Credit**
C135E3	Soil and Water Science	45		20
D211F1	Food: Manufacturing, Nutrition and Health	68		10
D235E4	Dynamic Interactions: Pure and Applied Population Biology	38		10
C13688	Avian Biology and Conservation	50		10
F82228	Patterns of Life	45		10
D23BEP	Research Project in Environmental Biology 2	55		40
F83223	Ecology, Conservation & Management	52		20
2003 - 2004		**Mark**	**Resit Mark**	**Credit**
C12321	Animal Behaviour	38		10
C12327	Conservation Biology & Biogeography	51		10
C12338	Ecology	49		10
C123E3	Soil Science	63		10
D223E2	Environmental Science Field Course	57		10
D223Z5	Animal Physiological Ecology	62		10
C111E2	Oceanography	62		10
C12458	Biological Photography and Imaging 1	40		10
C124E4	Aquatic Science	49		10
C124E5	Aquatic Science Field Course	45		10
D224P4	World Agroecosystems	52		10
D224Z4	Research Techniques in Agriculture and Physiology	50		10
2002 - 2003		**Mark**	**Resit Mark**	**Credit**
C111E1	Global Environmental Processes	50		10
D211E2	Foundation Science	61		10
D211E4	Principles of Ecology	56		10
D211N1	Introductory Biochemistry: The Molecules of Life	55		10
D211P1	Genetics and Cell Biology	48		10
D211Z1	Whole Organism Biology	39	39	10
C112E2	Atmospheric Environment	49		10
C41236	Evolutionary Biology	25	37	10
D212E1	Data Transfer, Analysis and Presentation	61		10
D212P1	Community & Whole Plant Physiology A: Systematics, Growth & Differ	26	41	10
D212P2	Plant and Cell Physiology A: Growth and Differentiation	33		10
D212P3	Genetics with Specialist Options	26	43	10

Total Credits	360
Final Mark	52
Date of Award	15 Dec 2005

CERTIFICATION OF THE SUPPLEMENT

Signature	*ELECTRONIC SIGNATURES OF VC & REGISTRAR*	
Name	Professor Sir Colin M Campbell	Mr Keith H Jones
Capacity	Vice-Chancellor	Registrar
Date Diploma Supplement Issued	01 Feb 2006	

Figure 4-3 A Europass Diploma Supplement example, reprinted from [53]

4.2.1.4 Advantages

The additional information provided with the award certificate, benefits both the award certificate holders and the reviewers: "*award holders will be able to communicate their qualifications and competences in an effective way; employers will find the qualifications and competences of job-seekers easier to understand; education and training providers and guidance counsellors will find it easier to provide accurate advice to award holders regarding suitable learning opportunities*" [51].

4.2.1.5 Limitations

The Europass clearly states that, "The Europass Certificate Supplement is not: a substitute for the original certificate;" or "an automatic system that guarantees recognition" [52]. But this is not good enough for security in the real world. Also, this does not solve the problems that are faced with paper-based certificates as it needs to be accompanied by the original certificate. Furthermore, the document is not suitable as a standalone proof of qualification in an ePortfolio as its detailed records, such as individual module marks, which may work against privacy issues.

4.2.2 The HEQC

In China, an online information verification service for higher education qualification certificates (HEQC) has been running since 2001. The service is carried out by the China Higher-Education Student Information and Career Centre (CHESICC). It is based on information collected since 1991.

All information collected here is from the CHESICC website[10].

4.2.2.1 The service and its organization

CHESICC is "*a specialized body authorized by the Chinese Ministry of Education (CME) for verifying any certificates or diplomas awarded in China*" [37]. Its

[10] HEQC: an online information verification services for higher education qualification certificates. http://www.chsi.com.cn/about_en/

website is the sole website designated by the CME for HEQC inquiries. It has the only database for information of the HEQC.

The service provides online certificate information, verification for those certificates that were gained in higher education since 2001, and an offline certificate verification service for any year's certificates. The certificates that have been verified offline will then be also available for online verification.

The service is designed for individuals as well as organizations although a charge is made.

4.2.2.2 The method

The government announced that every student starting their HE course since 2001 must have an electronic student status registration.

The students who have a electronic status registration record will be able to register their certificate information and build it up in their years of study.

Both the student status and the certificate information are verified step by step under the management of government body. Figure 4-4 shows the work flow of the electronic registration system in China.

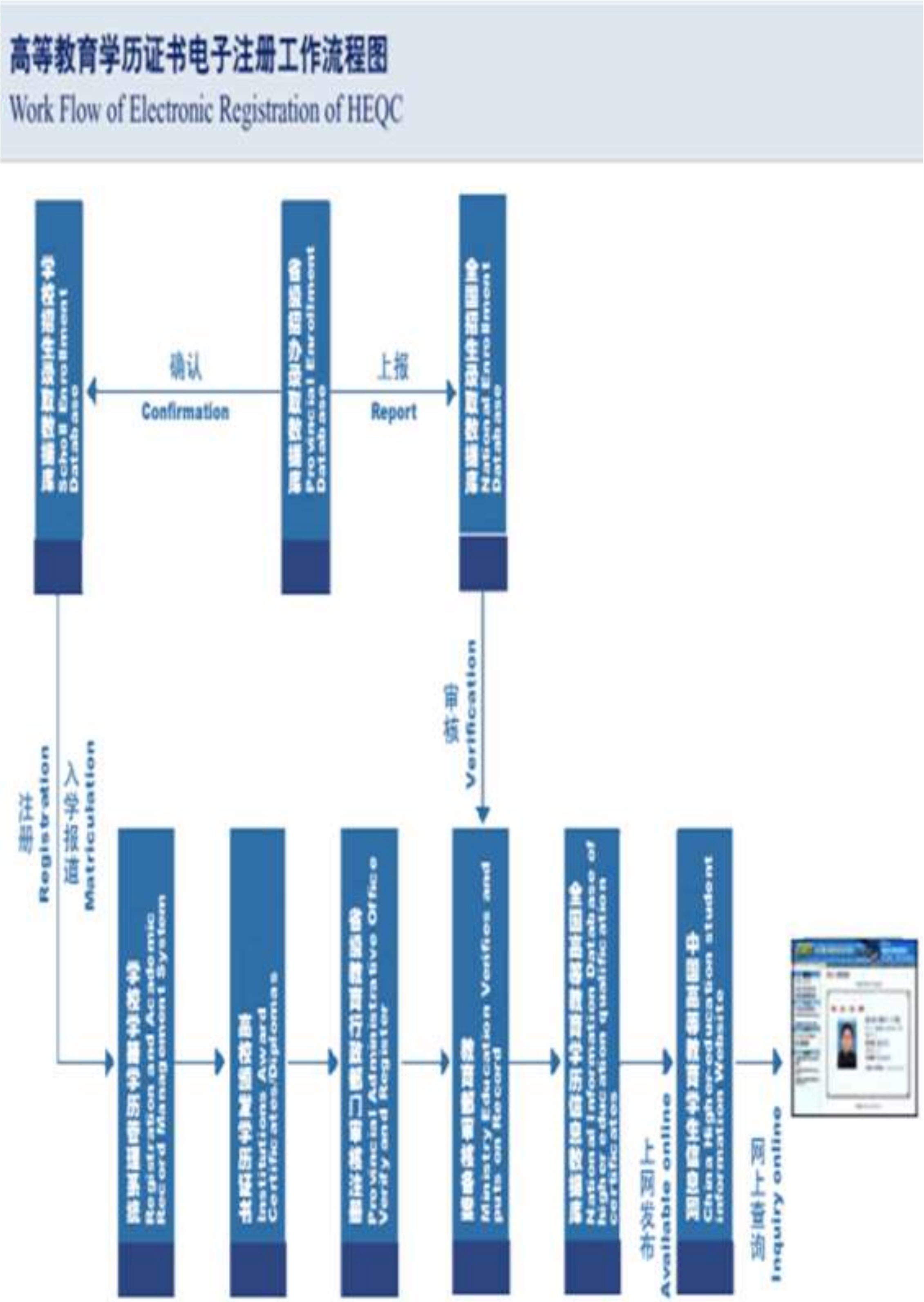

高等教育学历证书电子注册工作流程图
Work Flow of Electronic Registration of HEQC
学校招生录取数据库
School Enrollment Database
确认
Confirmation
省级招办录取数据库
Provincial Enrollment Database
上报
Report
全国招生录取数据库
National Enrollment Database
审核
Verification
注册
Registration
入学报道
Matriculation
学校学籍学历管理系统
Registration and Academic Record Management System
高校颁发学历证书
Institutions Award Certificates/Diplomas
省级教育行政部门审核注册
Provincial Administrative Office Verify and Register
教育部审核备案
Ministry Education Verifies and puts on Record
全国高等教育学历信息数据库
National Information Database of Higher Education Qualification Certificates
网上发布
Available online
中国高等教育学生信息网
China Higher Education student Information Website
网上查询
Inquiry online

Figure 4-4 electronic registration system work flow, reprinted from [37]

The certificates that were awarded before 2001 will require offline certificate certification before they can be available for the online verification service.

4.2.2.3 Advantages

The system is on a large scale in both time and coverage, and its government authorized body provides the trust.

4.2.2.4 Limitations

The whole process sounds like creating an ePortfolio (with the student status as the ePortfolio account and the certificate information as its contents), but it is at a government level, not a personal level, so that the student (the account holder) has no control and use of it.

The service aims for verification only, not the use of eCertificate that is the focus of this research.

4.2.3 Digitary

Digitary, which stands for "Digital Notary", was established by Framework Solutions in 1999. It worked with the Higher Education sector to issue, distribute and authenticate official electronic graduation documents over the Internet. It was first implemented in 2005 [43].

All information collected here is from the Digitary website[11].

4.2.3.1 The service and its organization

Digitary describes itself as "*a high-security software system developed with the Higher Education sector for the online issuing and authentication of tamper-evident electronic official graduation documents*" [43]. It also states that documents issued through the system are electronically signed by officials of issuing institutions and are therefore legally valid.

A charge is levied for the service. Educational institutions who want to use the service need to install the system on their site, and students need to login to their

[11] http://www.digitary.net/

institution's system to access their documents. Employers who want to verify qualifications that were sent by the students or graduates, are required to carry out registration on Digitary at the issuing institutions, in order to authenticate and view the documents.

Digitary is "a trading name of Framework Computer Consultants Limited, registered in the Republic of Ireland" [43].

4.2.3.2 The method

Graduates and students "*who have been issued with Digitary documents by their institutions can allocate rights for who can access them by emailing a Document Access Ticket to them. People who have been given the right to access can authenticate and view documents*".

If some students decide to restrict access, "*people to whom they send Document Access Tickets will need to complete an online account registration process, including proof of ownership of their email address*".

Audit trails enable users to see all activities against their accounts, such as "*when documents were issued, and when and from where they were authenticated*".

When an employer or third party verifies a Digitary document through the system, it performs a number of security checks on the document:

- they have been granted access to the document by the owner
- the document has not been revoked for any reason
- the document was issued by authorised officials of the institution in question
- the document has not been tampered with in any way

4.2.3.3 Limitations

Employers need to register with every institution's system where the qualifications were originally issued, to be able to verify the documents.

4.3 Domain Experts Advice

Nottingham University is one of the leading research groups in ePortfolio studies. Contacts with their researchers, e.g. Kirstie Coolin and Clive Church, were carried out during the eCert-GDP2008 project, an e-certification project for qualification records. Feedback on ePortfolio operations were supplied as secondary data to this project.

Contact with these experts has again been carried out at an early stage of this research to collect professional opinions on the new eCertificate system. As the topic was new to both parties, no specific requirements were noted at that time. However, concerns were raised, such as potential file size of the certificates which must be sent out by email; and the nature and role of such a system. The UK Government has a history of losing entire databases of sensitive personal information! Advice was that for the new eCertificate system to be a success, these concerns need to be addressed in the design stage.

4.4 Chapter Summary

Systems exist that provide the services for signing and/or verifying online qualification records or eDocuments. However, they are built with specific purposes, and therefore do not satisfy the eCertificates' requirements.

The eCert-GDP2008 project 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. Using this method also increases the risk of database attacks on those institutions. It does not involve eCertificates, so the paper-based certificate problem remains unsolved.

The European Community provides a Europass Certificate Supplement and a Diploma Supplement. 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 security in the real world. Also, this does not solve the problems faced with the paper-based certificates as it must be accompanied by the original certificate. Furthermore, the document is not suitable as a standalone proof of qualification in an ePortfolio as its detailed records, such as individual module marks, may work against privacy issues.

The Chinese Certificate Information Verification service is an eCertification service for qualification records, similar to eCert-GDP2008, but with different inputs and outputs. The service takes unique student numbers and unique certificate numbers as input, and outputs the specified qualification detail along with the student's personal details, including a photo. It provides more reliability to the viewers as it also verifies the identity of the person. But this method does not suit every country, e.g. it contravenes the Data Protection Act in UK. Again, this service does not deal with eCertificates.

The Digitary system issues, distributes and authenticates eCertificates over the Internet with the system installed at individual institutions. Students need to login to their institution's system to access and manage their e-Certificates, such as setting access for individual reviewers. Reviewers can then access the e-Certificates through the received URLs using access tokens; this may involve registration depending on the access level that was set. This is the closest system to this research for an eCertificate, except that the system only works for individual institutions. This is good for the eCertificate issuing process, but is not suitable for reviewers, who need to verify information received from a wide range of institutions. It also has storage issues as it requires the system to maintain all students' eCertificates, their different versions, and the corresponding access tokens. More importantly, lifetime validation of the issued eCertificate is a problem, if anything happens to the institution (e.g. it closes down) or its database (e.g. being hacked).

The eCertificate related systems that mentioned above is compared in Table 4-1. The issue of how to provide trust for a system that deals with sensitive data is a very important point raised by the domain experts. This will be the main task that needs to be addressed.

Table 4-1 eCertificate related systems comparison

	Verify eCertificate	**Verification nationwide**	**Require system storage**	**User control usage**	**Solve (certificate)^2 problem**	**Solve lifetime validation issue**
The GDP2008 project	No, records of awards only.	Yes/No (for linked institutions only)	Little (plus access to linked institutions' database)	N/A	N/A	No
The Chinese	No, records of awards only.	Yes	Medium (record only)	N/A	N/A	Yes (reported and stored in central)
Digitary	Yes	Yes/No (for installed institution only)	Huge (eDocs, access controls, and histories for each account)	Yes	No info	No
Europass	Yes	Yes	Little	No	No	No

Chapter 5 eCertificate Case Study

Following the SORM methodology, the domain definition was explored in Chapter 3 Literature Review and Chapter 4 Domain Research. An eCertificate case study was then carried out for the next layer: use cases. This chapter describes the formal use cases and the processes that lie between the related layers: the common usage patterns and gap analysis. These involve summarising the key activities from the domain, identifying the eCertificate stakeholders, developing the use cases where these stakeholders act, whilst considering techniques that address similar issues through a gap analysis.

This chapter is entirely the researcher's own work. It has been published in conference papers [29-33, 36] and in the eCert project website [28].

5.1 Common Usage Patterns

From the literature review and domain research that were described in Chapters 3 and 4, key activities for the eCertificate domain were identified. As a result, the common usage patterns were generated as requirements for the new eCertificate system, and these are summarized in Table 5-1.

Table 5-1 Common usage patterns as eCertificate system requirements (SR)

SR Identity	Summary
SR-01	can be used stand alone or served within an ePortfolio
SR-02	security control throughout the whole eCertificate lifecycle: from generation, issue, distribution, to verification; involves hardware, software, database, information, and human control
SR-03	can be verified in a legal context, supports withdrawal of an eCertificate and the content status validation as well as the signing key status validation
SR-04	ensure that the owner has control over the usage of their eCertificates
SR-05	effective usage: easy to use, supports lifetime validation, and can be widely verified and recognized throughout the UK

5.2 Stakeholder Analysis

In ePortfolio systems, an ePortfolio is considered to have two stakeholders: the ePortfolio creator as the owner, and receiver as the reviewer. In eWork, the qualification data is considered to have three stakeholders: record creator as the issuer, government bodies as the holder/owner, the student and any third parties who need access as the reviewer [92, 93].

In this study, the eCertificate owner is considered to be the student graduate, just like the ownership that they have of their paper-based certificates. According to studies of related systems, the eCertificate system is considered to have three stakeholders: the originating institution as the issuer, the student as the owner, and the receiver as the reviewer. Any government bodies that co-own the qualification records are not considered as eCertificate owners. Likewise they do not own the students' paper-based certificates. However, the proposed eCertificate could record, hold, and provide access to any government bodies, as it will be able to be used standalone or serve within other systems.

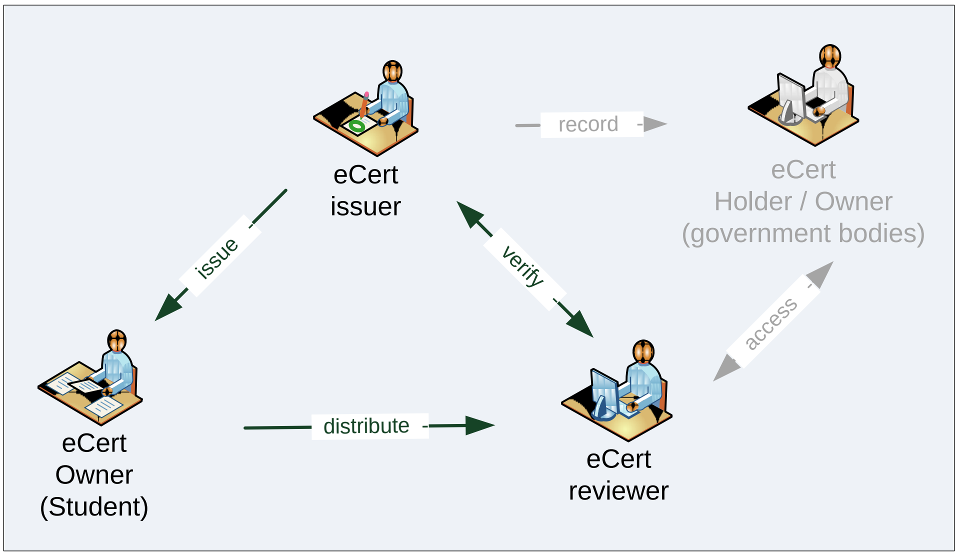


Figure 5-1 eCertificate Stakeholders and Activities

These three stakeholders perform three processes: issue, distribute, and verify, as showed in Figure 5-1, and are described below.

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

- issue a huge range and number of certificates
- have to restrict database access for any incoming verification requests to minimize database attacks.

An eCertificate owner is the certificate holder who has successfully passed the qualification certification process and gained the award, such as a student or a graduate. They may

- hold low, high, and/or special level of qualifications
- have qualifications achieved in different areas of the UK (world-wide certificates are considered as out of the scope for this study)

- have differing levels of IT skills
- or may not have an ePortfolio account

An eCertificate 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 a big organization
- may receive e-qualification certificates as part of applications or within ePortfolios
- may have few IT skills or may have a team of IT literate staff with high tech IT equipment
- may need to check a few qualifications occasionally or may need to check a huge number of qualifications efficiently
- may need to review varied levels of qualifications that were issued across the UK.

5.3 Use Case

Based on the certificate process study from the literature review, with the selected three eCertificate stakeholders in mind, and the user case collation [76] from the eWork project, the related personas and scenarios have been arranged to help with understanding the situation, as depicted in Table 5-2 and Table 5-3.

Table 5-2 Stakeholders

Stake holders	**Types**	**User details**
eCertificate Owner (Student)	Low level qualifications	User Ann, aged 16, a secondary school student, has achieved GCSE in Maths; she hasn't set up an ePortfolio account, and her IT skill level is low.
	Combination of low and high level qualifications	User Ben, aged 43, a computing lecturer of a university, has achieved PhD Computer Science & MSc Complexity Science; he has an ePortfolio account, and his IT skill level is high.
	Special qualifications – e.g. life critical	User Chris, aged 38, a hospital surgeon, has achieved qualifications MD Medicine & FRCS (Surgery); he hasn't got an ePortfolio account, but is IT literate
	qualifications achieved in different areas of the UK	User Dave, aged 23, studied A level in the south of the UK, and the first degree in the north of the UK, has achieved A level in English & BA in English; he has got an ePortfolio account, but only has basic IT skills.
eCertificate Reviewer	Potential employer	User Eric, an director of a small company, needs to employ a couple of staff from time to time, has received information of potential employees on both paper-based CVs and ePortfolios; he has internet access, basic IT skills only, and needs to check a few qualifications occasionally.
	Further education institution	User F, a department of a university in the UK, takes in hundreds of new students every year, has received a huge number of applications on paper-based CVs, UCAS forms and ePortfolios. Some qualifications were achieved overseas. User F has high tech IT equipments, a team of IT literate staff, and needs to check a huge number of qualifications efficiently, all levels of qualifications, across the UK and from abroad.
eCertificate Issuer	Certifying Authority – an exam board	User J, an exam board, offers many certification courses, issues a huge range and number of certificates all year round. User J maintains a database for all these records itself. It is happy to carry out any verification processes for either individuals or big companies, but its data protection is considered as very high, and it is doing its best to prevent information leaking in any way.

Table 5-3 Use case, published in [11, 29-32]

Processes	Scenarios and conditions
create	An exam board checks that the students have successfully passed the particular exams, and are who they claim to be, and then creates the eCertificates accordingly. -- This involves identification and verification against the exam board's database. The creation process needs to have standard control for both low and high level qualification certificates in order to suit educational institutions of a wide range.
withdraw	An exam board found out that an eCertificate was mis-issued, and must be withdrawn. -- This needs security methods to support the withdrawal mechanism.
issue	The exam board issues the eCertificates for students. -- This needs security methods to a) indicate that the eCertificates are issued by the exam board, in order to prove their genuineness, and prevent unauthorized editing and copying after issue; b) issue the eCertificates.
receiving award	The students receive their eCertificates, and view the contents. -- This needs security methods to ensure that no one other than the students themselves can view their own eCertificates.
manage	A student specifies certain eCertificates to be visible to particular employers. -- The student needs to be able to control which eCertificates are visible by which employers 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 eCertificates to potential employers. -- The student should be able to send the eCertificates alone or within an ePortfolio. For students sending the eCertificates through ePortfolio accounts, only the selected eCertificates in the account should be visible to the employers.
review	An employer views the received eCertificates. -- This needs security methods to a) ensure only the specified employer can view the eCertificates, and no-one else; b) protect from modifying and unauthorized copying.
verify	The employer verifies the received eCertificates. -- The system needs to be able to verify all level qualifications that are issued using the same standard from any education institutions nationwide, and check that the eCertificate and the key are still valid.

5.4 Use Case Analysis

The scenarios are shown diagrammatically as use cases in Figure 5-2 published in [29-32]. Through the scenarios and use case study, we may note that the eCertificate system involves assertion, trust, privacy, distribution, property rights, and the lifetime issues. As the eCertificate and the qualification claims in ePortfolios face similar situations, some of the issues have already been identified by Blowers [20] in his ePortfolio study, such as the assertion, trust, privacy and distribution.

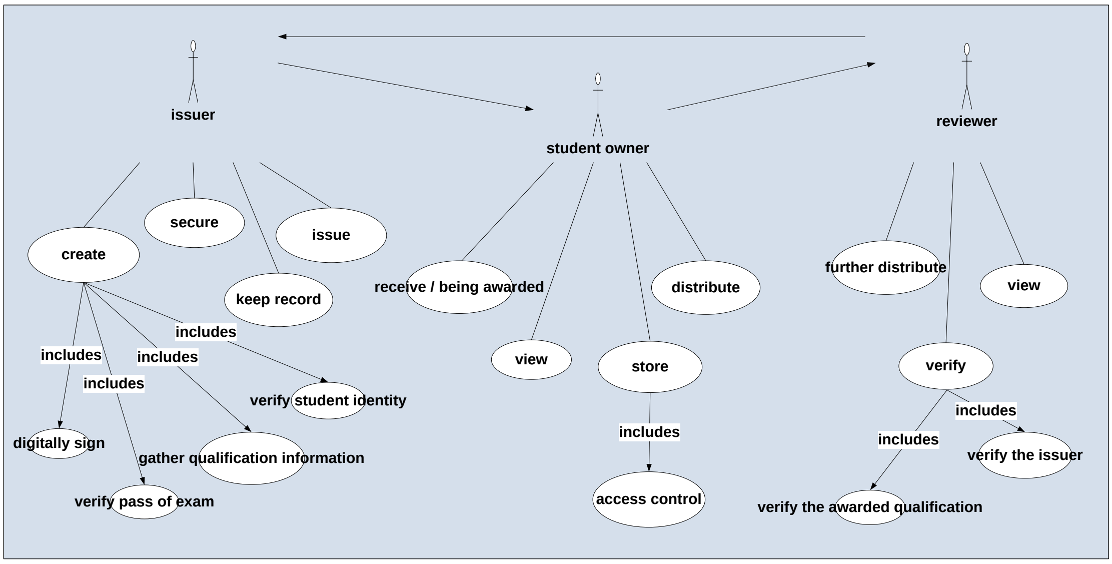


Figure 5-2 eCertificate use case diagram

eCertificate assertion: the system need to be self certificating to prove it is genuine, and also 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 [154].

eCertificate 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 particular audience [66]. This means the owner can tailor their portfolio to best support their application. This also applies to eCertificates, as no matter whether they are used standalone or within an ePortfolio, one aim is to give students control over who can see their eCertificates and for how long. This can prevent untrustworthy reviewers republishing the eCertificate without the owner’s permission; for example, to an ePortfolio bank which recruitment agencies might access. This is a similar paradigm to Web 2.0 social networking sites where a user can “*categorize their network (of friends) into different access groups with different access privileges*” [121].

Information property rights: the learners have not only needs, but also rights. They have the ownership right of their qualification attainments, in the same way 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” [133].

Stakeholder trust: A fundamental requirement from the use cases is the need to establish trust amongst all three stakeholders, such that one stakeholder can place faith that the identity of another is true, and their eCertificates have not been tampered with. The issuer needs to maintain a reputation for credible awards; they do not want to be known as an awarding body that is linked with suspect eCertificates, for example, so it is important that their eCertificates can be proven not to have been tampered with. The owner (student) also wants to know that they can trust the credibility of the award they have obtained; but they also need to trust the reviewer not to misuse the information on the certificate, for example by harvesting the information and selling it on to recruitment agencies. The reviewer needs to be able to trust the issuer, not only to maintain standards, but also to have protected against fraud (e.g. if a corrupt employee were to accept a bribe to produce a fake eCertificate); and similarly, to trust the owner not to have tampered with the eCertificate. 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 methods such as Pretty Good Privacy (PGP) where chains of trust are formed between users who already know each other [116].

Distributed stakeholders: To "*stimulate large-scale uptake*" of users [125], eCertificate tools need to define an "*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 [111].

eCertificate lifetime validation: In standard approaches to computer security, authentication and validation are typically considered as instantaneous activities – the system authenticates a user and validates their request or data immediately. Longer periods of time are necessary in transaction processing, but authentication and validation are still only relevant for the duration of the transaction. Indeed, long periods of authentication are undesirable, so it is common for "sessions" to be "logged off" or terminated if they exceed a predetermined length of time. If we consider the three parties authentication problem outlined above, it can be seen that the effective "transaction" period lasts for the entire lifetime of the eCertificate owner. Considering the parallel of paper certificates, many of us can probably think of people who have continued studying well past the age of retirement. Yet they may still be presenting awards they acquired as children, decades previously. The important factor in this is the lifetime of the eCertificate owner. During their lifetime, it is almost certain that awarding bodies will have come and gone, so an eCertificate system needs to be able to validate an award long after the issuer has ceased to exist. Similarly, reviewers will come and go, although this is less of a problem in practice. The implication of this is that an eCertificate system needs to be independent of both issuer and reviewer and to be able to provide a mechanism for the eCertificate owner to continue to provide evidence of their attainment long after the issuer has disappeared.

5.5 Gap Analysis

With the use cases defined, a gap analysis was performed to discover whether it is required, and if yes, what services can be reused and what technical gaps need to be addressed.

5.5.1 Is it required?

The literature review indicated that eCertificate is a new field in research. The problems faced need a solution. As technology develops rapidly, eCertificate could be a solution for many situations, such as ePortfolio. In order for a third party to verify qualifications that are claimed in an ePortfolio, it is necessary for ePortfolio systems to implement an on-line equivalent of paper-based certificates. However, and to date, no literature was found in eCertificate for qualifications. This indicates that no implementations have explored the underpinning technology or mechanisms required in this area. The eCertificate of qualifications is a new field of research, and this is true across the world.

Even if there are no studies in this area, the point has been spotted, and the European Communities [51] "Europass" provides Certificate Supplements and Diploma Supplements, and there are eCertificate systems produced by commercial companies. These provide facsimiles of award certificates and information about the qualifications, but the system clearly states that "*The Europass Certificate Supplement is not a substitute for the original certificate*;" nor "*an automatic system that guarantees recognition*." However, with their various design purposes, they do not satisfy our requirements sufficiently. Therefore, a framework for a secure eCertificate system is definitely required.

5.5.2 Feasibility

There are technologies available for constructing an eCertificate framework: digital signing, encryptions have been used in document security and transitions; online identification and validation has been addressed and implemented securely in other contexts such as e-Commerce and on-line auctions. The challenge now is to identify and design what is required; and adapt the available technologies to the eCertificate system and make it really secure.

5.5.3 Gaps in Related Technology

A gap analysis against current techniques and services was carried out to discover what could be reused and which technical gaps need to be addressed.

The process of confirming the veracity of an academic award using paper certificates is well established, and the potential for exploitation is also well understood [61][63][98]. In the on-line world, the concepts of digital signing, locked PDF, and watermarking are also well understood, with technologies available to support such processes [58]. The literature review for encryption and digital signature application in section 3.4, showed that digital signing turned out to be the most suitable technique for an electronic version of qualification certificates (eCertificates), among these eDocument security techniques; it is a mathematical scheme for authentication of a digital message or document. It not only detects unauthorized modification, but also proves the issuer, and therefore provides trust that the eDocument is genuine. However, the literature review also indicated that some limitations exist, such as service support, key management, and lifelong validation. These crucial limitations affect its security efficiency when applied to an eCertificate system, especially for an eCertificate that may contain non-static contents, and needs to be transferred to three or more parties.

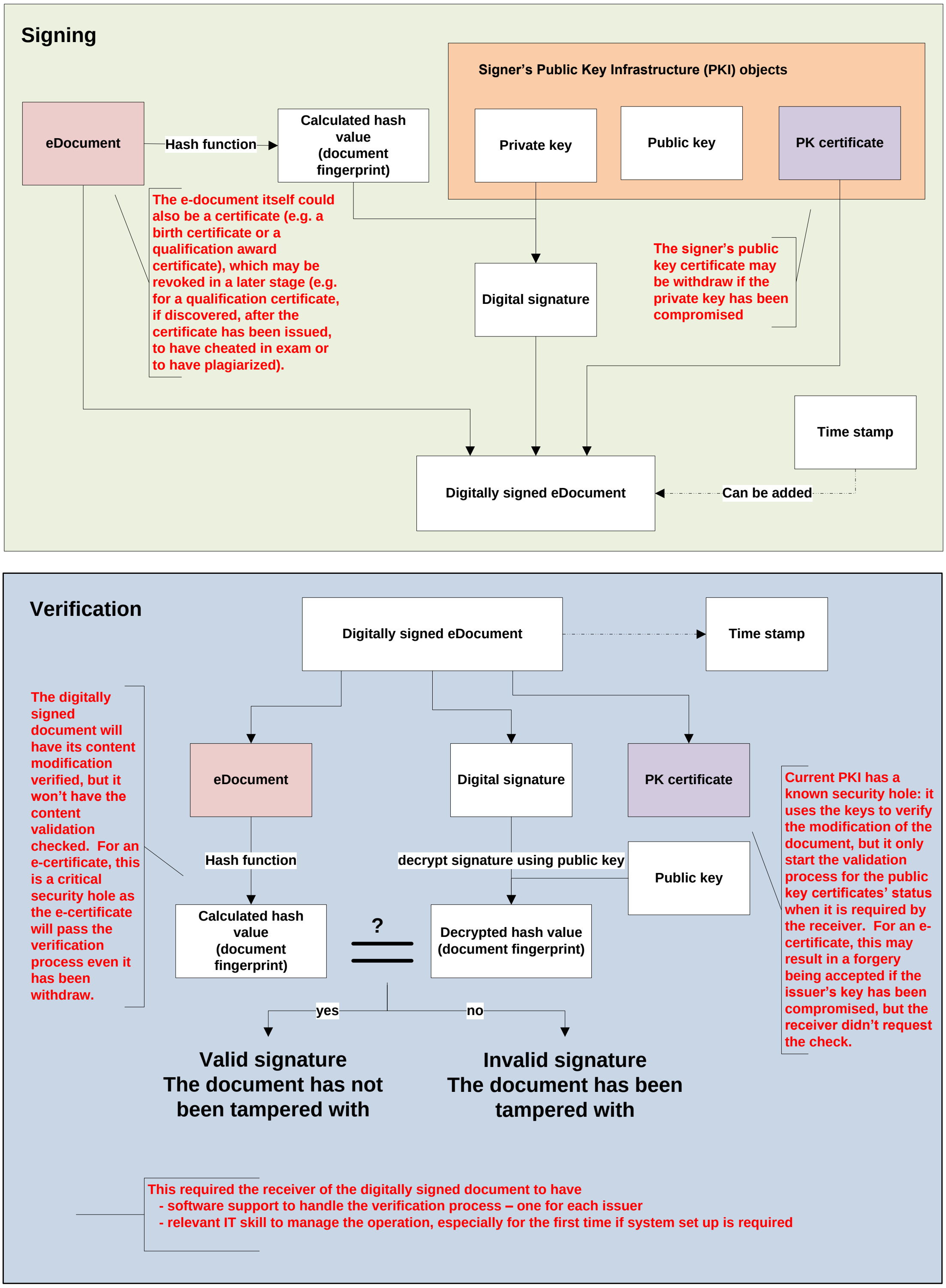
Access support & owner control: As computing technology developed, the concerns of data privacy and eDocument ownership rights intensified. It has been noted that an eDocument owner has the right to store, manage, share and track their personal data, “under their control, with their consent, and for their benefit” [133] (see 3.5 Privacy and Ownership). Unlike paper-based documents that can be presented anywhere, digitally signed eDocuments are currently based on organizations for their service support, so that the reviewer can only verify them through the organization-provided service (see 3.4.8 PKI and 3.4.9 Digital Signature Theory). Many organizations also provide access control functions for the stored eDocuments through a system to satisfy the ownership right, such as Digitary (see 4.2.3 Digitary). However, this method depends heavily on the issuing body; in the case of the eCertificate, it is inconvenient for a reviewer, who has eCertificates issued from many different organizations, to verify the eDocuments through many different systems. Moreover, anything happening to the issuing organization, e.g. going out of business, or the database being damaged, will result in the eDocument becoming invalid. This lifelong validation issue is crucial to an eCertificate as a genuine eCertificate must remain valid even if the issuing body no longer exists.

eDocument content validation: eDocument content for digital signing can present in various forms, such as Unsigned content, Signed content groups, Externally referenced content, and Dynamic content. It also portrays various content types, such as text documents, media files, and programme code. To accompany the various content types and forms, digital signature with XML syntax was defined. It has three signing methods: detached signature, enveloped signature and enveloping signature, each designed to handle the various content forms (see 3.4.10.2 Issue 2 – eDocument content validation). However, the content of an eCertificate will not solely comprise one content type or form, but a combination of them. For example, the evidence file could be the Externally referenced content, the transits file and the qualification file could become the Signed content groups, and the qualification award itself is the Dynamic content as it may be withdrawn at a later stage. What is more, there is no specification of how an eCertificate file should be structured and how it should be verified. Therefore, how to combine the different XML signing methods together to sign the various content types and forms to ensure the security and trust becomes the main technical gap that needs to be overcome.

eDocument content status validation: digital signature is most suited to sign static eDocuments, but not for eDocuments with changing status, as it only validates the eDocuments' content modification and the status of the signers' public key certificates (PKC), without validating the status of the document's actual content (see 3.4.10.2 Issue 3 – eDocument status validation). This is crucial to an eCertificate as this signed eDocument itself is also a certificate, which may have a valid period (e.g. first aid certificate), and may be revoked in a later stage (e.g. if it is discovered, after the certificate has been issued, that the student cheated in the exam or plagiarized). The problem we are dealing with is a certificate squared issue (referred to as $(\text{certificate})^2$ issue), which involves the issuer's PKC and the qualification certificate as a whole.

Auto request of signing key status validation: Current Public Key Infrastructure (PKI) does not start the validation of the public key certificates' status automatically. It will only undertake this process if required (see 3.4.10.1 Issue 1 – public key certificate status validation). In the case of an eCertificate, this is a critical security hole as it may result in a forgery being accepted if the key has been compromised.

The issues of content validation and auto request of validation are explained in Figure 5-3, after [31, 32].


Signing
Signer's Public Key Infrastructure (PKI) objects
eDocument
Hash function
Calculated hash value (document fingerprint)
Private key
Public key
PK certificate
Digital signature
Time stamp
Digitally signed eDocument
Can be added
Verification
Digitally signed eDocument
Time stamp
eDocument
Digital signature
PK certificate
Hash function
decrypt signature using public key
Public key
Calculated hash value (document fingerprint)
?
Decrypted hash value (document fingerprint)
yes
no
Valid signature
The document has not been tampered with
Invalid signature
The document has been tampered with

The e-document itself could also be a certificate (e.g. a birth certificate or a qualification award certificate), which may be revoked in a later stage (e.g. for a qualification certificate, if discovered, after the certificate has been issued, to have cheated in exam or to have plagiarized).

The signer's public key certificate may be withdraw if the private key has been compromised

The digitally signed document will have its content modification verified, but it won't have the content validation checked. For an e-certificate, this is a critical security hole as the e-certificate will pass the verification process even it has been withdraw.

Current PKI has a known security hole: it uses the keys to verify the modification of the document, but it only start the validation process for the public key certificates' status when it is required by the receiver. For an e-certificate, this may result in a forgery being accepted if the issuer's key has been compromised, but the receiver didn't request the check.

This required the receiver of the digitally signed document to have
- software support to handle the verification process – one for each issuer
- relevant IT skill to manage the operation, especially for the first time if system set up is required

Figure 5-3 Digital signing issues

5.5.4 Technical Requirements

Referring to the system requirements summarised from the domain definition and common usage pattern, the corresponding technical requirements from the use case study and gap analysis are listed in Table 5-4.

Table 5-4 Technical requirements (TR)

SR ID	**TR ID**	**Summary**
SR-01	TR-01	system adaptability and compatibility so that the system can be embedded as a plug-in within other systems, e.g. eFolio
SR-02	TR-02	Security control: include hardware, database, and network
	TR-03	system access control for students, reviewers, and any third parties
	TR-04	eCertificate access control for students, reviewers, and any third parties
SR-03	TR-05	support content modification validation
	TR-06	support withdraw of an eCertificate
	TR-07	support revocation of signing key
	TR-08	can verify and prove issuer
SR-04	TR-09	the student owner of the eCertificate can have control over who can see it and for how long, without the need of re-signing by the issuer
SR-05	TR-10	Stimulate large-scale uptake, enabling eCertificate to be widely verified and recognized throughout the UK
	TR-11	support lifetime validation, can be independent from the issuing body
	TR-12	easy to use, suits low IT skill users, both students and reviewers
	TR-13	Minimize system storage
	TR-14	Establish stakeholder trust between all involved parties

5.5.5 Chapter Summary

The eCertificate case study has identified the three stakeholders involved, and explored the issues through use cases analysis. A gap analysis against current techniques and services for such issues was carried out to discover what could be reused and what was still required. The technical requirements from the use case study and gap analysis were tabulated in line with the system requirements. These will then need to be addressed and reflected in the design of the new system.

Chapter 6 The Proposed eCertificate System

The last 2 layers of the SORM methodology are service profile and implementation. This chapter describes these two layers through the following steps: first generation of the services profile to bridge the gap, then the decisions made for the technical approaches, then the system design, and finally summary of the system implementation.

The eCertificate system development was carried out under the eCert project. The researcher was fully responsible for the whole system analysis and design while over-viewing the system demonstrator production as the eCert project manager. All sections in this chapter are the researcher's own work, expect that section 6.6 System Demonstrator includes contributions by other eCert project team members. Two workshop proposals [11, 33] and a conference paper [32] were published during the development. This work has also been published as reports on the eCert project website [28].

6.1 Service Profile

With the use cases defined and gap analysis produced, the next step in following the SORM methodology is to develop a complete service profile. Hence, techniques to tackle the issues were investigated.

6.1.1 Existing Services

Service Orientated Architecture (SOA): the eFramework, whose aim is to build a common approach to Service Oriented Architectures for education, offer greater interoperability between systems and software across the eLearning community. By adopting the eFramework SOA, the distributed stakeholder use case can then be met since the SOA provides an architecture for participation.

Digital signing: digital signatures are used in eDocuments to provide authentication, integrity, and non-repudiation. By adopting the 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 meets part of the stakeholder trust use case as the CAs provide a chain of trusted nodes.

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 [72]. This is based on SAML (Security Assertion Mark-up Language) published by OASIS, and provides a decentralized solution for institutions to share trusted user identities between each other, so that a home user identity is valid at any of the partner institutions within the federation [135]. This could provide the service for identity management of the eCertificate owners. However, such systems may need to be extended in order to associate the requirements of the eCertificate system.

6.1.2 Services Required

Stakeholder trust: Although the identities of the eCertificate owners could be addressed by adapting Shibboleth, and digital signing can provide the stakeholder trust as the CAs provide a chain of trusted nodes, we still require services to provide the trust between all stakeholders, especially when the eCertificate is transmitted further to three or more receivers, where extra care of key management and service support are involved.

Unique ID system: In order to verify eCertificates nationwide, it is necessary for the eCertificates and their owners to have unique id numbers within the system.

Access control: A privacy control service is required to enable eCertificate owners to set up controls for who can see what and for how long.

Lifetime Validation: We also need a service to deal with the Lifetime Validation issue, so that the eCertificates can be validated even if the issuing institution does not exist years later.

6.1.3 Bridging the Gap

XML Signatures: By adopting the XML signature, which combines the detached and enveloped method, using the detached signature to sign any eCertificate related support documents, and then using the enveloped signature to sign the whole eCertificate with the detached signature value embedded, will meet the assertion use case for any information involved in an eCertificate.

XML metadata: The ownership, usage, and privacy issues can be solved by generating the related information in XML metadata while employing the detached and enveloped signature methods to create an eCertificate, thereby allowing the owner to set access control to the document while retaining the integrity of the digital signature.

A timestamp can also be added with the XML Signatures to enhance its integrity.

Auto verification of CRLs: to solve the (certificate)^2 problem, the system needs 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 withdrawn. Therefore the system needs to maintain the document's revocation list as well as the signer's certificate revocation list (CRL). The system can provide a service to automatically verify the status against both of these lists, without the need to raise a request by the reviewers.

Unique number systems: Systems such as the National Insurance Number, UK unique learner number, Chinese student registration number, and US citizen number, can be adapted to form the unique student ids and eCertificate ids.

An independent system that provides a verification service for eCertificates issued throughout the UK would be ideal to solve the lifetime validation issue. However, it needs to overcome the storage and security issues, as this may require a huge memory space if the system needs to store the eCertificates issued throughout the UK, and the database that stores all these details will be a target for hackers.

6.1.4 Approaches for Meeting the Requirements

Based on the service profiles, the ideas to bridge the gap, and the technical requirements (TR) that have been covered previously in chapter 5, the Design Approaches (DA) to meet the requirements were compiled and summarised in Table 6-1. The design approaches given here are mapped to system implementation in Table 6-2 in section 6.5.

Table 6-1 Design approaches (DA)

TR ID	DA ID	Summary
TR-01	DA-01	Use XML to enable easy transaction between systems with different platforms
TR-02	DA-02	The eCertificate generation and issuing process, the hardware, database, and network security, and human control for both staff and students, will be guarded by the issuing body
TR-03	DA-03	Adapt Federated Identity system technique; access control to eCertificate system will be based on system roles
TR-04	DA-04	Access control to eCertificate will be restricted to authorized users only
TR-05	DA-05	Employ digital signing technique to support the content modification validation
TR-06	DA-06	Design a new function for eCertificate content status validation, address the unique eCertificate squared problem, support withdrawal of an eCertificate
TR-07	DA-07	Design a new function to support the auto verification of signing key CRL
TR-08	DA-08	Design a new structure for eCertificate so that it can contain the various information files while can be legally accepted and verified
	DA-09	Adapt the XML signature technique to support the verification of the various information types involved in an eCertificate
	DA-10	Employ timestamp technique to enhance the signature integrity
TR-09	DA-11	Employ XML metadata for eCertificate access control values
	DA-12	Design a new signing method that allows the modification of eCertificate metadata while maintaining the integrity of the digital signature, so that the student owner can set access control to an eCertificate without the need for re-signing by the issuer
TR-10	DA-13	Adapt SOA to provide the architecture for participation which will enable large-scale uptake
	DA-14	Adapt a national unique number system to enable the eCertificate system to be rolled out throughout the UK
TR-11	DA-15	An independent system to provide the required services
TR-12	DA-16	Provide functions with user friendly interface to deal with complicated technical requirements, such as keys management
TR-13	DA-17	Avoid storing sensitive data, minimize system storage to reduce the attraction of database attacks
TR-14	DA-18	Employ PKI to establish stakeholder trust between all involved parties

6.2 System Structure Development

Although digital signing is widely used for verifying eDocuments, it is more suitable for a “one stop” situation. When applying it to a “multiple stops” situation, a system designed is needed to handle the trust issue, such as the keys and their related security problems.

Existing systems deal with the authentication of eDocuments, such as mobile eBoarding cards, secured mailing systems and commercial eCertificate systems. However, they were built for specific purposes, and only transmit data between two parties. They do not address the security requirements involved in data transmitting between multiple parties.

6.2.1 Approach 1: Existing Transmission Process

If a digitally signed document is used to replace the paper-based document within the existing issue, distribute, and verify process path, as show in Figure 6-1, it raises many issues. The two main ones are:

- Service support to handle the digitally signed documents
    - An efficient way to prove the issue of an eDocument is to have it digitally signed. However, this requires all the receivers (the eDocument owner and all inspectors) to have service support to handle the verification process. They will need to have the relevant IT skills to manage the operation, especially for the first time if system setup is required.
    - As different institutions will use different methods to sign their eDocuments, this may require all receivers to have services for each issuing institution.
- Privacy and Confidentiality issues
    - If an inspector has the service support (with the public key) for a selected issuer, this may mean that the inspector can view any eDocuments signed

by this issuer; if these services are publicly available for inspectors (and anyone could be an inspector), this may mean that everyone can access any digitally signed documents, including stolen ones. There is no way for the users to have control over their usage. This is strictly against the confidentiality and privacy requirement.

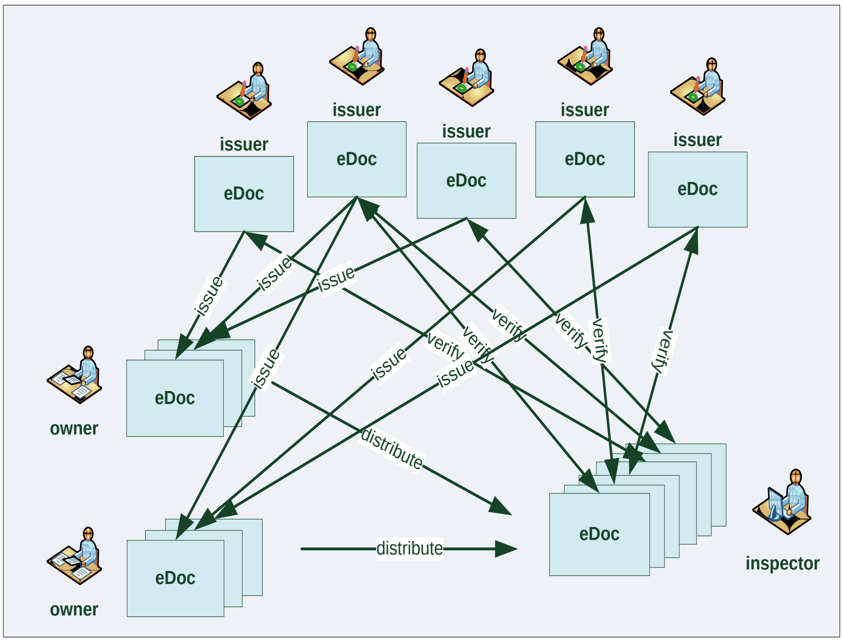


Figure 6-1 Transmitting eDocument with existing process, published in[28]

6.2.2 Approach 2: Institution Based Transmission

There could be an institution based approach, as shown in Figure 6-2, taking the Digitary system as an example.

a) eDocuments stored in the issuer’s system;

b) The issuer also provides an online support service for eDocument management and verification;

c) the owners can access the online management system to set access control for their own eDocument before sending out the link and access token to the specified inspector;

d) the inspector can access the online verification system through the link and use the access token to view, verify, and download the eDocument.

This approach addresses the privacy and confidentiality issues by setting access tokens. Therefore, the inspectors can only access those that they have the tokens for. However, some issues have arisen:

- Privacy and Confidentiality issue
  - The access token only controls the first time round. Once the inspector has accessed the online system and downloaded the eDocument, the owner will have lost control of it afterward.
- System storage
  - This approach requires huge storage as it needs to store all the issued eDocuments for a lifetime.
- Lifetime validation
  - This approach relies heavily on the institution (the issuer). Lifetime validation is a problem if the institution no longer exists.
- Security
  - The information stored is considered as high value and sensitive. The support service provides an active channel to the backend database, which could increase the risk of attacks.
- Usage
  - It is inconvenient for the inspector when eDocuments are issued from many different institutions, as shown in Figure 6-3.

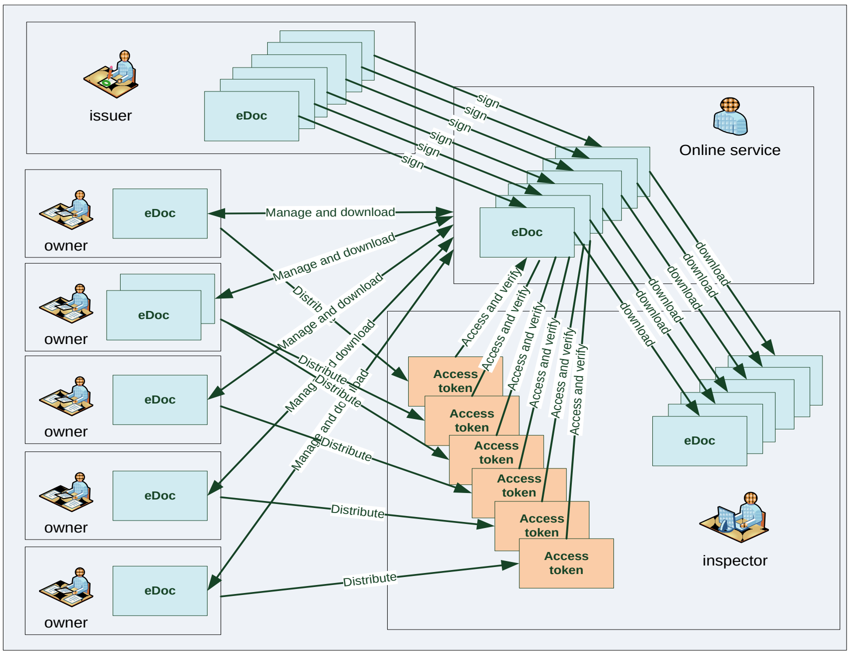


Figure 6-2 Transmitting with an institution approach, published in[28]

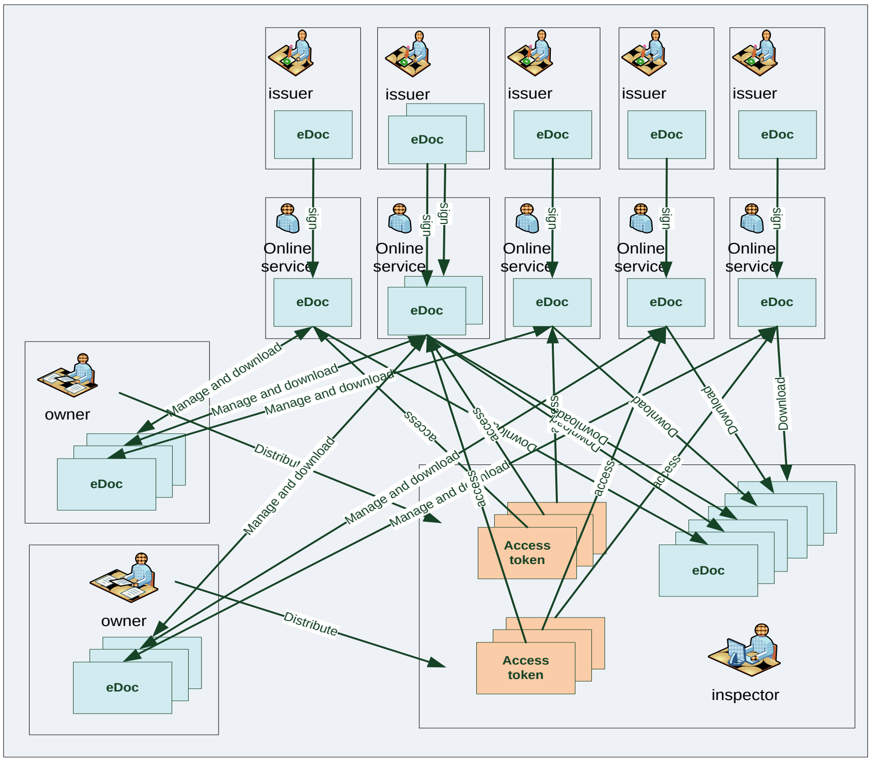


Figure 6-3 Usage issue of the institution approach, published in[28]

6.2.3 Approach 3: Central Service and Storage

Taking the Chinese system as an example, a central service approach, as shown in Figure 6-4, could be provided.

a) a central online system provides the management and verification service for all institutions that have joined;

b) all institutions issue eDocuments using the same standard, which are then uploaded 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 inspector;

d) the inspector can access the online verification system through the link and use the access token to view, verify, and download the eDocument.

Compared to the institution approach, this approach addresses the lifetime validation issue, and also solves the inconvenience problem as the inspectors only need to access one reference point for all the eDocuments. However, it requires an even bigger store, and increases the risk of database attacks as it now has a much bigger database.

- System storage
  - This approach requires huge storage as it needs to store all the eDocuments issued for a lifetime.
- Security
  - This approach stores all issued eDocuments from institutions that have joined into one backend database; the risk of being attacked is considered very high.
- Trust
  - Who will host such a system? It must be trusted by all institutions as it holds the information for all of them. The English government has a history of losing sensitive information, and in some cases, the whole database.

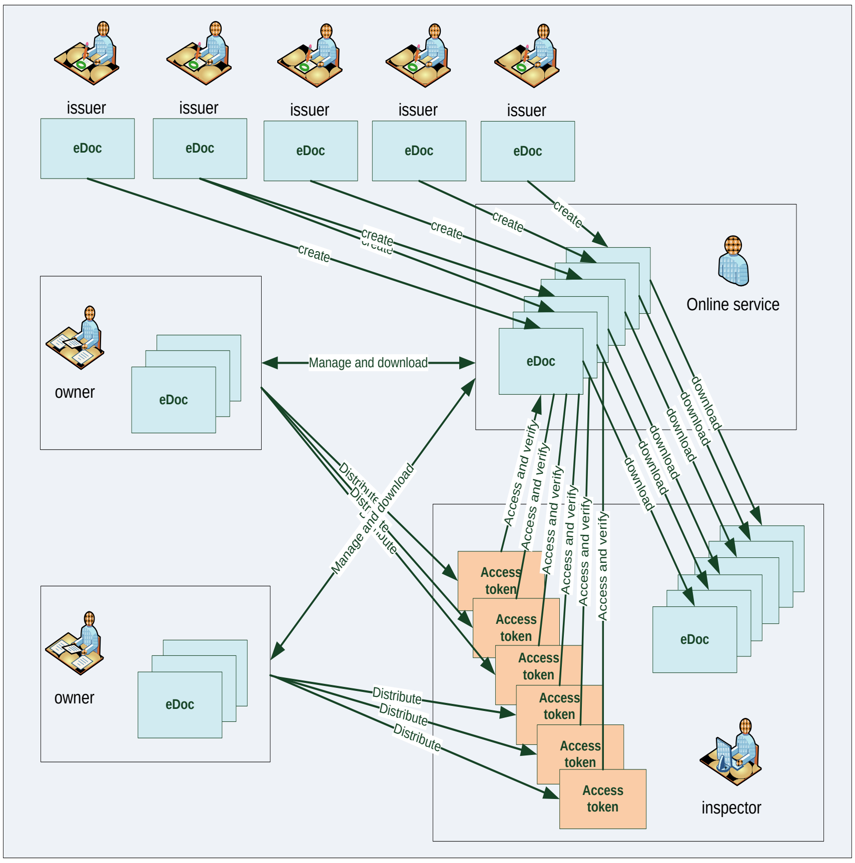


Figure 6-4 Transmitting with a central storage approach, published in[28]

6.2.4 Approach 4: Central Service Only

As the central storage in approach 3 above causes lots of problems, perhaps a central service approach without storing the eDocument in the system, as shown in Figure 6-5, would suffice.

a) a central online system provides the management and verification service for all institutions that have joined;

b) all institutions issue eDocuments using the same standard, which are then sent to the owners;

c) the owners can access the online management system to set access control of their own eDocuments before sending out to the inspector;

d) the inspector accesses the online verification system to verify the eDocument.

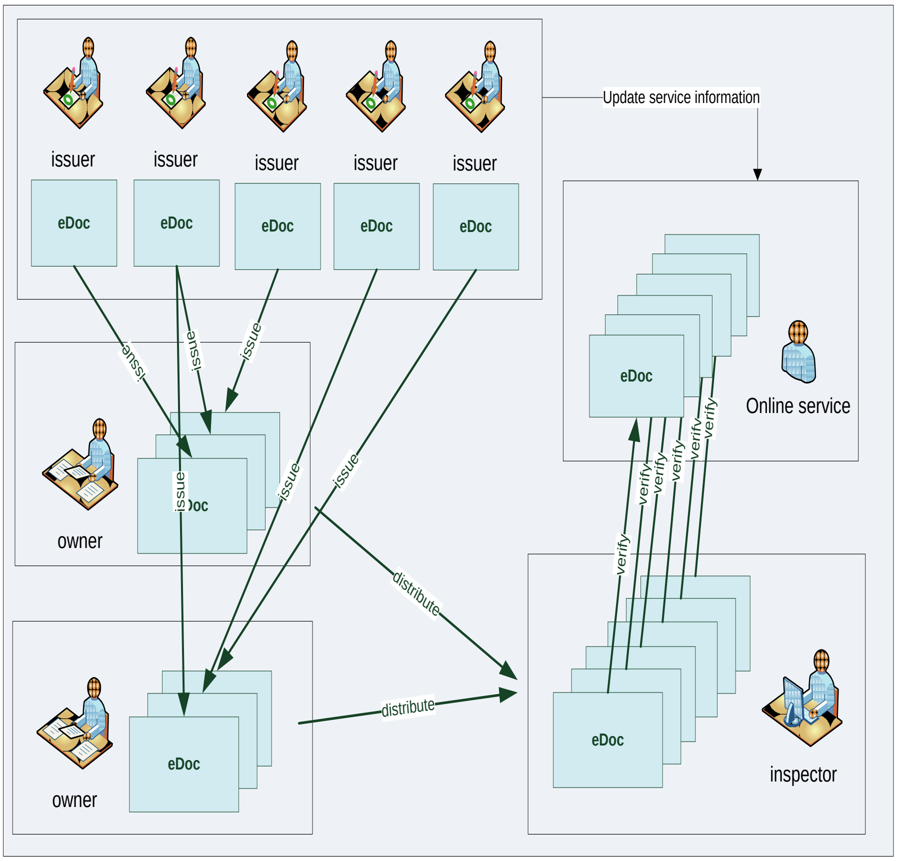


Figure 6-5 Transmitting with a central service approach, published in[28]

Compared to the approach of central service with stored eDocuments, this approach solves the three issues that the other one faced: a) it does not require storage for the eDocuments; b) the eDocuments are not stored in one system, thus dramatically reducing the likelihood of attacks; c) the eDocuments are not stored in one system, so there will be no risk of data being lost, therefore it will be much easier to find a body to run the service that everyone can agree on. However, this approach brings back the three way transmitting situation, and again face the keys management, privacy and confidentiality issues described earlier.

- Privacy and Confidentiality issue:
  - In this approach, an inspector can have service support for all issuers. If the inspector has the public key for one eDocument, he can access all eDocuments issued by that issuer. If the inspector can get hold of one eDocument from each issuer, then they can access any eDocuments,

including stolen ones. This is strictly against the confidentiality and privacy requirement.

6.2.5 The Chosen Approach

As the approach of an online central service – without storing eDocuments – meets most of the major requirements, it has therefore been selected as a basis for the system structure design.

Pros:

- System storage: it does not store eDocuments on the central system, saving huge storage;
- Security: as sensitive data is not stored in the system, many attacks can be avoided;
- Trust: The central system is only there to provide a service, as the sensitive data is not stored in the system, there will be no risk of the data being lost. People in general, do not trust any government bodies holding their personal data, so this approach makes having such a central system a possibility.
- Usage: convenient for the inspectors to access eDocuments from a wide range of issuers.
- Lifetime validation: independent central system, can validate eDocuments even when the issuer no longer exists.

Cons:

- Privacy and Confidentiality issue: an inspector can have the service support for all issuers. If the inspector has the public key for one eDocument, he can access all eDocuments issued by that issuer. If the inspector can obtain one eDocument from each issuer, then they can access any eDocuments. This is strictly against the confidentiality and privacy requirement. It is the main issue that still needs to be addressed.
- Issues noted in the gap analysis still need to be addressed.

6.2.6 The eCert System Structure Design

The proposed solution is shown in Figure 6-6.

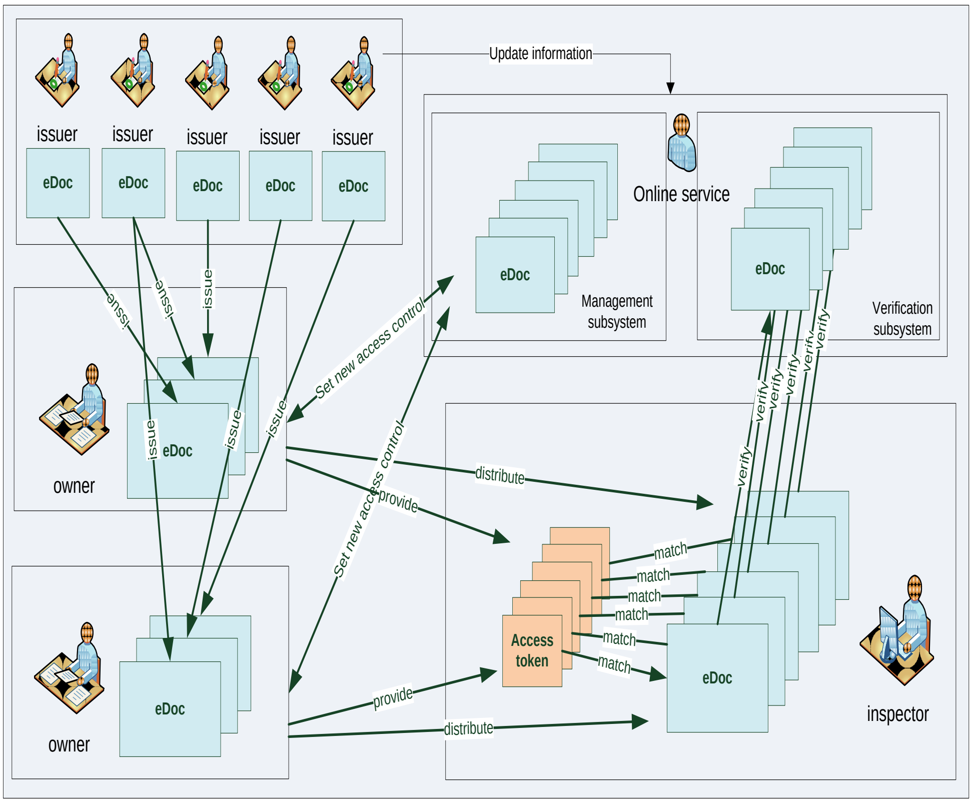


Figure 6-6 The new eDocument transmitting design, published in[28]

a) a central online system provides the management and verification service for all institutions that have joined;

b) all institutions issue eDocuments using the same standard, i.e. the document signed using the issuer’s private key, the metadata that contains the access token, and the whole XML document will be signed using the owner’s public key. The file is then sent to the owners;

c) the owners can access the online management system to set new access control of their own eDocument before sending out to the inspector;

d) the inspector accesses the online verification system to verify the eDocument.

6.3 Decisions and Assumptions

In order to secure the eCertificate system, a number of decisions and assumptions have been made.

6.3.1 SOA

The development of the system will adopt the SOA of the eFramework 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” [114]. When used with interoperable ePortfolio XML schemas, this makes it easy for any ePortfolio vendor to integrate eCertificate services into their application; hence enabling and encouraging user take up and participation between users using software from potentially different providers.

6.3.2 UK Focus

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

6.3.3 Unique Student ID and eCertificate ID

For the eCertificate system to be rolled out nationwide, a unique student ID system is required. Such an ID system can be adapted from either the UK unique learner number, or the learning record system, or the Chinese student registration number system (see 6.1.2 Required Services and 6.1.3 Bridging the Gap). However, this unique student ID system will not be investigated further in the current work phase. It is assumed that such a system has been adopted, and every student will register a unique student ID when they start studying at sixth form or college (the level that they will start to receive all sorts of qualification certificates). The version of the ID system adopted should not affect the eCertificate system provided the identities are all unique.

For the purpose of this study, a simple and self maintained numbering system was used, and every eCertificate issued would also have unique eCertificate ID associated with the student ID. The version of the ID system should not affect the eCertificate system as long as all IDs were unique within the system. The rules for the unique student ID and eCertificate ID are:

- Every student will only have one unique lifelong student ID nationwide
- Every eCertificate that the student achieves will contain this student ID along with the eCertificate ID as proof of ownership
- Student : student ID → 1 : 1
- Student ID : eCert ID → 1 : many

6.3.4 Security Control by the Issuing Institution

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 bogus 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.

It is assumed that only authorized issuers from the registered education institution can access the issuing system and the student record database. Such staff control and database security will rely on the institutions' security policy, and not be investigated further here even it is related.

6.3.5 Ownership Control

To ensure that the eCertificate owner has the right to control who can see what and for how long, the system will allow the owner to set controls on their eCertificates. This will include an option for the display content, display time limit, and who can have access to the controlled eCertificate.

6.3.6 Solving the eCertificate Squared Problem

The eCertificate squared problem described in the gap analysis will be dealt with by maintaining a eCertificate revocation list as well as the signer's public key certificate revocation list (CRL). The system will verify both of these revocation lists every time an eCertificate is accessed.

6.3.7 Students' Unique Keys vs systems' Default Key

Encryption can be used for access control of the onward distributed eCertificates after they are issued, so that only the reviewers with the corresponding decrypt keys can have access.

At first, it was decided that every student would receive a key pair when they register for a student ID, and all institutions will use the student's public key to encrypt the eCertificates when issued, so that the privacy issue could be addressed, as only the student with the corresponding private key can access them. This is shown in Figure 6-7.

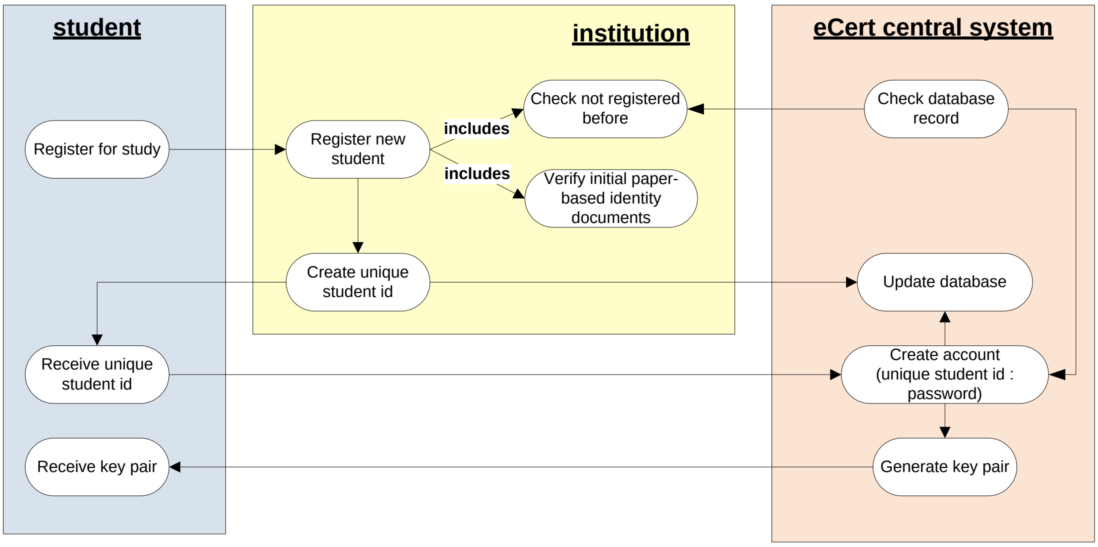


Figure 6-7 Registration, published in[28]

However, it was finally decided to use a system default key rather than unique personalised student keys for encrypting the initial eCertificates. The reasons are:

- Using a default key makes open access possible, as eCertificate owners may like their eCertificates to be open access in some situations,
- Considering that keys are likely be forgotten at some point, creating eCertificates using students' personal keys may end up with their initial eCertificates becoming inaccessible.
- The eCertificate owners can always set access control to the initial eCertificates through the management system when needed.

To enable this, the initial issued eCertificates must only be accessible by their owners during the issuing process. Therefore, the design decision was that the initial eCertificates would be encrypted with a default key, and saved under the corresponding student's account, so only the owner can have access. The eCertificate can be encrypted with a personalized key through the management system before sending to the reviewer.

6.3.8 Federation Management vs. eCert System Management

To ensure that only the eCertificate owner can change the access value to their own eCertificates but no-one else, a system login for access control is required.

There are two options: a) adopt a federation identity management system, with eCert as part of the education institution federation, passing the student ID and password to its identity management system for access control; or b) eCert maintains its own access control system with a student ID and system password.

Many projects are currently running in the area of identity management under the Access and Identity Management Programme by JISC, such as login for life, Identity management toolkit, and Service-Oriented Federated Authorization (SOFA)[12]. As a result, it is difficult to pick a suitable one before these projects are completed. However, login access control to the eCert system is not the main issue that the eCert

[12] http://www.jisc.ac.uk/whatwedo/programmes/aim.aspx

project needs to address. Investigating these identity management solutions would require considerable time, so it was decided that the eCert system would have an in-built access control system, and would defer investigation of a suitable federation identity management system to future work.

6.3.9 Starting Point

Every institution will have different attribute names in database tables, and may be using different methods to collect the required information when forming a paper-based certificate. So that the eCert system can easily fit into any institution, the eCert system will let the institution form the base of the award qualification file using their existing methods, and take over from for the stage at which the paper-based certificate is ready for printing, and from that, set links to collect any required information. This should simplify the configuration of the system setup when it is installed.

It is assumed that the database has the required information fields ready for the eCertificate issuing process. Any missing fields can be created and unmatched field names can be configured at the system set up stage:

- student's name
- student ID – a unique learner ID nationwide
- student record
  - department
  - course / qualification title
  - academic year
  - qualification status (pass/fail)
- print-ready qualification award file,
- qualification transcript file
- assessment evidence file
- qualification award information
  - department / exam board
  - qualification title
  - level (first/2:1/2:2/third/A/A+/…?)
  - date of award

  - expiry date of award (when recertification is required)
- on system configuration
  - match the required field names
- signer’s information
  - signer’s ID
  - signer’s name
  - signer’s public key certificate

6.4 Core Design

The system design focused on four areas: the eCert file structure, the system structure, the signature method, and the authentication and verification processes.

6.4.1 Systems and Relationships

The eCertificate system (eCert) will be constructed in two parts: an issuing system and an online central system.

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 eCertificates issued from any involved institutions, and will be the single reference point nationwide. This will prevent confusion to reviewers of not knowing which system to choose or which can be trusted, especially when they have large numbers of eCertificates issued from different institutions. This will also have the advantage of having close monitoring and control against bogus systems.

The issuing system will be installed at individual institutions. The institution creates and issues digitally-signed and access-controlled eCertificates to the specified students through the local issuing system. The students view and set new access controls on the received eCertificates through the central management system before sending them out to further reviewers. The reviewers use the central verification system to view and verify the access-controlled eCertificate. This is shown as a use case diagram in Figure 6-8. The procedure for the issue, distribution, and verification processes between the stakeholders and the service support systems is shown as a sequence diagram in Figure 6-9.

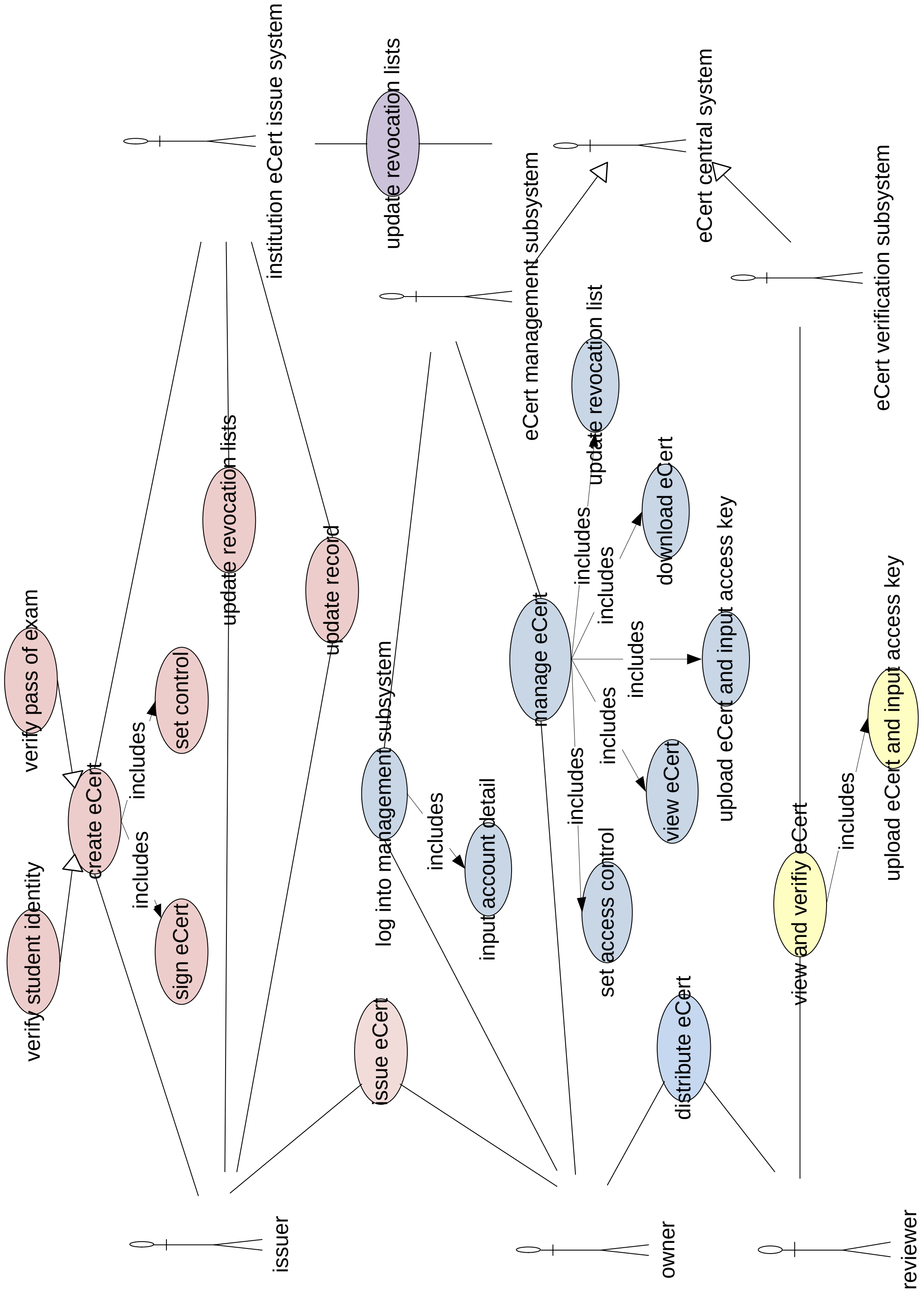


Figure 6-8 eCert system design in use case diagram, published in[28]

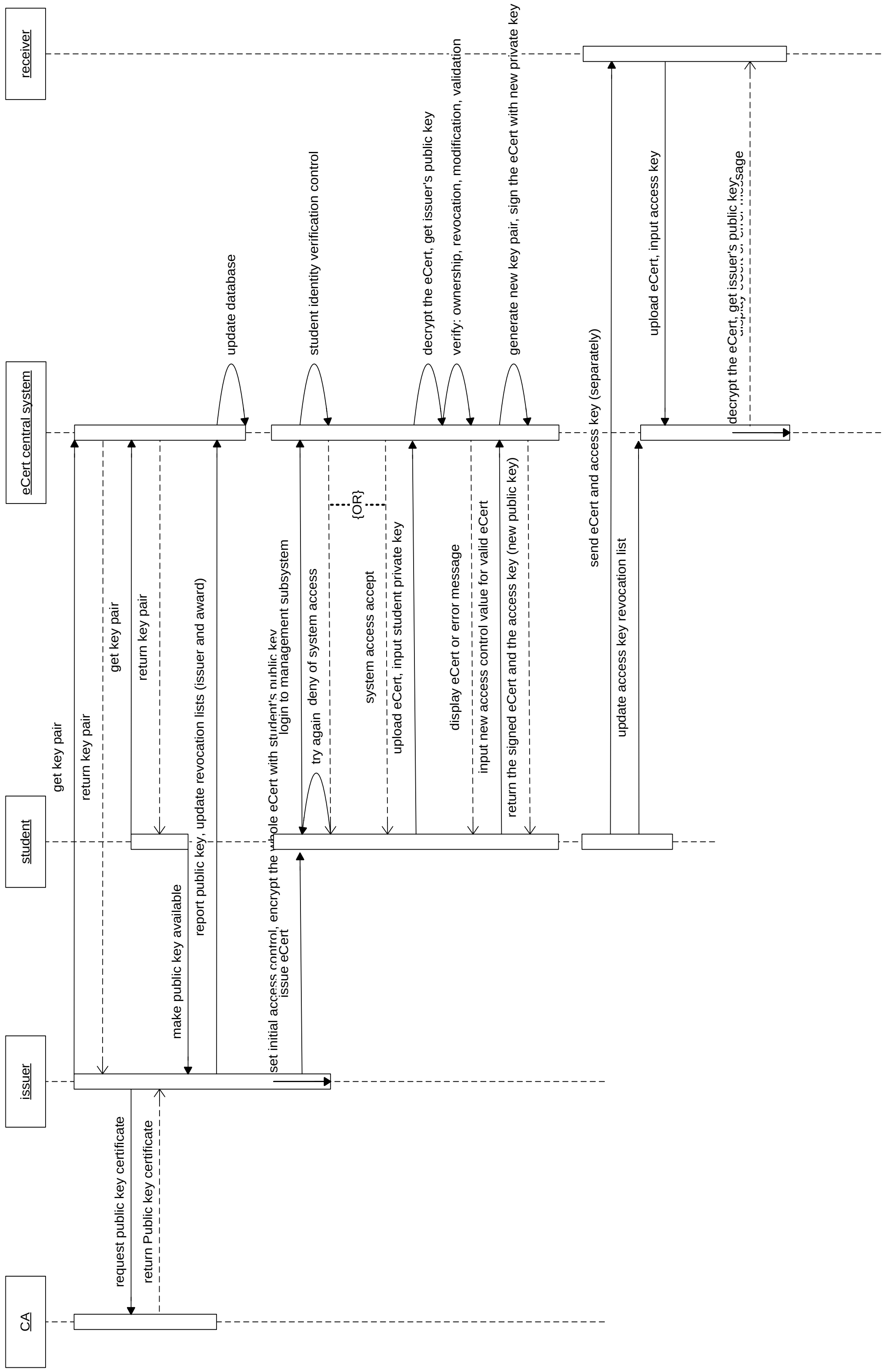

receiver
eCert central system
student
issuer
CA
get key pair
return key pair
get key pair
return key pair
make public key available
report public key, update revocation lists (issuer and award)
update database
request public key certificate
return Public key certificate
set initial access control, encrypt the whole eCert with student's public key
issue eCert
login to management subsystem
try again
deny of system access
student identity verification control
{OR}
system access accept
upload eCert, input student private key
decrypt the eCert, get issuer's public key
display eCert or error message
verify: ownership, revocation, modification, validation
input new access control value for valid eCert
generate new key pair, sign the eCert with new private key
return the signed eCert and the access key (new public key)
send eCert and access key (separately)
update access key revocation list
upload eCert, input access key
decrypt the eCert, get issuer's public key
display eCert or error message

Figure 6-9 eCert system design in sequence diagram, published in[28]

6.4.2 File Structure

An eCertificate will contain three files: a qualification award file, providing qualification award details that a paper-based certificate would offer; a transcript file, providing the related course and institution information so that the qualification can be clearly understood; and any evidence files if applicable, providing the information that the assessment was based on. An evidence file can be in any format, and can be seen as proof of the skill as it is bound with the awarded qualification. An eCertificate file will be a compressed file of these three files with their access metadata, and the signers' signature information.

To ensure that the eCertificate owner has the right to control the usage of the document, the transcript file and the evidence files will be set as optional for display, while the qualification award file will be compulsory at all times. The system will enable the eCertificate owner to select the preferred section(s) and set an access time limit for individual reviewers to best fit their various purposes. The metadata will contain the section display values and access time limit, as well as the eCertificate ID, student ID, and certificate expiry date. The section display values for the transcript file and the evidence file will be set to *true*, and the access time value will be set to *unlimited* by default on issue. All values in the metadata will be verified, and the eCertificate will be regarded as invalid if it fails to pass any of the verification processes. The controlled eCertificate will be encrypted individually, so that only the person with the given corresponding decryption key can access it.

6.4.3 The eCert Signature

Simple digital signatures are not secure enough for signing the eCert file due to their special file structure.

With the traditional method, an enveloped signature can be used to sign the qualification award file, and the detached signature can be used to sign the attached transcript file and evidence file. However, by using this method, individual sections can be swapped with, for example, another piece of better work by a classmate, and signed by the same issuer. This is shown diagrammatically in Figure 6-10.

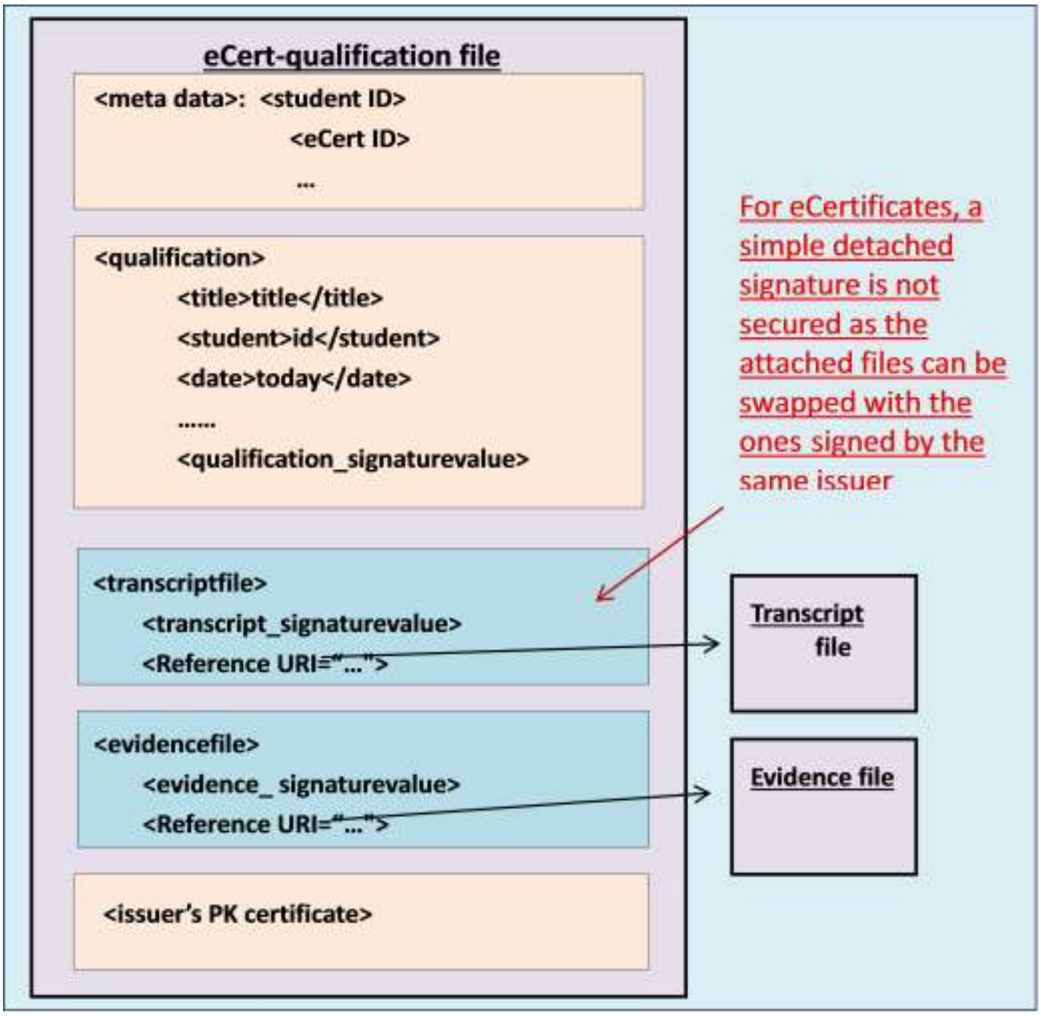

eCert-qualification file
<meta data>: <student ID>
<eCert ID>
...
<qualification>
<title>title</title>
<student>id</student>
<date>today</date>
......
<qualification_signaturevalue>
<transcriptfile>
<transcript_signaturevalue>
<Reference URI="...">
<evidencefile>
<evidence_ signaturevalue>
<Reference URI="...">
<issuer's PK certificate>
For eCertificates, a simple detached signature is not secured as the attached files can be swapped with the ones signed by the same issuer
Transcript file
Evidence file

Figure 6-10 Issues when applying traditional signature method directly

Furthermore, digitally signed documents are not editable after they are issued, not even by their issuer or owner; any modification will be detected. This is not suitable for the eCertificate as the owner would like to set controls on their distributed documents.

The system will employ a new signing method, the eCert signature, to ensure the integrity of the digitally signed eCertificate, so that the eCertificate can have the attached files securely bound together. Any unauthorized modification will be detected during the verification process, while it allows access control values to be changed and still claimed to be valid. This method will combine the detached signature and the enveloped signature, with the condition statements to meet the specified eCertificate situation, as shown in the code below.

```
<metadata>
    <access time limit>,
    <transit_visible = 1>,
    <evidence_visible = 1>,
    ......
    ......

<qualification>
    <student ID>,
    < eCert ID >,
    <eCert time limit>,
    ......

    if <transcript_visible = 1> then validate the signature
        <transitfile>
            < transcript_signaturevalue>
            <Reference URI="…">
    if <evidence_visible = 1> then validate the signature
        <evidencefile>
            < evidence_ signaturevalue>
            <Reference URI="…">

    <qualification_signaturevalue>
```

Using this method, any changes to the signed content, either the qualification section, the transcript section, or the evidence section, will be detected; the owner controlled access values can be changed in the metadata; the optional file will not be attached within an eCert file if it is set to 0 (representing non-display). This can minimise the transfer file size while the signed document remains valid as the system will only carry on to verify and display the optional section if the condition in the metadata is met, such as the display value set to 1 (representing display). The file structure of an eCertificate is described diagrammatically in Figure 6-11.

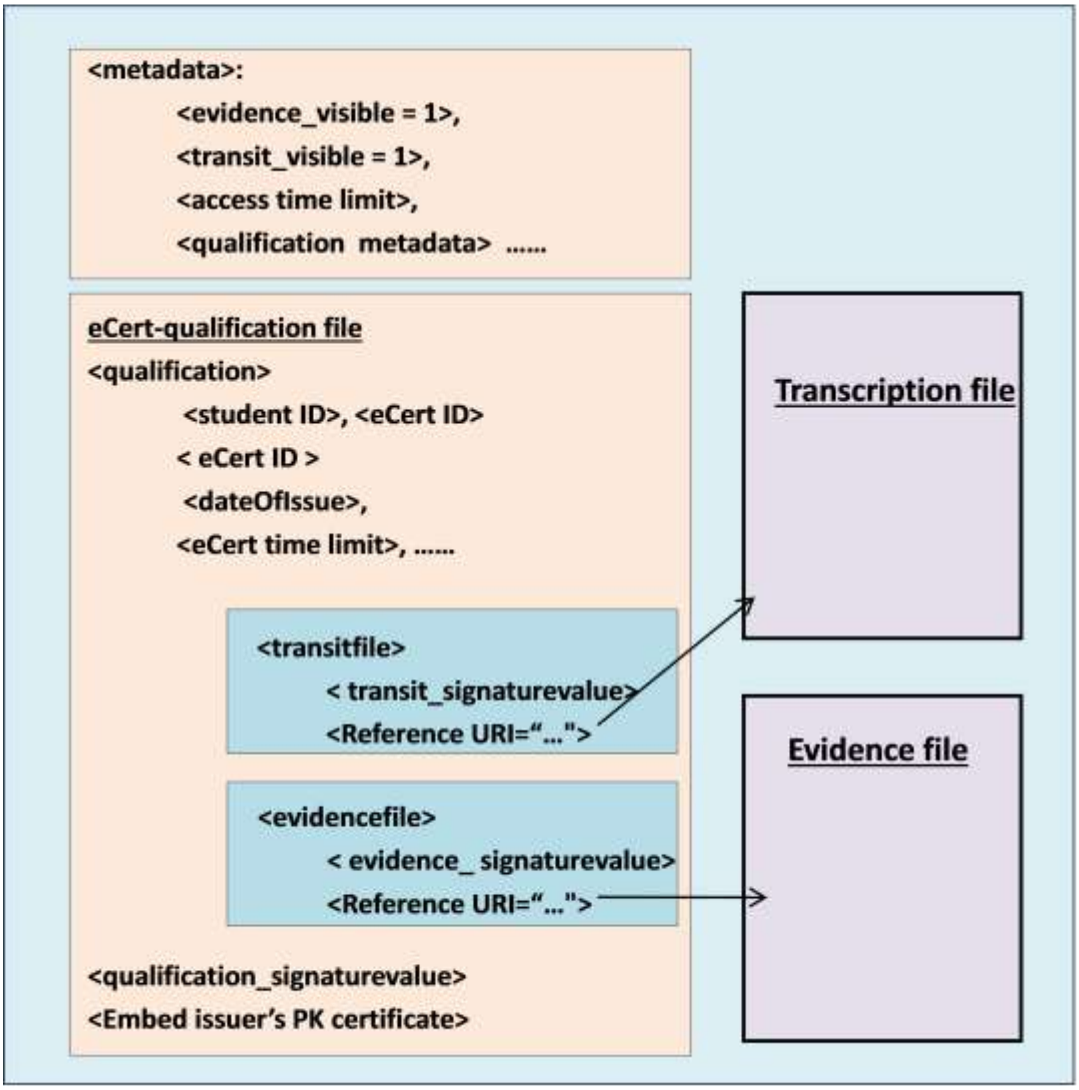


Figure 6-11 eCertificate file structure design

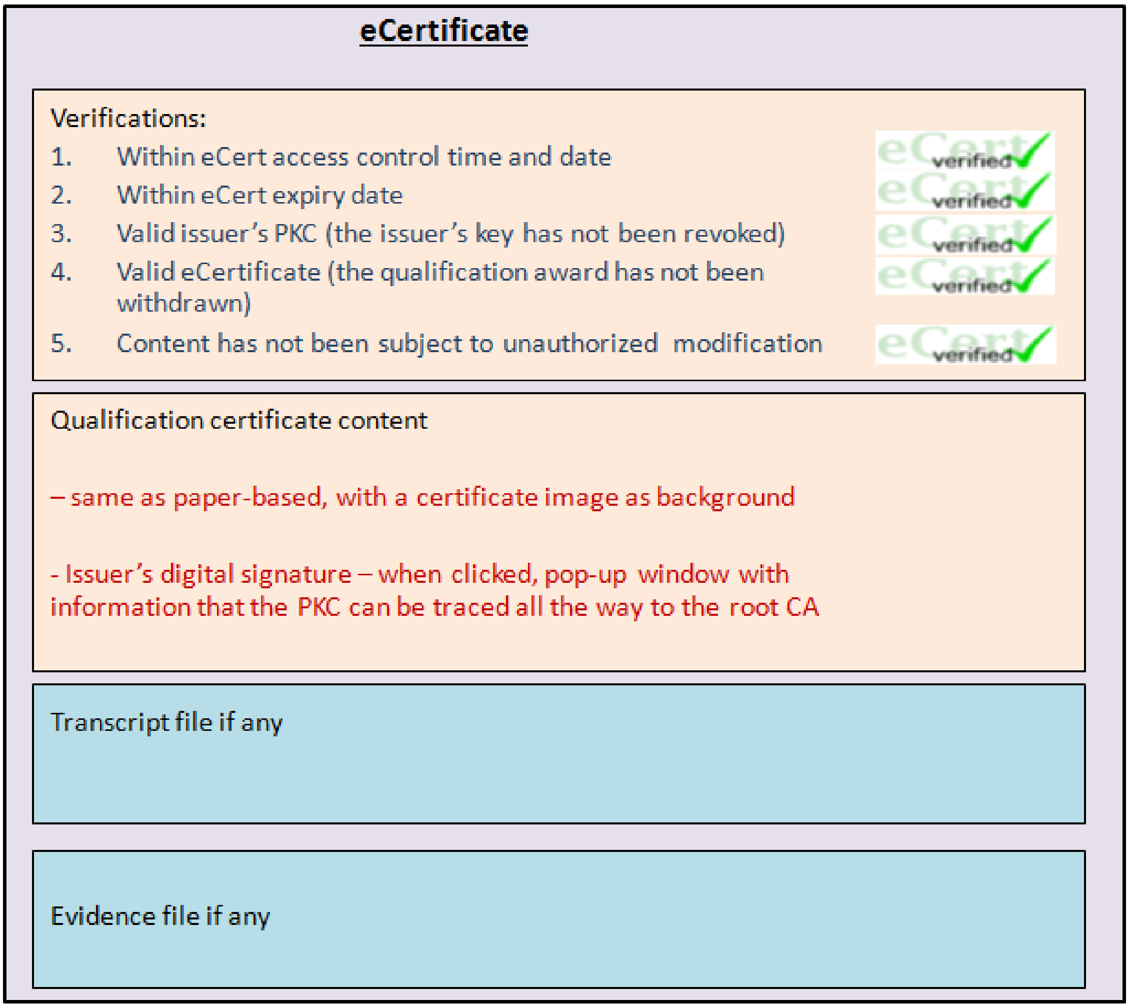
6.4.4 System Authentication and Verification

The management system is for students to view and / or set new access controls on their eCertificates. To ensure only the owner can set controls on their own eCertificates but not other receivers, the management system will require a login control. This will consist of a combination match of the student ID and system password. The management system will verify the login student ID against the uploaded eCertificates.

The system will verify the embedded information in an eCert file every time it is accessed; failure of any single checking process will result in denial of access. These verification processes include:

- Validate eCert access control time and date
- Validate eCert validation date
- Validate issuer's PKC against CRL
- Validate eCert status against eCert CRL
- Verify eCert ownership: eCert ID = login ID
- Verify content modification for the qualification section
- Verify content modification for the transcript and/or evidence section(s), if the corresponding visible setting = 1

The actual interface of a valid eCertificate will contain the three files as well as the verification result. The qualification award file will use a corresponding certificate image from the institution's system as background to maintain the interface of a paper-based certificate. It will contain the digital signature(s) of the signer(s). When the signature is clicked, the system will display a pop-up window with the information that the PKC can be traced all the way to the root CA. It is shown in Figure 6-12 .



eCertificate

Verifications:

1. Within eCert access control time and date — eCert verified ✓
2. Within eCert expiry date — eCert verified ✓
3. Valid issuer’s PKC (the issuer’s key has not been revoked) — eCert verified ✓
4. Valid eCertificate (the qualification award has not been withdrawn) — eCert verified ✓
5. Content has not been subject to unauthorized modification — eCert verified ✓

Qualification certificate content

– same as paper-based, with a certificate image as background

- Issuer’s digital signature – when clicked, pop-up window with information that the PKC can be traced all the way to the root CA

Transcript file if any

Evidence file if any

Figure 6-12 The interface design of a verified eCertificate, published in [31]

6.5 The Proposed System

The implementation of the proposed eCert system is summarised in Table 6-2 and is described in detail in the following sections: from its creation, issue, distribution, management to authentication and verification.

Table 6-2 System implementation (SI)

DA ID	SI ID	Summary
DA-01	SI-01	The system was developed using XML to enable easy transition between systems with different platforms.
DA-02	SI-02	The security control of hardware, database, and network for the eCertificate generation and issuing processes is handled by the issuing institution.
DA-03	SI-03	As explained in the Federation Management vs. eCert System Management section, an in-built access control system was implemented instead of a federated identity system.
	SI-04	Based on their system role, only authorized staff can access the issuing system and only authorized students can access the management system, but everyone can access the verification system.
DA-04	SI-05	Students can only set controls on their own eCertificates through the management system.
	SI-06	Only reviewers with the correct access key can access the corresponding eCertificate.
DA-05	SI-07	Traditional digital signing technique is used as the foundation of the signing process to support the content modification validation.
DA-06	SI-08	Taking the signing key CRL as an example, a new qualification CRL was created and its validation process was added to the traditional digital signing process to solve the eCertificate squared problem.
DA-07	SI-09	A function was added to call for the verification of the signing key and display the result every time an eCertificate is accessed.
DA-08	SI-10	A new file structure for eCertificate was defined, which contains all elements that a paper-based certificate has, as well as the new elements that meet the eCertificate and ePortfolio requirements, such as the evidence file.
DA-09	SI-11	The XML signature has been adopted with a new wrapping method for the various file types in the eCertificate to increase the signature security in the verification process.

DA ID	SI ID	Summary
		A timestamp has been added to the signature so that an eCertificate will be digitally signed, with certified signature time, and therefore tamper evidence and non-repudiation criteria are met.
DA-10	SI-12	Owner controlled access token, display sections, and access time limit values have been placed in metadata.
DA-11	SI-13	A new signing method, eCert signature, has been implemented, which allows eCertificate owners to modify the metadata of a signed eCertificate without invalidating the signature.
DA-12	SI-14	The system was implemented with SOA.
DA-13	SI-15	Standards and policies have been set up for all institutions which use the system.
	SI-16	As explained in the Unique Student ID and eCertificate ID section, a self-maintained numbering system was implemented.
DA-14	SI-17	An online centre system has been implemented to provide eCertificate management and verification services. As the newly designed file structure and signing method enables the modification of access control values without re-signing, the system can be used independently from the issuers (with the last updated CRLs).
DA-15	SI-18	Support functions have been implemented to handle the complicated requirements from the back end, such as signing and key management; therefore, front end web user friendly interface development can easily be set up by using the support functions.
DA-16	SI-19	The system only provides the service, as no personal sensitive information is stored, only storing the CRLs for validation purposes.
DA-17	SI-20	As the implementation is based on traditional digital signature, the PKI is maintained to provide trust between the stakeholders.
DA-18	SI-21	The system was developed using XML to enable easy transition between systems with different platforms.

6.5.1 System Overview

An overview of the system design is shown in Figure 6-13.

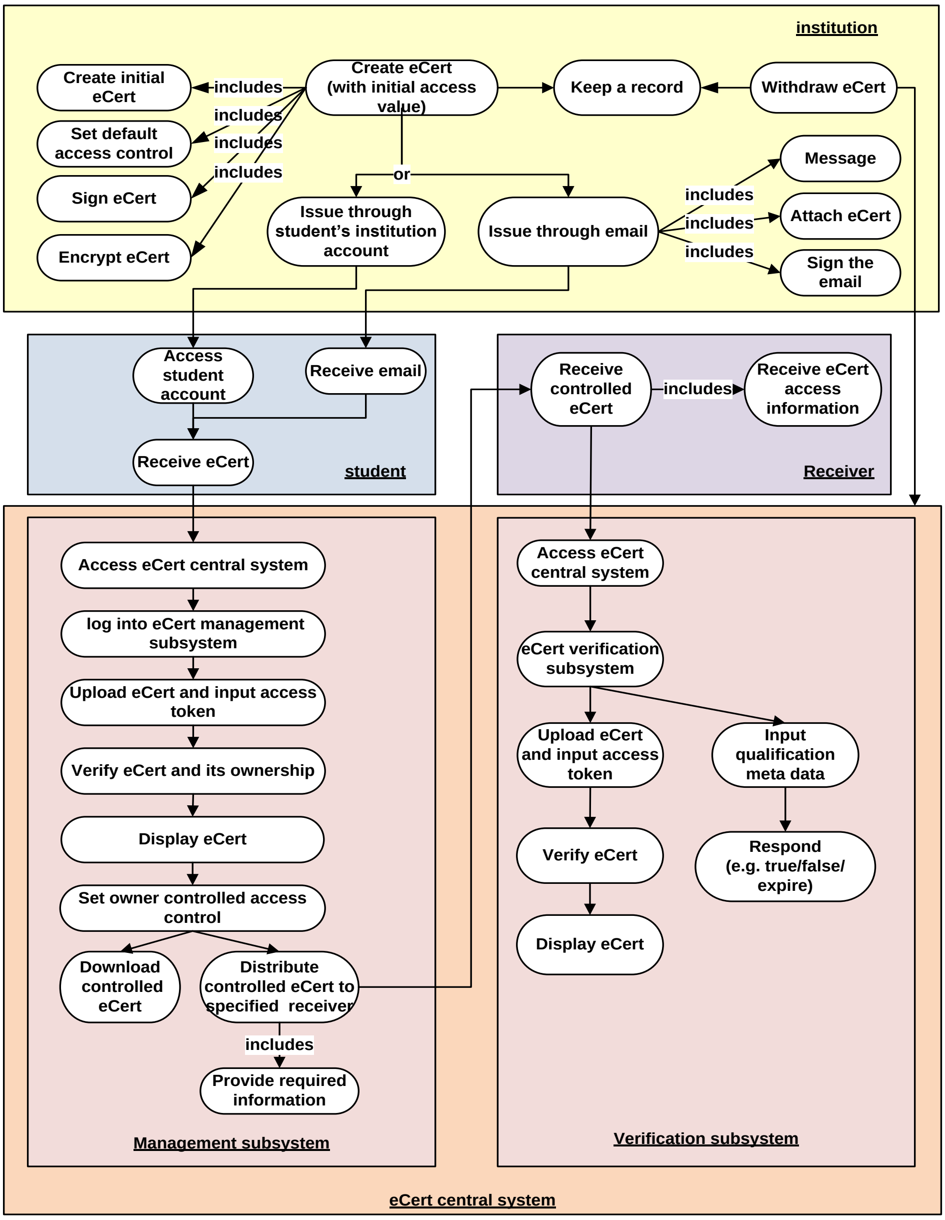

institution
Create initial eCert
includes
Create eCert (with initial access value)
Keep a record
Withdraw eCert
Set default access control
includes
includes
includes
Sign eCert
Encrypt eCert
or
Message
Issue through student's institution account
Issue through email
includes
includes
includes
Attach eCert
Sign the email
Access student account
Receive email
Receive eCert
student
Receive controlled eCert
includes
Receive eCert access information
Receiver
Access eCert central system
log into eCert management subsystem
Upload eCert and input access token
Verify eCert and its ownership
Display eCert
Set owner controlled access control
Download controlled eCert
Distribute controlled eCert to specified receiver
includes
Provide required information
Management subsystem
Access eCert central system
eCert verification subsystem
Upload eCert and input access token
Input qualification meta data
Verify eCert
Respond (e.g. true/false/ expire)
Display eCert
Verification subsystem
eCert central system

Figure 6-13 System overview, published in [11, 28, 29, 31]

6.5.2 Creating an eCertificate – the Issuing System

The process of creating eCert will be carried out through the issuing subsystem, which will be installed locally at the authenticated institution.

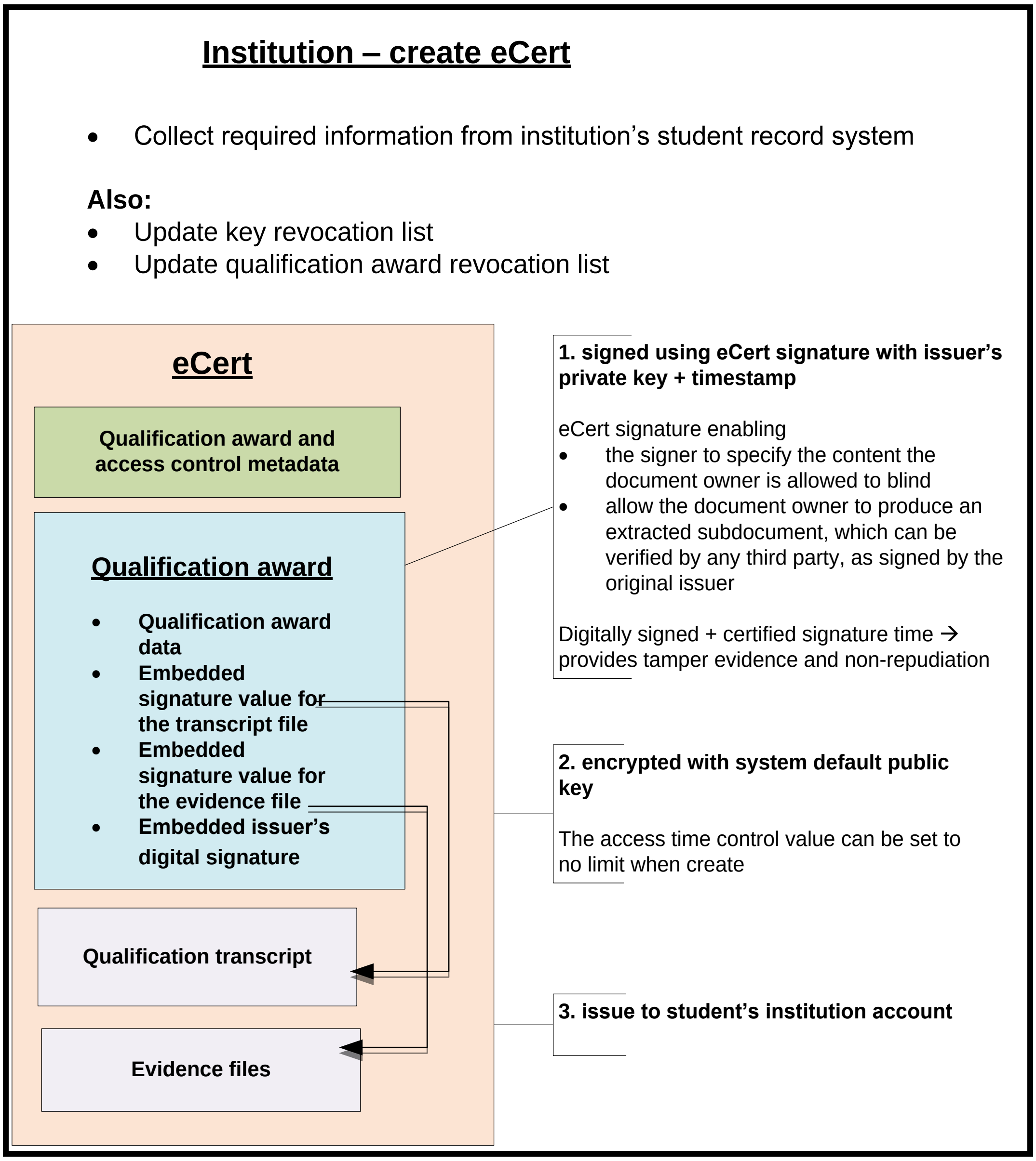

Institution – create eCert
Collect required information from institution's student record system
Also:
Update key revocation list
Update qualification award revocation list
eCert
Qualification award and access control metadata
Qualification award
Qualification award data
Embedded signature value for the transcript file
Embedded signature value for the evidence file
Embedded issuer's digital signature
Qualification transcript
Evidence files
1. signed using eCert signature with issuer's private key + timestamp
eCert signature enabling
the signer to specify the content the document owner is allowed to blind
allow the document owner to produce an extracted subdocument, which can be verified by any third party, as signed by the original issuer
Digitally signed + certified signature time → provides tamper evidence and non-repudiation
2. encrypted with system default public key
The access time control value can be set to no limit when create
3. issue to student's institution account

Figure 6-14 Signing an eCert

All certified institutions are required to use the same standards and methods, so that the issued eCertificates can be verified by the central system nationwide. All eCertificates will be in XML format, and provide information such as "valid time" and "issue time" to meet the requirements of re-certification, revocation, and deal with future software update issues. Every eCertificate will have access control values e.g. who can see it and for how long. This is to keep control of the distributed eCertificates, protect the students' privacy, and prevent any unauthorized use in the future. All eCertificates will be digitally signed using the newly designed eCert signature. Here, techniques such as timestamp will be used.

Overview of an eCertificate signing process is shown in Figure 6-14. The detailed process is described below.

- Take selected issuing target (for who, or for which group) from input
  - Option1: for issuing an eCertificate to a specified learner
    - student ID
  - Option2: for issuing eCertificates to a specified group of learners
    - department (dropdown list)
    - course / qualification title (dropdown list)
    - academic year (dropdown list)
    - qualification status (dropdown list)
- Retrieve the data from database
  - Use the input, collect the required information of the learner(s)
    - student's name
    - student ID
    - print-ready qualification award file
    - qualification transcript file
    - assessment evidence file
    - department / exam board
    - qualification title
    - level
    - date of award
    - expiry date of award (when re-certification is required)
    - corresponding background image and logo
    - email address

    - Display error message if a print-ready qualification award file for the specified learner, or anyone in the specified group, is not found
- Collect the signing information
    - Provide a button for browsing and uploading the signer's private key
    - Collect and authenticate the signer's ID and password to ensure they are correct and belong to an issuer, before allowing upload the signing key
    - Use the ID to get the signer's name and public key certificate from the database
    - The system needs to be able to uptake more than one signer
    - For security reason, the private key should be kept in a removable device when not in use
- Create the eCertificate
    - In the qualification file, set display control for the transcript file and evidence file: if visible value = 1, and use detached signature to sign the files;
    - Prepare for the verification, only verify the signature when the file is selected and included
    - Embed signer's PK certificate within the qualification file
    - Use enveloped signature to sign the qualification file
    - Generate an unique eCertificate ID nationwide
        - E.g. Institution code + course code + year + student ID + certificate code
    - Set the metadata for the signed qualification file (outside the signed section! So change of access value will not break the integrity of the digital signature)
        - student ID
        - eCertificate ID
        - eCertificate expiry date
        - eCertificate access time limit – get the specified time from database if it exists, set to no limit by default on issue
        - visible option value of the transcript file – set to 1 by default on issue, for use when changing access control
        - visible option value of the evidence file – set to 1 by default on issue

  - Wrap the 3 files, the transcript file, evidence file, and the signed qualification file with meta data into one folder
- Compress all sections (the 3 digitally signed files, PKC, meta data),
- Encrypt the file with a default private key

Encryption will be used for access control of the distributed eCertificates, so that only those reviewers with the corresponding decrypt keys can have access.

Reasons for using a default key rather than unique personalised keys for the initial eCertificates are as follows:

  - Using a default key makes open access possible, as eCertificate owners may like their eCertificates to be open access in some situations. Owners can set access control to their eCertificates when needed. To enable this, it should be ensured that the initial issued eCertificates will only be accessible by their owners during the issuing process.
  - Keys are likely be forgotten at some point, creating eCertificates using students' personal keys may end up with their initial eCertificates becoming inaccessible.

Therefore, it was decided that the initial eCertificates will be encrypted with a default key, and saved under the corresponding student's account, so only the owner can have access. The eCertificate can be encrypted with a personalized key through the management system before sending to the reviewer.

- Name the encrypted file with a unique eCert ID generated by the system, and end with a file extension of "ecert" plus the technical version code, e.g. abc12345.ecert01. The technical version code will be used for selecting the correct services during the verification process, in preparation for technical updates in the future.

6.5.3 Issuing an eCertificate

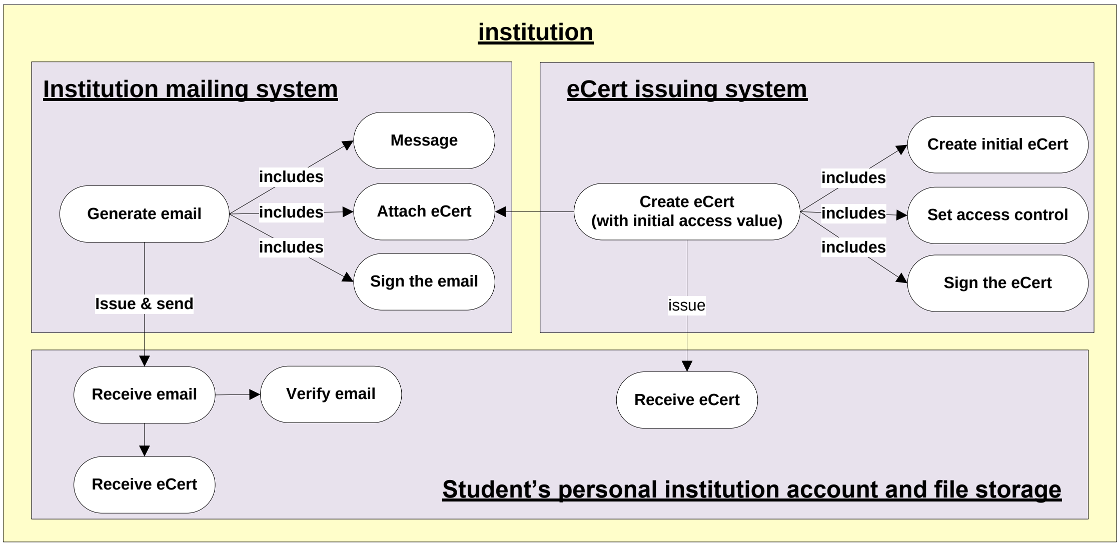


Figure 6-15 Overview of the eCertificate issuing process

The system will issue the eCertificate to the corresponding student's institutional account. In addition, the system can send the eCertificate to the specified student through its internal email system which supports secure mailing functions. This email can also be signed, so that the email will be verified when received, and the sender's certificate can be traced.

The overview of an eCertificate issuing process is shown in Figure 6-15. The detailed process is described below.

- Issue eCertificate to learner
    - option 1:
        - save the eCertificate under the learner's institution account for the student to download
    - option 2:
        - get issuer's mailing message from input
        - get the student's corresponding email address from the database
        - email to the student through a secure mailing system

6.5.4 Setting Control on an eCertificate – the Management System

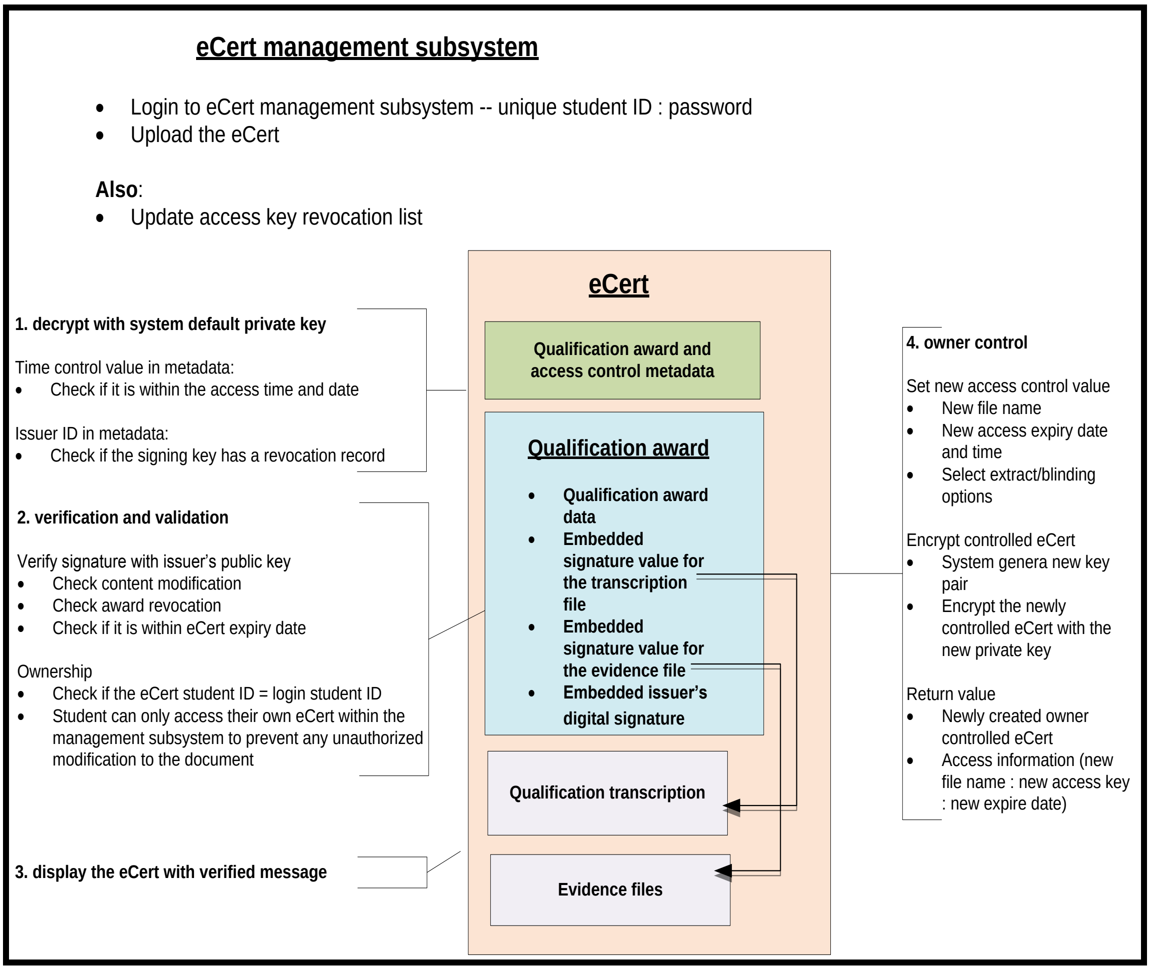

eCert management subsystem
• Login to eCert management subsystem -- unique student ID : password
• Upload the eCert
Also:
• Update access key revocation list
eCert
Qualification award and access control metadata
Qualification award
• Qualification award data
• Embedded signature value for the transcription file
• Embedded signature value for the evidence file
• Embedded issuer's digital signature
Qualification transcription
Evidence files
1. decrypt with system default private key
Time control value in metadata:
• Check if it is within the access time and date
Issuer ID in metadata:
• Check if the signing key has a revocation record
2. verification and validation
Verify signature with issuer's public key
• Check content modification
• Check award revocation
• Check if it is within eCert expiry date
Ownership
• Check if the eCert student ID = login student ID
• Student can only access their own eCert within the management subsystem to prevent any unauthorized modification to the document
3. display the eCert with verified message
4. owner control
Set new access control value
• New file name
• New access expiry date and time
• Select extract/blinding options
Encrypt controlled eCert
• System genera new key pair
• Encrypt the newly controlled eCert with the new private key
Return value
• Newly created owner controlled eCert
• Access information (new file name : new access key : new expire date)

Figure 6-16 Set control on an eCert

For students to set access control to their own eCertificate, they need to log into the management subsystem. Here, the federated identity system Shibboleth will be adapted for the login control. Once the eCertificate is uploaded and the access token entered, the system will automatically carry out the checking processes, which will include a) the access token is correct and within the access time limit, b) the eCertificate is within the valid time limit, so that no re-certification is required yet, c) the signing key has not been withdrawn (key revocation), d) the eCertificate has not been withdrawn, and e) whether the uploaded eCertificate belongs to the student.

An overview of an eCertificate set control process is shown in Figure 6-16. The detailed process of the management system is described below.

- User needs to login to the management system
  - Login using the unique student ID and a registered password
  - Use an independent login control for now, but will investigate a federation access management system in the future
- Take the uploaded eCertificate and its access key from input
- Carry out all the verification processes detailed in the verification system section
- From the eCertificate metadata, get the eCert ID, verify the eCert ownership by matching the login student ID with the student ID in the eCertificate metadata
- Students can only set access control to their own eCertificates, to prevent unauthorized access to other people's eCertificates
- Take from user input new access time limit, selected visible sections, and a preferred new file name
- Compress all visible sections
- Generate a new key pair, encrypt the file with the private key
- Name the encrypted compressed file with the user input file name with the current service version code for the file extension
- Make the controlled file available for download, inform user of the access key (the public key)

6.5.5 Verifying an eCertificate – the Verification System

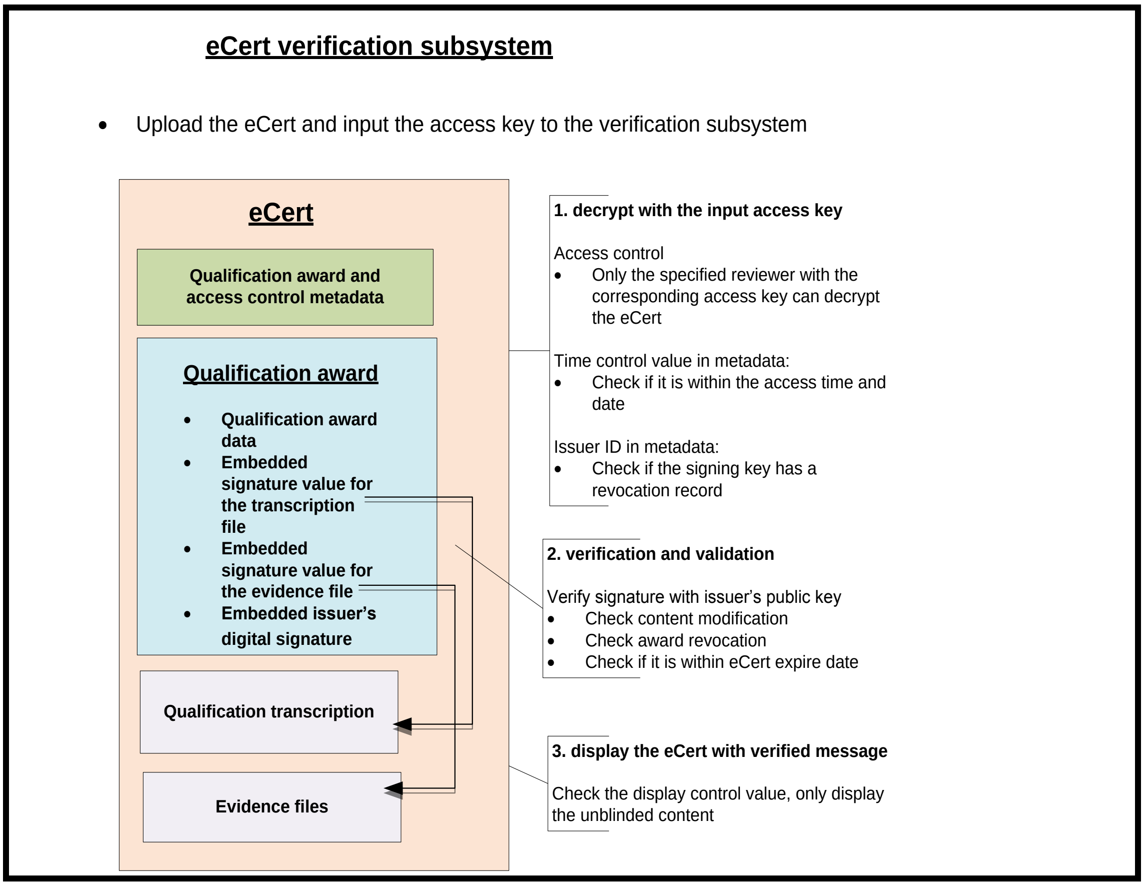

eCert verification subsystem
• Upload the eCert and input the access key to the verification subsystem
eCert
Qualification award and access control metadata
Qualification award
• Qualification award data
• Embedded signature value for the transcription file
• Embedded signature value for the evidence file
• Embedded issuer's digital signature
Qualification transcription
Evidence files
1. decrypt with the input access key
Access control
• Only the specified reviewer with the corresponding access key can decrypt the eCert
Time control value in metadata:
• Check if it is within the access time and date
Issuer ID in metadata:
• Check if the signing key has a revocation record
2. verification and validation
Verify signature with issuer's public key
• Check content modification
• Check award revocation
• Check if it is within eCert expire date
3. display the eCert with verified message
Check the display control value, only display the unblinded content

Figure 6-17 Verify the signatures

For anyone to view and verify an eCertificate, the only requirement will be uploading the eCertificate and entering the access token onto the verification subsystem. The verified eCertificate will be displayed automatically if it has successfully passed all the validation checking processes.

An overview of an eCertificate verification process is shown in Figure 6-17. The detailed process of the verification system is described below.

- Take from input the uploaded eCertificate and its access key
- Check the service version code from the file extension, select the correct version for the service

- Decrypt the file using the input access key, if no input, using default key
- Validate the eCert time limit, access time limit, against the current day and time
- Validate issuer's PKC against CRL
- Validate eCert status against eCert CRL
- Verify content modification for the qualification section
- Verify content modification for the transcript and/or evidence section(s), if the co-responding visible setting = 1
- Display error message, and stop the rest of the process, once it fails any one of the processes above
- Display the eCert and its signature, if it passed all the processes above – display the transcript and/or evidence file(s), if the co-responding visible setting = 1
- Compare the eCertificate version code with the current service version code, display warning message and advice if the eCertificate has not been updated
- Issuer's PKC must be able to display the trace all the way to the root CA if required

6.5.6 Other Required Operations

A number of operations are required to support the design of securing the system, as described below:

- Withdrawal
  - Update the award CRL with the corresponding eCert ID when withdrawn
- Revoke issuer's key
  - Update the signing key CRL when the key is revoked
- Technical update
  - Name the server with unique version code

6.6 System Demonstrator

A system demonstrator has been produced to test the design from the technical angle. With the specification and test plan set up, the project for the production of the demonstrator was joined by the eCert project assistant.

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

6.6.1 The Back end – Code Library

The core of eCert demonstrator implementation is a code library, providing basic support for the eCert issuing, management, and verification system development. The code library is built in Java, with the programming environment of J2SE 1.6.

The eCert code library includes a number of features that meet 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 digital signing of prepared files, file compression and decompression, and fully verifying signed qualification files.

6.6.2 The Front End – online Demonstrator

A web interface service 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 the database.

The website provides the user interface for the issuing, management, and verification systems, with calls to the code library for functional support. All web pages share a common interface design for consistency with a different colour scheme to distinguish the three systems. Different pages are rendered by loading different sub-pages in the menu and content areas using Ajax technologies.

6.7 Chapter Summary

A system has been developed following the SORM methodology. Based on the research decisions and assumptions for the new eCertificate system, a secure and user-centric approach has been presented to address the issues identified, such as the eCertificate squared problem and ownership rights. With a newly designed eCert file structure, signing method, and system structure, the new design enables authorized modifications to signed eCertificates while signature integration remains without the need for re-signing; it forms a framework for secured and owner controlled distributed data.

Chapter 7 Testing & Evaluation

The eCertificate is a new field of research, so at this starting point, the evaluation of the proposed system was focused at the theoretical level, such as whether the related issues have been understood and the design is appropriate, rather than on the production level of how well the demonstration system performs. With this focus in mind, the Delphi methodology was employed, step-by-step alongside the development, to evaluate whether the proposed design meets all system requirements.

To assist this evaluation and have a better understanding of issues that arise when theory is applied in practice, two system testing processes were carried out at the technical level: (1) through the eCert demonstrator to test the system function against requirements ID SR-03 and SR-04, and evaluate whether these requirements can be achieved technically; (2) through an experiment subproject to integrate eCert in ePortfolios, test the system against the requirement ID SR-01, and evaluate whether the proposed eCert system can be adapted into the ePortfolio systems technically.

The eCertificate system testing was carried out by the researcher and the eCert project assistant. The test results recorded in Section 7.1.2 were expressed in the researcher’s own words. The development of the eCert in ePortfolio system was carried out by the subproject team members. This is expressed in the researcher’s own words in section 7.2.4 and 7.2.5. Apart from these, all other sections in this chapter are the researcher’s own work. This work has also been published as reports on the eCert project website [28].

7.1 eCert System Testing

The aim of this testing is, through the eCert demonstrator, to evaluate whether the proposed eCert system meets the requirements ID SR-03 and SR-04.

7.1.1 Test Preparation

1. Create a Public key certificate for issuerA.

2. IssuerA issues an eCert, named eCertA, to userA through the issue system.

3. IssuerA issues an eCert, named eCertB, to userB through the issue system.

4. Create a user account for userA in the management subsystem.

7.1.2 The Test Plan and Test Result

System testing for the produced demonstrator against system requirements ID SR-03 and ID SR-04 were carried out. After some debug process, the final test results were emerged as expected. Details of the test plan and result are shown in Table 7-1

Table 7-1 eCert system test plan and result

SR ID	DT ID	Test items	Test method	Expect result	Test result
SR -03	DT-01	Unauthorized modification through displayed eCert	Access eCertA, change part of the displayed content, e.g. from BSc to PhD, and save as eCertD	The displayed content is read only. In the case of being modified, it will not be a valid eCert	As expected: Can not modify the content of displayed eCert
	DT-02	Unauthorized modification through file code	Change the encrypted string for BSc to PhD, save as eCertE (Assume a hacker can manage to access the qualification section of the eCert); then upload eCertE to the verification system	Display error message (invalid digital signature)	As expected: Returning an error for validating content modification step of verification without displaying eCert's content
	DT-03	Withdrawal of signer's key	Update the CRL for eCert issuers – revoke issuerA's key, then upload eCertA to the verification system	Display error message (key has been revoked)	As expected: Returning an error for validating issuer's PKC against CRL step in verification
	DT-04	Withdrawal of the qualification award	Update the CRL for eCert qualifications – revoke eCertB, then upload eCertB to the verification system	Display error message (award has been revoked)	As expected: Returning an error for validating CRL step in verification
	DT-05	Lifetime validation	Delete issuerA from the system; then upload eCertA to the verification system	Display the eCert	As expected: Displaying the eCert
SR -04	DT-06	Unauthorized access	Open eCertA or eCertB with Microsoft Word, Notepad, IE, or XML editor (without any access key or	May achieve the encrypted string only, not meaningful data	As expected: Content of eCert files can not be accessed

SR ID	DT ID	Test items	Test method	Expect result	Test result
			system)		
			Login to the management subsystem as userA, upload eCertB with access token	Display error message (the user is not the owner of the uploaded eCert)	As expected: Returning an error for wrong user
			Access eCertA or eCertB through the verification subsystem without or with incorrect access token	Display error message (invalid access token)	As expected: Returning an error for wrong user
	DT-07	Authorized access	Login to the management subsystem as userA, upload eCertA with access token	Display the eCert	As expected: Verifying the eCert file and displaying its content
			Access eCertA or eCertB with access token through the verification subsystem	Display the eCert	As expected: Verifying the eCert file and displaying its content
	DT-08	User control of usage	Login to the management subsystem as userA, set new access token to eCertA, save as eCertC. Access eCertC with access token through the verification subsystem within the time limit. Access eCertC again with access token through the verification subsystem after the time limit	Display the eCert when access is within the time limit; display error message when after the time limit	As expected: Verifying the eCert file and displaying its content; Returning an error for time limit step of verification without displaying the content of the eCert

7.1.3 eCert System Design Feature Summary

Compared with the current techniques and existing systems that mentioned in chapter 3 and 4, the eCert system offers significant advantages.

- **Ownership**: the eCert system is designed with a user-centric approach, the eCertificate is in the owner’s hands, and the owner has full control of it. For example, the owner can set access control to an eCertificate, and it can be stored in the owner’s preferred repositories while still maintaining verification functions.

- **Technical**: the system contains functions to handle the eCertificate squared and the auto validation problems; also allows settings for usage control while still verifiable 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 registered educational organizations.

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

- **System storage:** the system does not store any eCertificate copies or sensitive data, 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 lifetimes.

- **Security**: as sensitive personal data is not stored in the system, and there is no traffic raised against any organisations’ database for the verification process, many of the potential attacks can be avoided.

- **Trust:** the central system is only there to provide a service, as sensitive personal data is not stored, so there will be no risk of data being lost. Regarding people who do not trust government bodies to hold their personal data, this approach makes having such a central system possible.

The drawback of the eCert system is that it has only be tested with stakeholders in design and development situations, but not yet with live groups of users. More issues could be raised from this unexplored area. In addition, the legal issue of digitally signed documents needs to be followed up, as this is what the eCert system based on. It is the key issue of whether the eCertificate system as designed can eventually replace the paper-based system.

7.2 Integrating eCert into ePortfolios

One of the goals of this eCertificate research is to investigate a solution for a secured eCertificate system that can overcome the paper-based certificate problems, and enable such eCertificates to be used standalone or serviced within other systems, most importantly the ePortfolio systems. The ePortfolios require verifiable qualification claims, and will be the main systems that the eCertificates are embedded in, therefore they are the best test-bed for the eCert system. A successful result of integrating eCertificates into ePortfolios will not only verify the applicability of the eCertificate system, but will also provide a solution for the ePortfolio artefacts' assertion issues. Therefore, after evaluating the eCertificate system through the Delphi method, the system was evaluated again, under a subproject named Integrating eCert in ePortfolios, to test its usage in the related applications, as explained in the following subsections.

7.2.1 The Selected ePortfolio System

Two ePortfolio systems were selected for the purpose of this study: eFolio[13] and Mahara[14].

[13] eFolio: University of Southampton ePortfolio system. Available from : http://www.efolio.soton.ac.uk/

[14] Mahara: an open source ePortfolio system. Available from: http://mahara.org/

eFolio was selected as it is an in-house ePortfolio system. It was newly developed at the University of Southampton, which allows full access to both the code and the development team. The eFolio system is written in PHP and JavaScript, and allows authorized students to create a number of portfolios with their academic achievements. It is also used by staff for setting assignments and displaying coursework results. The system links with many central services provided by the University of Southampton, including the Banner student information system[15]. The eFolio system was at its live-trial stage at the time of this research, and has not yet been released.

On the other hand, Mahara is mature and open source software, which has advantages over eFolio in terms of system functions and development environment. The Mahara system is written in PHP, and uses the Model-view-controller (MVC) software architecture. The system’s structure is highly modular; it contains several libraries to support its functionalities, has the capability of handling most of the eCert requirements, and offers a pluggable environment for customisation.

7.2.2 Systems Integration Analysis

The eCertificate file format: The structure of an eCertificate file is newly designed and developed, and contains three files: a qualification data file, a transcript file, and an evidence file. The main qualification file also holds the signatures for the related transcript and evidence files. All these are bound together, signed and encrypted, and named with a new file extension of .eCert. For the integration of eCert into an ePortfolio, the .eCert file must be able to be recognized and function as designed.

The eCert system: The eCert system includes two subsystems: the issuing subsystem for issuers to generate eCertificates; and the management and verification subsystem, an online service that enables users to upload their eCertificates. This allows owners to set access control to their eCertificates by adjusting particular variables, while reviewers can verify their received eCertificates. Assuming the eCertificate owners present their eCertificates by making them available as part of the

[15] Ellucian: Available from http://www.ecu.edu/banner/

ePortfolios, the ePortfolios have then become the user-friendly, web-based front-end, while the eCert Central System remains ultimately responsible for the management and verification process at the backend. For the integration of eCert into ePortfolio, the eCert functions have to be maintained, so that eCertificates presented in ePortfolios are access controlled and verifiable.

7.2.3 The Challenge

The overall goal of this subproject was to integrate the eCert system into existing ePortfolio systems. From the system integration analysis above, it is clear that the challenge is to ensure the newly proposed eCertificate file, which has a unique file structure with file extension .eCert and secured by access key and digital signature, can be recognized and verified by the selected ePortfolio systems, eFolio and Mahara.

7.2.4 Decision on the Encryption Method

With the ePortfolio systems selected and integration issues analysed, a project specification was set up (the eCert-GDP2010) and passed on to a group of four masters students to integrate the newly developed eCertificate system into eFolio and Mahara. After the group studied the eCertificate system and the two selected ePortfolio systems, they suggested a new encryption method for the eCertificate system.

eCert encryption method: as proposed by the researcher, eCertificates are encrypted using the system default public key, and stored under the corresponding owner's institution account. The owner can then access the eCert central management subsystem to set access control values, where it will be encrypted with a unique private key. The owner can then make the access key (the public key) and the controlled eCertificate available to the reviewer by different methods, e.g. making the eCertificate available online, and sending the access key through email. The reviewer will need to use the access key (in a similar way to using a password) to verify the eCertificate in the eCert central verification subsystem. This method ensures that only the reviewer who has the access key can verify and view the eCertificate content. However, it is inconvenient that the reviewer needs to store the access key as well as the eCertificate. This in turn also affects the ePortfolio system as every embedded eCertificate requires its unique access key. It is also worth noting that none of the existing ePortfolio systems examined offers the functionality for uploading two associated files, which would have presented another barrier to implementation.

The new encryption method: as proposed by the GDP2010 group, in the eCertificate issuing process, the localised issuing subsystem will make a request to the eCert Central System for a new key pair. The central system will generate the key pair, store both in its database, and send the public key back to the issuer. The issuer will then embed this key within the eCertificate before using it to encrypt the entire package. This will result in a file that can only be decrypted using the associated private key, which is only ever known and kept by the central system.

However, even though this new method avoids the use of an access key, it has lost the function of access control, so that everyone who gets hold of an eCertificate can verify and view its content, as the access key (the private key) is stored and can be retrieved in the eCert central system. These approaches are compared in Table 7-2 below.

Table 7-2 eCert initial encryption method vs. subproject team proposal

	Researcher’s original eCert design	**eCert GDP2010 team proposal**
Initial issued eCert	Encrypt with system default public key, and decrypt with the corresponding system default private key - access key stored in eCert central system, no key handling required from the student	Encrypt with unique public key, and decrypt with the corresponding private key - all keys will be stored in the eCert central system, no key handled by the student or the receivers
Owner controlled eCert	Encrypted with unique private key, and decrypted with the corresponding public key - need to make the pubic key available for the receiver to access the corresponding controlled eCertificate	
Benefits	On initial issue, the use of system default keys enable open access whenever required; no key handling suits low IT skill users; one key for one controlled eCertificate that the student can send to the desired receiver(s); this ensures only the reviewer with the corresponding decrypt key can access the eCertificate; loss of key is not a problem as the student can generate another one	No key handling required from any users; this suits low IT skill users, and suits the ePortfolio integration as the ePortfolio currently has no support for taking access keys for uploaded documents
Issues	The owner needs to manage the keys (keep a record of the matching keys with the corresponding controlled eCertificates) Requires function support for the uploading key when eCert integrated into ePortfolio Need to make sure that the student can only access their own initial eCertificates but no-one else’s	This method requires the keys to be reported to the eCert central every time a controlled eCertificate is generated The central system needs to store the key pairs for the matching process when decrypting For a system that is designed to be rolled out nationwide, this requires huge storage, and also increases the chance of database attack If the database is in error or modified/hacked, this will result in invalid eCertificates Most importantly, loss of owner control on who can access their eCertificates, as no access key is required from the reviewers

Using a default key makes open access possible, as eCertificate owners may like their eCertificates to be open access in some situations. Owners can set access control on their eCertificates when needed. To enable this, the initial issued eCertificates must only be accessible to their owners during the issuing process.

Considering that keys are likely be forgotten at some point, creating eCertificates using students' personal keys may end up with their initial eCertificates becoming inaccessible.

Therefore, it was decided that the initial eCertificates would be encrypted with the default key, and saved under the corresponding student's account, so only the owner can have access. The eCertificate can be encrypted with a personalized key through the management system before sending to the reviewer.

The GDP2010 team has proposed a number of solutions to their new encryption method, such as a white-list policy, in which the eCert Central System will be able to determine the identity of a genuine employer, or ePortfolio making a verification request (perhaps by its IP or domain name) and only responding to those entities. An alternative is to operate a blacklist policy, where malicious users are identified and blocked; however, this assumes they will re-offend and with this solution the system will still suffer violation before being able to determine who is and is not a malicious user.

As the user access control is one of the main requirements of the eCertificate system, it must be met when it is applied to the ePortfolios. Therefore, it was decided that the new encryption method would be rejected, and the eCert encryption method would be maintained. A function to support the upload of two files (eCertificate and access key) in ePortfolio was implemented.

7.2.5 Development

Apart from the decisions I made as the project manager and the eCertificate system designer, the development work summarized in this section is the group's contribution.

The eCertificate integration development covers two segments: a new layer of Java code as the API for the eCert code library, and the extensions for eFolio and Mahara to enable the upload of eCertificates and their corresponding access keys, and the verification process with the eCert central services. The group carried out the tests step-by-step throughout the project to ensure that the system worked as expected and meets the original specified requirements.

Full details of this eCertificate integration project can be found from the eCert project website.

7.2.6 Results

From analysis and design to development and testing, the Integrating eCert in ePortfolio sub-project was carried out through the development lifecycle. With successful implementation, both the eFolio and the Mahara can now be fully utilised by those with eCertificate qualifications. This proved that the newly developed eCertificate can be used in ePortfolio systems at both the theoretical and the technical level.

During the project, the eCert code library was employed. As a result, the eCert system has also been improved since errors were found and fixed.

7.3 Development and Evaluation with Delphi Methodology

The eCertificate study employed two research methodologies: SORM and Delphi. The mini-Delphi methodology [131] was used step-by-step alongside the SORM methodology throughout the development stages, to guide and evaluate whether the design met all five requirements theoretically.

For the mini-Delphi method, a group of domain experts in the UK were selected for security system design, ePortfolio study, and to represent the stakeholders. These included employment managers, IT security experts, exam board managers, and ePortfolio researchers (details can be found in Appendix I). Two workshops were run during two stages of the development to collect professional opinions from these experts. The first occurred at the system design stage, aiming to evaluate and adjust the design at the strategic level. After the first round of information collection, analysis, feedback, and system adjustments, a second workshop was run on the system demonstrator completion stage, when the system was shown to the domain experts again. The aim of this round was to evaluate and adjust the design not only at the theoretical level but also at the technical level.

7.3.1 The First Round – the First eCert Workshop

Following the eCertificate research, analysis, and initial design phases, the first workshop was held to review the design before moving onto the demonstrator development stage. It was aimed at bringing leaders in the field together to consider and report on design issues for the secure eCertificate system, to check whether the eCertificate problems and issues had been adequately understood, and that the project was on the right track for the solution.

7.3.1.1 The method

The workshop was arranged in two parts. In the morning, the eCertificate topic was first introduced; then the determination of eCertificate issues and problems was opened up through presentation; this was followed by a group discussion to explore and define the problem areas.

During the discussion, the Delphi technique was followed. The participants were given 4 questions, arranged in 2 groups. Group A discussed question in the order 1 to 4, while group B discussed the same questions from 4 to 1. The questions were:

1. Are there any missing issues? If yes, what are they?
2. Should there be any more requirements? If yes, what are they?
3. Anything that is over and above what is required?
4. Are there any errors and misunderstandings?

At the end of the group discussion, the two groups joined to report their views and have further discussion across groups.

In the afternoon, the proposed eCertificate system design was introduced through a presentation, entitled “Towards solving the problems: the eCert plan”. This was followed by a Round Table discussion on the proposed design and its related issues.

All conversations during group discussion and feedback were recorded with the permission of the participants. At the end of the workshop, all participants were informed of the plan for the following meeting.

A copy of the first workshop PowerPoint presentation is available in Appendix G. Information of the workshop, including venue, date, participants, and format can be found in Appendix I.

7.3.1.2 Feedback Summary

In this round of Delphi, the first phase was to collect the required information from the expert panel to explore the subject issues.

From the workshop, the eCertificate use case analysis and the proposed system were accepted without many issues being raised. Instead, there was a wide-ranging and interesting discussion of the higher level issues of rationale that covered several topics:

- Security issues
    - Is more than one approach needed? If Digitary has a working solution, why look for an alternative? This issue also relates to issues such as scalability, since Digitary currently only deals with HE awards.
    - The statement was made to the effect that putting secured data in the hands of the user puts the central system at risk. It is not immediately

obvious why this should be the case, so it raises a number of questions about what architecture is being assumed.

- Longevity. The point was made that a certificate issued by a CA typically has a life of a year or so, hence one might jump to the conclusion that an eCert award certificate would not be secure after this period. Taking this thought further, one would therefore have to assume that a digitally-signed document would also only have a useful life of a year or so.
- Data persistence. The question was raised of what happens when the awarding body no longer exists? There was an assertion that awards are all recorded by the British Library. The question then arises of which awards, and of how robust the procedure is – the practice may be very different in some cases.
- The question of prevention of data theft was also discussed. It was pointed out that it is not possible to prevent screen scraping (or other forms of data capture for that matter); however, it is possible to provide a system whereby scraped data cannot be verified.
- Implicit in the discussion was the fact that perception of security is important if a practical system is to be adopted in due course. Providing a demonstrator may be helpful, but regardless of the reality, if there is an underlying doubt that the system may be insecure, adoption of the mechanism will not follow on.

- Scalability and Granularity
  - It is believed that Digitary currently deals exclusively with HE awards. That leaves open the question of potential loading and performance issues if one wishes to deal with (a) 6th form awards, and (b) lower-level (GCSE, NVQ, etc) awards.
  - There is an issue of granularity. There is interest in exploring the potential for validation of pieces of work (e.g. for NVQs) not just entire awards.
  - It was also noted that there is a move to validating the assessor rather than the work per se.

- Ownership and Control of Data
    - Does the student own their own award data, or does the awarding body? Might the employer/recruiter also claim ownership of the data relating to their student or employee?
    - It was evident that ePortfolio systems are currently capable of giving the student full control over who sees what of their data and for how long.
    - It might be assumed that Digitary also considers that it can give full control to the student over their data.
- Other Issues
    - A question was asked about the Southampton context – why are we exploring the eCert approach? This has been answered: it is two-fold – the research is a direct response to the scenario specified in the JISC bid; but it has also been exploring the extent to which it is firstly possible, and secondly desirable, to implement an electronic equivalent of the paper awards, which are still widely used in practice. This research is also currently exploring the potential application of such technology to other areas such as passports, driving licences, and other secured forms of identity confirmation.
    - Another discussion topic was the concept that perhaps ePortfolios should not provide validated information, but information which can be validated externally. This has been very helpfully expanded at length in Simon Grant's blog[16].

7.3.1.3 Outcome Analysis

The second phase was to analyse how the group viewed the issues, what was agreed, what not, and what needed further action.

No issues were raised concerning the accuracy of the use cases on which the eCert design is based. It was understood that these were a satisfactory basis for the

[16] Simon Grant's blog regarding ePortfolio information validation http://blogs.cetis.ac.uk/asimong/2010/04/19/portfolios-need-verifiability/ (lass accessed: 29/06/2013)

design of the eCert code library and demonstrator. There were a significant number of issues of rationale raised that need to be explored. These are as follows.

- How does the eCert approach compare and contrast with that taken by Digitary? Unfortunately, Andy Dowling (CEO Digitary) was unable to complete his trip to Nottingham, so a separate meeting was arranged – this took place on the 28th April 2010 through Skype. Also, Jonathan Dempsey, CTO of Digitary, provided useful information through emails. As a result, a comparison between eCert and Digitary was carried out, which is detailed in Appendix D.
- Bearing in mind that the perception of security is as important for adoption as the reality, it will be helpful to outline the issues that distinguish a distributed solution from a centralised one, and to articulate the advantages and disadvantages of each approach.
- The issue of longevity needs to be explored in greater depth. Linked with this idea is the concept that the eCert protocol, and similarly the code library, should transcend specific implementations, so that it can utilise whatever techniques and algorithms might become available in the future.
- The issue of data backup also needs to be investigated further. In this context, what is the theoretical approach to ensuring a paper award can be validated if the awarding institution closes, and what happens in practice? How robust are the procedures? How does this differ depending on the type of award considered?
- In order to address issues of loading and performance, it would be helpful to obtain an indication of the level of requirement from EdExcel.
- It might be helpful at some stage to produce some scenarios to illustrate and highlight the issues relating to competition for claims to ownership of student award data. The (UK) Data Protection Act 1998 might provide helpful insights, as might equivalents from other countries.
- Some thought will need to be given to the mechanism by which the student controls access to their data. Rather than making an assumption about the mechanism, it might be helpful if the code library made provision for

control to be managed by various means (e.g. centrally, or through an ePortfolio system, for example).

- It will be helpful to think through whether there are any specific implications if one takes the view that an ePortfolio should provide verifiable, rather than verified information.
- The eCert project is tasked with producing an eCert digital award certificate system library and demonstrator. If the resources can be suitably managed, it would be helpful if, in addition, the project could show how the approach would work within (i) an ePortfolio system, and (ii) a different context, such as a mobile identity confirmation system.

7.3.1.4 Actions taken after the workshop

The third phase of Delphi was to further explore the areas of disagreement and unaddressed issues. As a result, the system design was revisited according to the workshop feedback, which included:

- more study into the certificate’s lifetime issue, in terms of the award, the CA, and the issuing institution;
- some additional functions have been designed to enhance the usability and security, such as version support to deal with technology upgrades in the future;
- more research into document certification related systems, such as Digitary, to provide clearer vision and descriptions of the eCert innovation and advantages;
- more research into ePortfolios to explore the ePortfolio artefact verification requirements.

7.3.2 The Second Round – the Second eCert Workshop

After system adjustment and further development, a second workshop was run. The first and second phases of the Delphi were repeated in this second round. It was hoped that the variety of opinions would decrease and tend towards convergence.

The second eCert workshop was held at the end of the system demonstrator completion stage. The aim of the workshop was to evaluate the system design from the technical level, and work through the potential practical issues that might be encountered in the introduction of such a system. It took place during ALT-C2010, the 17th International Conference of the Association for Learning Technology, which was held at the University of Nottingham.

7.3.2.1 The method

Following the Delphi method, the system was again presented to the domain experts. All participants from the first workshop had been invited to the second workshop, but not everyone could make the second round. However, all new participants who joined the latter workshop were experts in the domain, including the conference workshop facilitator, eLanguages technical developer, head of New Ventures at the Scottish Qualifications Authority, and the Project Manager of Cambridge Assessment.

During the workshop, the possibilities and potential problems of the eCertificate system were revisited. After being introduced to the improved system design through the system demonstrator presentation, the participants were organised into 4 groups with a set of questions to revisit the system's possibilities and potential problems. The questions were redesigned to reflect the topics that concerned the first workshop.

- Group A:
  - Have we a need for the eCert system in our institution?
  - Would our students want this?
  - Whose data is it anyway?
- Group B:
  - Would there be problems for staff implementing this, or would this help?
  - Are there infrastructure problems that might create difficulties?
  - Would this be useful for other purposes?
- Group C:
  - Would there be institutional barriers to introducing an eCert system?
  - What gains would we foresee in using an eCert system?

  - Would this be useful for other purposes?
- Group D:
  - Have we a need for eCertificates in ePortfolios in our institution?
  - What about the "club" scenario, would this be attractive?
  - Whose data is it anyway?

All conversations during group discussion and feedback were recorded.

A copy of the second workshop PowerPoint presentation is available in Appendix H. Information of the workshop, including venue, date, participants, and format can be found in Appendix I.

7.3.2.2 Feedback Summary

The workshop had a positive result. There was no strong disagreement as all participants liked the idea of eCert. One of the participants, who is the head of New Ventures UK Awarding Body[17], wrote in his blog: "… Some really useful example uses from across UK… can be used to verify exam results, project work, e-portfolios. … can see lots of applications for this, … potentially useful links to Bologna process and E-Certification E-pass work." The feedback from the workshop indicated that the eCert system would be of use, and provide applications that would be enthusiastically welcomed.

Besides the suggested discussion topics, participants were also interested in the fine detail of the system, and the legal, societal and institutional barriers that would get in the way. The general feedback from the groups:

- Legal – international legal issues; insurance costs
- Systems would have to run in parallel – cost
- Who is going to pay? In general terms?
- System for employers would have to be really easy to use
- EdExcel and the other bodies would have to sign up

[17] Joe Wilson, Head of New Ventures UK Awarding Body, wrote about the eCert system in his blog: http://www.joewilsons.net/2010/09/e-cert-programme.html

    - Puts their reputation on the line
    - Insurance/money
- You would have to train students to manage their eCerts, not to lose them, how to share them
    - Some students wouldn’t be able to do this
- You would have to integrate with many other systems – portfolios, class lists, Banner, etc.
- At the moment the system is a generic verification engine that is being put into the context of education
    - Consider giving the system some semantic knowledge of the educational qualification structure and qualification requirements
        - Bologna Process integration – huge market – people are really struggling
- This system would be very useful for lifelong learning and expiring certificates: FSA, Doctors, Lifeguards
- People seemed less interested in certifying qualifications, but very interested in certifying evidence and portfolios. EdExcel have been working on the problem for years and keep returning to watermarked paper, etc.
    - However, people were very interested in validating international certificates, as it is very expensive to do now.
- There are so many vocational qualification bodies who will have to be signed up
- You would need secure infrastructure links from institutional systems in eCert
- It would change working practice for student-records staff
- Open up parts of student records, e.g. for a particular course – prerequisites.

7.3.2.3 Outcome Analysis

In this second phase of the second round, the feedback from the workshop indicated that the eCert system would be of good use, and provide applications that would be enthusiastically welcomed.

Feedback related to the system's running cost and integration with other systems were dealt with during the system design stage. For example, it will be open source, free for all users and institutions, but will require maintenance costs for system support and technical updates; and some requirements for eCertificates to be used within ePortfolios have been added.

Feedback related to organizational sign-up was considered during the system design, so that:

- The system is free for any registered education institution who wants to use the system.
- The eCert system was designed to work for any size of federation: the system can start to operate with one registered organization, and can provide services for all member registered educational organizations throughout the UK.
- No access to the issuing subsystem will be provided for non-registered bodies; and even assuming unauthorized access has been gained, the resulting issued eCertificates will not pass the validation process.

Feedback related to easy use of the system will be reflected in the system HCI design, with more instructions and messages added to increase usability.

Feedback relating to security issues, such as links from Institutional systems to eCert, was addressed: once the eCertificates are issued, there are no links between institutional systems and the eCert system. There is no database access to any of the issuing institutions for viewing or the verification process. However, all institutions need to report their CRLs (certificate revocation list) to their CAs, which the eCert system will access during the verification process.

Many of the questions raised were due to unclear information provided during the limited presentation time. The explanation was not deep enough; people had lots of clarification issues. These resulted from shifting away from the cloud computing paradigm, contrary to participants' expectations.

During the workshop, only the eCert system aims and how it works were discussed, but not the differences between eCert and other existing methods (e.g. digital signing) and systems (e.g. Digitary), which led to confusion. The missing crucial information would have helped with the explanation, but also have given an inside view of eCert's features. Without a good understanding of the system, participants were not able to provide more useful feedback. This type of information should be added in any future presentations.

There were also vocabulary issues: *Certificate* as used in Public Key Cryptography and *Certificate* as used in qualification; *eCert* as used in bundle of encrypted data and *eCert* as used in the more generic idea of an eCertificate. These need to be clearly defined in any future presentations.

Answers to open-ended questions were too long to write down. Most of the participants did not record their thoughts, or write in sentences. This made recording feedback from the groups more difficult. A more efficient solution to collect feedback from groups is needed next time.

7.3.3 The Last Phase of Delphi – Final Evaluation

In addition to the two workshops with the domain experts, a few more workshops and presentations also took place at national and international computing security-related conferences to collect the opinions from a wider range of domain experts. These included: The 2nd International Conference on Computer Modelling and Simulation (ICCMS 2010), held in San Ya, China; The World Conference on Educational Multimedia, Hypermedia & Telecommunications (EdMedia2010), held in Toronto, Canada; London Learning Forum, held in London, UK; Federated Access Management 2010 (FAM10), held at Cardiff, UK; and The World Congress on Internet Security

(WorldCIS2011), held in London, UK. The eCert system was adjusted accordingly each time round.

After each round, feedback was reflected upon, and the system (including the design, demonstrator, documentation, and reports) were adjusted accordingly. For example: the eCert file structure now includes the transcript file to enhance its usage nationwide; a photograph 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 comparing the new design and existing systems; and the explanation of the chosen approach has been given in more detail.

Towards the end of the project, much positive feedback was received from conferences and workshops internationally while negative feedback was mainly related to the future work that cannot be completed within the current project. The Delphi method was, therefore, effective in achieving a convergence of opinions.

7.4 Chapter Summary

Referring to the system requirements set in Chapter 5, the proposed eCertificate system has been tested and evaluated in three steps: demonstrator testing to evaluate its technical satisfaction; ePortfolio integration testing to evaluate its adaptability; and workshops with a mini-Delphi methodology to evaluate the design from the theoretical level.

As a result, this has all proved that the eCertificate system can not only be used standalone, but can also be plugged into other applications, such as ePortfolios. The eCert system’s accessibility and scalability were improved after taking into account a considerable number of observations and recommendations from the evaluation processes.

Chapter 8 The Abstracted eCert Protocol and Proof of Hypothesis

This chapter summarizes the abstracted eCert protocol and its evaluation in two applications, and through these, proof of the research hypothesis.

The implementation of the Mobile eID system summarized in section 8.2.5 was contributed by a Masters student. It is expressed in the researcher's own words. All other sections in this chapter are the researcher's own work. This chapter has been published in conference paper [36], journals [31, 179], and on the eCert project website[28].

8.1 The Initial eCert Protocol

At the heart of the eCertificate system is the initial eCert protocol (the eCert file structure design, system design, eCert signing method, and the supported code library). It provides a unique, secure and trusted system for the management of eCertificates in a web-based environment with a secure user-centric approach. This user-centric focus is the key to this research.

The Delphi methodology [88] was used for the evaluation of the eCertificate system design throughout its development stages, alongside the SORM research methodology [173]. Following this methodology, a group of domain experts in the UK were selected for their knowledge of security system design, ePortfolio studies, and to represent putative stakeholders. This included employment managers, IT security experts, examination board managers, and ePortfolio researchers. Two workshops were run during 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 at the strategic level; and the other workshop when the demonstrator was completed, aiming to evaluate the system at the technical level.

The system was subject to further evaluation under a subproject named Integrating eCert in ePortfolios [29], to test the usage of the design principle. In this project, the eCertificate system was integrated with the UK ePortfolio system, the eFolio [60], and Mahara [113], an Australian system. Both systems can now be fully utilized.

Going through all these testing and evaluation processes resulted in the eCert protocol being adjusted and improved to suit the eCertificate requirements.

The case of eCertificate represents typical eDocument transmitting issues (that involve non-static content, authentication requirements, lifelong availability, maintenance of ownership rights, and the need to be transmitted to two or more parties). It is believed that the solution presented here could solve eDocument transmitting issues in other cases. Therefore, with the aim of proving this claim, and evaluating the applicability of the eCert protocol in a wider domain, a Mobile eID project and a eHealthcare patient data case study were set up.

8.2 The Mobile eID Project

With the aim of proving that the eCert concept could be applied in a wider eDocument transmission domain, the eCert protocol was tested under a project, named Mobile eID, to explore the issues that arise in implementing the eCert protocol within a mobile platform to provide certified and verifiable identity information.

8.2.1 Background Research

Technological development enables electronic identity (eID) to be employed in daily life, such as smart cards, online user accounts, and public key certificates. With the aim of replacing paper-based ID documents, these developments provide flexibility and efficiency with transportability.

Mobile devices have been constantly developed with a high computational complexity, providing flexible mobility, multi-functionality, and personal settings, and have become an indispensable daily object, used more commonly than any other technical device, such as the PC.

By combining the eID development with the mobile environment, using the mobile device as the eID platform could realise the maximum benefit. In that case, all an individual's ID cards and documents can be left at home, and the mobile phone will be the only device needed.

However, combining these two also results in their problems being combined, which are of a wide variety but mainly about security. The challenges in this emerging area of technology adoption need to be considered and addressed.

8.2.2 Scenario

Consider the following situation: young-looking Bob goes out clubbing and often has to certify his age to enter. By presenting his paper ID, he is forced to disclose all the sensitive information on that document, as well as his 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 was to apply the eCert protocol to present an ID document as digitally signed, owner-controlled ID certificates through mobile devices. The eCert for eID managed in mobile devices proved itself as the permanently available tool to provide a huge variety of ID in order to avoid the previous scenario.

8.2.3 Analysis

eID application development: an eID is an electronic document for online and offline identification, providing digitally the same (or more) information as the paper-based ID document in many cases, with more secure, flexible, and accessible functions.

An eID is usually a plastic smart-card (or EIC), and has the format of a regular bankcard, besides the embedded microchip. It also contains the printed identity information, e.g. personal details and a photograph. The chip will also contain the issuer's signature keys and certificates. To use an EIC, the user will also need the card reader and the middleware software. Another form of eID is the public key certificate. As mentioned earlier, on the eCert system, a public key certificate is also known as an identity certificate, digital certificate, or eCertificate; it is an eDocument that uses a digital signature to provide verifiable identity, which verifies that a public key belongs to an individual.

Mobile application development: Mobile application software is developed specially for small low-power handheld devices such as mobile phones. These applications are either pre-installed on phones during manufacture, or downloaded by customers from app stores and other mobile software distribution platforms.

Mobile software is developed using different platforms and programming languages based on the target mobile device. Each of the platforms for mobile applications also has a development environment which provides tools to allow a developer to write, test, and deploy applications into the target platform environment. Many different hardware components are found in mobile devices, so their applications are developed using different software architectures.

eCertificate vs. eID: The eCertificate and eID are both aimed at providing a secured and trusted system for the management of the verified personal data. However, even though the eCertificate and eID are quite close in concept, their structures and execution environments are different.

- In a face-to-face situation, such as the clubbing scenario above, the eID system is a quick way of passing the eDocument to a reviewer for verification, rather than sending a request through email or accessing a website that the eCertificate system does.
- An eCert file is a collection of selectable support files, individually signed with references embedded in the main content, before it is signed and encrypted with the access control metadata. On the other hand, the ideal eID

file will be a collection of selectable text information with an ID image gathered into a single signed file and encrypted together with the access control metadata. The eCert protocol needs to be adjusted to adapt the new eID file structure, so that it can be recognized by the verification process.

- The eCert protocol makes use of the eCertificate owner's institution account in the issuing process, which allows the eCertificate to be issued directly into the access controlled environment. In the eID, these accounts are unlikely to exist. Hence, a new encryption method to secure the issue process between the issuer and the eID owner is required.
- Unlike the eCertificate system, in which all issuers are under the umbrella of education institutions, and can have the issuers chased all the way back to the a top education body, such as the UK Department for Education, the eIDs may be issued from a wide range of organizations. These could be the Driver, Vehicle Licensing Authority (DVLA), the General Register Office (GRO), or the Home Office. The eID system needs to be adjusted to suit this multiple top certification authority (CA) situation for the verification process.

8.2.4 Design

The aim of the Mobile eID system is to focus on the user-centric approach supported by the eCert protocol. Therefore, most of the eCert protocol features needed to be maintained. The initial eCert file structure needed be adjusted, and the related functions needed to be modified to suit the eID's needs.

As anyone can potentially fake an eID on their own mobile phone, the process of verifying an eID needs to depend on the reviewers' devices. Therefore, even when an eID is presented face-to-face by its owner to the reviewer, a quick data transfer method is required to address the unique eID situation. After investigating current mobile communication techniques, such as email, Bluetooth, bar code, QR code[18], and text messaging, the QR code with its increasing popularity and wide availability of a QR

[18] http://www.denso-wave.com/qrcode/index-e.html, accessed 22 Mar 2011.

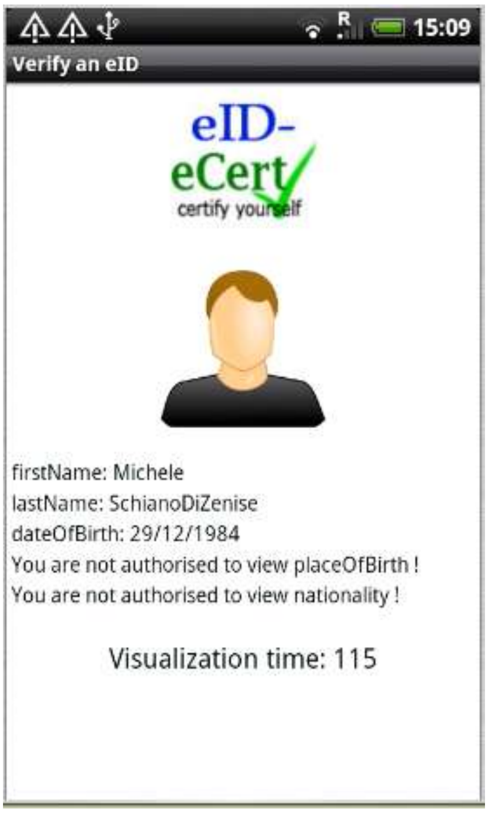
reader within mobile devices, has turned out to be the best solution for the eID data transfer.

8.2.5 Development

Based on the design decisions made, a project specification for a mobile eID application was set up and passed on to an MSc student, Michele Zenise, to develop a working system as a demonstrator. The development work for the Mobile eID application summarized in this section is Zenise's contribution. As project manager, I made the decisions alongside the processes to control the direction of development. We have published this work in a journal paper [179] as joint authors.

Zenise also carried out some related research himself. After studying the eCertificate system and the mobile eID requirements, he agreed that the QR code would be the best way forward, as a quick pass method, to address the eID system's unique requirement. He also noted that even though the concepts of the eID and the eCertificate are quite close, they are different in many ways. The eCert protocol that was initially designed for managing eCertificates in a web environment is not able to manage eID in a mobile environment straight away – a reverse engineering process to adapt the system is needed [178].

With no arguments against the design, Zenise then carried out the system implementation as set out in the specification. As a result, the Mobile eID application was implemented on the Android platform. The core of the application that employed the eCert methods was written in Java and linked to the Android interface with the use of PHP. The eCert file structure was adjusted, the related functions were modified to ensure the new file structure could be retained throughout the system, and a supporting function was added to deal with the multiple top CAs situation, so that eIDs would remain valid as long as they could be tracked down to any of the top CAs. For example, on a successful eID validation, the system will display the name and photo, along with the selected information, within the time set by the owner. This is shown in Figure 8-1, published in [179].



firstName: Michele
lastName: SchianoDiZenise
dateOfBirth: 29/12/1984
You are not authorised to view placeOfBirth !
You are not authorised to view nationality !

Visualization time: 115

Figure 8-1 eIDeCert: Verify an eID

8.2.6 Evaluation

Through the Mobile eID project, problems for the employment of the eCert protocol in a mobile environment were identified and the eCert code library was adjusted accordingly. Initial results indicate a real possibility of using the eCert protocol to manage eIDs in the mobile environment, supporting user-centric management of sensitive information.

Besides the positive outcome of system testing, a paper describing the protocol also successfully passed the domain experts evaluation processes and was published in the *International Journal for Infonomics*, [179].

As a result, the successful mobile eID application, which implemented a working demonstrator system on an Android platform, proved that the eCert protocol can be applied in other eDocument transmitting domains.

However, the proposed system was only developed and tested “in house”, no end users being involved. More issues need to be explored in this area in future study.

8.3 The eCert for eHealthcare Study

The current eHealthcare document transmitting issues provide unique challenges, such as security design for patient data privacy and ownership vs. emergency data access, which are excellent for testing the eCert protocol. To further test the claim that the eCert protocol can be applied to a wide eDocument transmitting domain, a study of eCert protocol for eHealthcare patient data transmission was carried out.

This section presents a system design for the management of healthcare information in the form of a securely distributed eHealthcare document, the eHealth-eCert, which can be owned and managed by the patient. By analysing the eHealthcare problem domain, a system was derived with both eCert supported functions and eHealthcare unique features. However, due to the time and human resources available, there has been no system implementation. This work has been published as a conference paper [36].

8.3.1 Introduction

While patient paper-based records and documents are gradually digitized, security concerns about how such electronic data is stored and transmitted have increased. This has a serious impact on the healthcare information system, as it contains sensitive patient data. The prevention of unauthorized modification and loss of records is highly important in the healthcare sector. Such concern is compounded by the knowledge that institutions that we ought to be able to depend upon are in fact unreliable. In this context, it is understandable that plans to computerize patient records in the US have caused public anxiety.

Besides the potential for human error, there is also legitimate concern that confidential patient data could be passed on to other organisations for financial gain. Without a system of checks in place, there is no guarantee that confidential patient data will not be abused. Information owners have increasing demands regarding their rights of ownership.

As a result of a wave of security breaches, there are now pressing calls for an opt-in system to be implemented for healthcare systems, giving patients the opportunity to choose whether or not to have their healthcare information collected and recorded. The security of healthcare information in the context of a networked, sensor-enabled, pervasive and mobile computing infrastructure is at the core of both the main challenges and potential risks of Healthcare ICT adoption.

8.3.2 Current eHealthcare Information Systems

There are various levels at which healthcare data is typically communicated, for example:

- National level across communities
- Regional level across organisations
- Enterprise level within the healthcare organisation
- Global information reach

Traditionally, healthcare data has been stored in filing cabinets. In progressing to computerised systems, the filing cabinet metaphor has typically been applied to digital database design.

The current security controlled system for eHealthcare information is very complicated. People who work in/with the NHS were interviewed about how patient data is accessed, stored and transmitted. Their responses indicated that access to patient data is very strict and in some cases could be difficult; patients have no control of who can access their data; and patient data transmission is generally consisted of paper records being put into envelopes and sending them by post, which lead to incidents of records being lost:

- Dr Nicola Englyst, a researcher and lecturer in Physiology, Faculty of Medicine, University of Southampton, said that after successfully gaining permission to access the NHS system as a researcher, she can access regional lab results and in some cases national records, for example, diabetes patients in the UK. All data accessed is read only. She stores the achieved data with her research data together in her own system, completely separate to the NHS system. For security purposes, no reference can be found on her system to identify the patients in the NHS system even when the database is hacked.

- Dr Ildar Abdoulline, a GP at Aldermoor Healthcare centre, Southampton, said that GPs can’t access patients’ hospital records and hospital doctors can’t access the GPs’ records either. Transfer of patient data is not through email or online systems, but by post, fax, or phone calls. For example, when a GP refers a patient to another healthcare professional, a letter that explains the situation and contains the selected patient data will be sent by post. A paper-based Summary Care Record is also available on request which can be passed on by the patient themselves.

- In an emergency situation, information is critical. Dominique Mylod, a midwife at Princess Anne Hospital, Southampton, said that besides the demographic details (e.g. name and next of kin), pathology results (e.g. blood tests), and Chronic conditions details (e.g. diabetes and severe allergy), information for previous birth and safeguarding are also very important. If a patient admitted in an emergency has been registered with the regional trust, then she will have the patient’s data on the system. Otherwise, she will rely on the pregnancy notebook that the patient brings in, which is a paper-based record of notes made by midwifes after every check-up. This should have all the required data.. If neither of these is available then she will need to phone the hospital that the patient is registered with and ask them to check on their system.

- Compared to non-NHS staff, patient data privacy issues are even more complicated within the healthcare sectors. Dr Nicola has raised an interesting question: how can NHS staff prevent their superiors/colleagues from seeing their patient records? - Currently, patients have no right to control who can access their data.

The challenge for the healthcare scenario is how to make patient data available as required to those who need to know, whilst preventing data being transmitted to organisations and individuals who have no right to know.

There are two competing aims that need to be considered when designing a secure system for the sharing of healthcare data. First, patients may wish their data to be made available without reservation or delay in emergency scenarios; they do not want doctors to be hindered in treating them because their patient data cannot be accessed. However, they may also wish to ensure that sensitive personal details are not visible to those who have no right to see them. These two aims are in conflict with each other. The safest way to ensure a doctor in A&E can see whatever they need to in order to treat a patient is to make all patient data visible to anyone at any time. However, this then means that patient data is now visible to those who the patient does not wish to see it.

A full healthcare information system includes the full data relating to a patient's care and includes information on support systems, for example. However, in this study, the focus is specifically on patient data only. The study will focus on the security issues of patients' data management, known in this paper as the Patient Record System (PRS).

8.3.3 eHealthcare Scenario

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 access or time-limited access to other people 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 sensitive private information cannot be forwarded to potentially malicious agents such as newspapers.

Scenario 1: Professor R in a Psychology Department needs to release some patients' health history records to her fellow researchers. However, by transferring the documents directly without going into them to delete some sensitive information individually, will lead to sensitive data being leaked, and she still cannot ensure that the distributed documents will not be modified without authorisation, abused, or stolen.

Loss of healthcare records: Medical records are crucial to patients' healthcare. Data corruption (e.g. unauthorized modification of records due to hacked databases or human errors) will lead to an incorrect diagnosis, while loss of records will waste inestimable amounts of valuable time.

Scenario 2: Patient A has a history of heart problems and has been taken to a hospital for emergency treatment. Normally, doctors can retrieve A's health record to make an informed decision, but unfortunately, this time, A's record is nowhere to be found, either in paper form or on a database. As a result, treatment has to be delayed, as doctors have to assess A as a new patient, and carry out new tests beforehand.

8.3.4 The Aim

In applying the eCert protocol to the eHealthcare problem, the goal is to provide a mechanism for user-centric distribution of data, which means giving patients control of who is allowed to see their data. It is aimed as an alternative option that could benefit patients, rather than a replacement of the current PRS.

In order to achieve this aim, security controls for the issue and distribution of data, and a verification service for this distributed data, are required.

8.3.5 Underlying Technologies

eCert protocol as policy for the signing and key management: The eCert protocol defines a secured and signed document that enables the user to determine what a reviewer is allowed to see and for how long, which is very close to the eHealthcare document transmitting requirements. Therefore, it is possible that it can be employed to provide a solution for eHealthcare issues.

eCertificate and mobile eID as applied examples: The eCert protocol was successfully applied to two eDocument transmitting use cases, the eCertificate for ePortfolio, and the eID in mobile environments. These can be taken as working examples for the eHealthcare system throughout its analysis and design stages.

8.3.6 Stakeholders

Three stakeholders were identified: the issuer, the patient owner, and the reviewer. Ownership of eHealthcare data is complicated, as it involves multiple government bodies and organizations. In the eHealth-eCert system, the issuer and the reviewer can be from the same organization, and a reviewer can be an issuer at the same time, and they can both be the owner.

However, for this eCert for eHealthcare study, the ownership was focused on the patients, as the system is designed to give patients control over their healthcare records. The patient should have ownership of the issued eHealth-eCert file. This is similar to the eCert system, where the student owns the awarded eCertificate.

8.3.7 Use Case

Three PRS use case scenarios were developed to highlight the benefits and issues related to data transfer in the healthcare sector: Sharing healthcare information is shown in Table 8-1; Record healthcare history is shown in Table 8-2; Transferring healthcare information is shown in Table 8-3;. These use cases are framed in terms of using a PRS.

Table 8-1 eHealthcare use case – Sharing healthcare information

Description	A professor in a psychology department wishes to share the patients' healthcare information with fellow researchers on a case study, as the researchers have no access to the PRS
Actors	• Professor • Professor's fellow researchers
Scenario	1. The professor retrieves the specified patient records from the PRS, and sends them to fellow researchers 2. The researchers receive and access the records
Variations	N/A
Benefits	• Researchers: can gain access to the required information • Professor: electronic transfer of the required information can provide efficient data sharing for group research activities
Issues	• Neither the professor nor the researchers can be sure that the sent or received information is from the respective person, and it has not been modified without authority or hacked (e.g. information leaked) during the transfer • The professor may need to manually select or delete information from the records to avoid some patients' personal information being exposed

Table 8-2 eHealthcare use case – Record healthcare history, published in [36]

Description	A healthcare sector member staff wishes to record a patient's healthcare information after providing the treatment
Actors	• Patient • Healthcare sector staff member
Scenario	1. Patient requires treatment and provides related information 2. Staff member retrieves the patient's healthcare history from PRS, and assesses the patient 3. Patient receives treatment 4. Staff member records the treatment process and result in PRS
Variations	If the patient has no record in the PRS yet, the staff member can create a new account
Benefits	• Patient: all treatment history is on record, no need to memorise them, specially the details in medical terms • Healthcare sector: maintain patients' healthcare history can provide efficient assessment, enable informed decision, and therefore, better treatment result
Issues	Records in PRS have risks: e.g. unauthorized modification, human errors, and database attacks. • Incorrect record will lead to wrong treatments • Loss of record or a whole database will affect the efficiency of assessments It is not easy for a patient to find out what is being held about them in the system, or to retrieve the information for any personal purposes (e.g. to forward it to a private healthcare provider)

Table 8-3 eHealthcare use case – Transferring healthcare information

Description	A staff member at healthcare sector A wishes to transfer a patient's healthcare information to a staff member at healthcare sector B
Actors	• A staff member at healthcare sector A • A staff member at healthcare sector B
Scenario	1. A patient at healthcare sector A is being referred to healthcare sector B 2. A staff member at healthcare sector A retrieves the specified patient record from PRS, and sends it to a staff member at healthcare sector B 3. The staff member at healthcare sector B receives and accesses the record
Variations	If the staff members at healthcare sectors A and B can access the same PRS, then only the patient's account information for retrieving the record is needed.
Benefits	• Patient: no need to handle the documents themselves • Healthcare sector: electronic transfer of the required information can provide efficient assessment, enable informed decision, and therefore, better treatment result
Issues	• The staff member at healthcare sector A cannot be sure that the receiver is the respective staff member at healthcare sector B, and the record has not been modified without authority or hacked (e.g. information leaked) during the transfer • The staff member at healthcare sector B cannot be sure the received information is sent from the respective staff member at healthcare sector A, and the record has not been modified without authority or hacked (e.g. information leaked) during the transfer The patient cannot be sure what is being transferred – patient's privacy is not satisfied

The relations of these stakeholders and use cases are shown diagrammatically in Figure 8-2, published in [36].

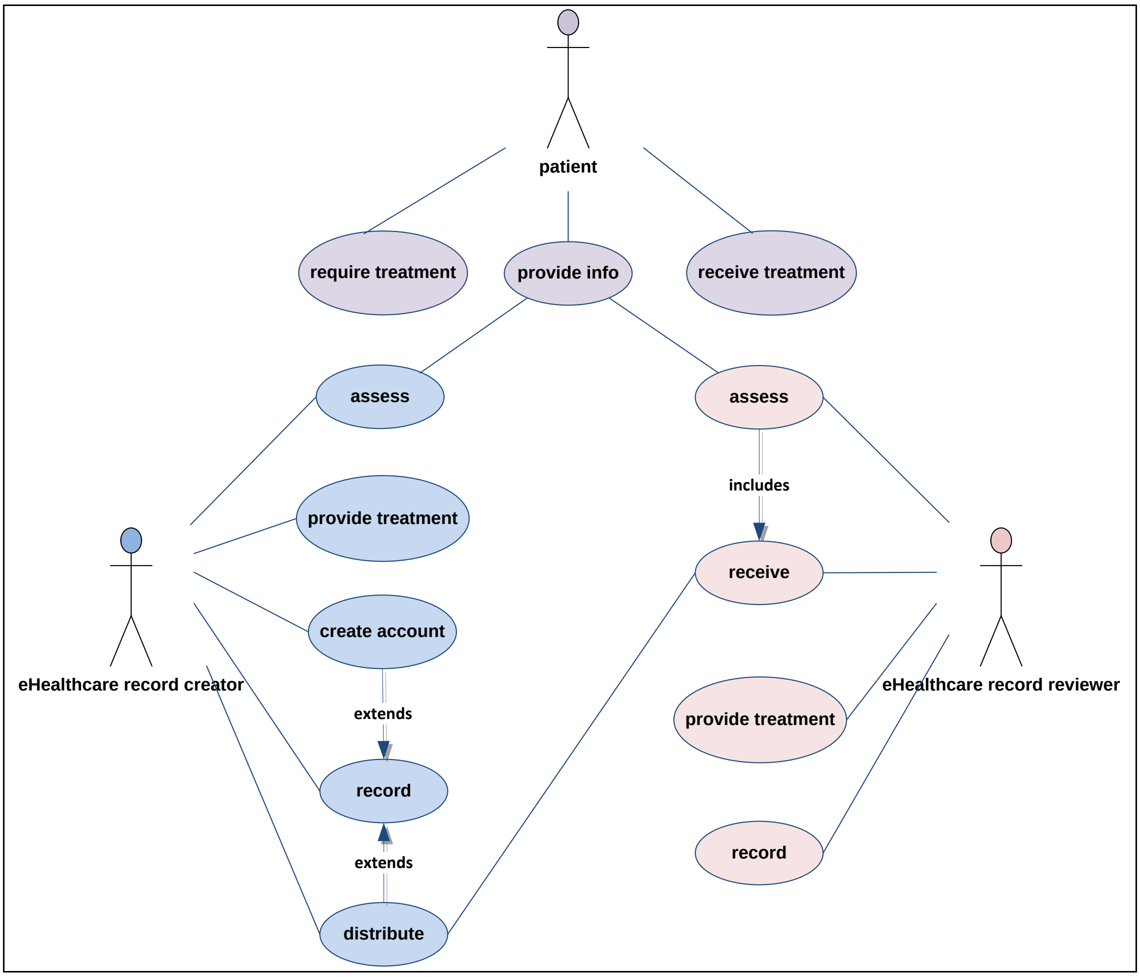


Figure 8-2 eHealthcare use case analysis

8.3.8 eHealthcare vs. eCertificate with eID

Comparison of the use cases of the three different systems shows that the implementation of the eCert protocol for eHealthcare is a mixed version of the eCertificate and eID applications, but with some unique features:

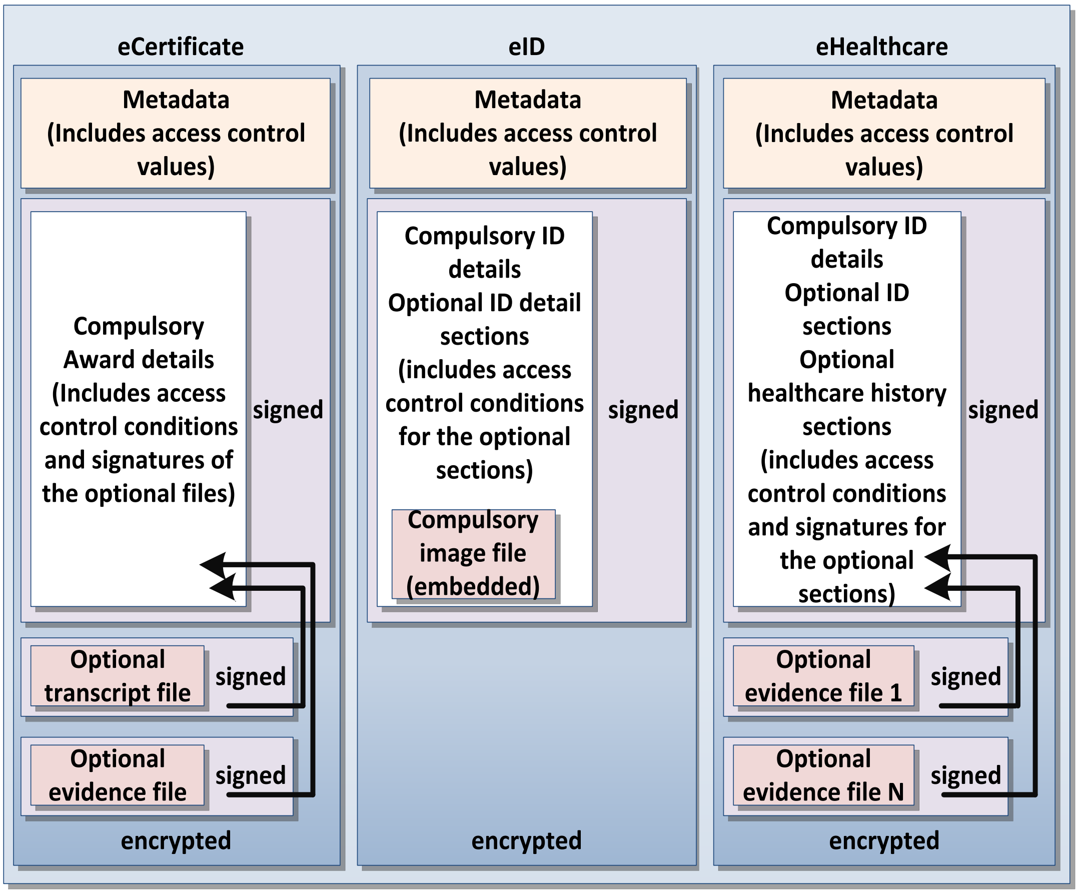

eCertificate
eID
eHealthcare
Metadata (Includes access control values)
Metadata (Includes access control values)
Metadata (Includes access control values)
Compulsory Award details (Includes access control conditions and signatures of the optional files)
signed
Optional transcript file
signed
Optional evidence file
signed
encrypted
Compulsory ID details Optional ID detail sections (includes access control conditions for the optional sections)
Compulsory image file (embedded)
signed
encrypted
Compulsory ID details Optional ID sections Optional healthcare history sections (includes access control conditions and signatures for the optional sections)
signed
Optional evidence file 1
signed
Optional evidence file N
signed
encrypted

Figure 8-3 Comparison of eCert file structures

- **File structure:** Unlike eCertificate and eID which are issued for personal use, an eHealthcare document may contain group information for research purposes, as well as for individual use. It should be constructed with optional text sections as in eID (e.g. to bind in some relevant data when required), and secured support files as in eCertificate (e.g. an image of a scan or x-ray). This is shown in Figure 8-3.
- **Usage control:** In both the eCertificate and eID applications, further transfer of the eDocument from the reviewer is prevented. However, in the case of eHealthcare, this should be allowed as the reviewer will normally also be a staff member in a certified healthcare sector, and they have the need and right to transfer the document further to the desired department. Therefore, not only the owner, but all stakeholders, should have usage control of the document. However, to protect information privacy, we need to ensure that only the specified reviewer can access it,

and no one should be able to access more information than they have received (no hidden information should be made available on further transmission). This is shown in Figure 8-4, published in [36].

- **Technical skills:** Unlike the case of eCertificate and eID, the information owners in the eHealthcare case are patients, who can be of any age, may be new to computing technologies, or may have no capability of managing their own documents. A way needs to be found so that they can have the required data in a simple but secure method.

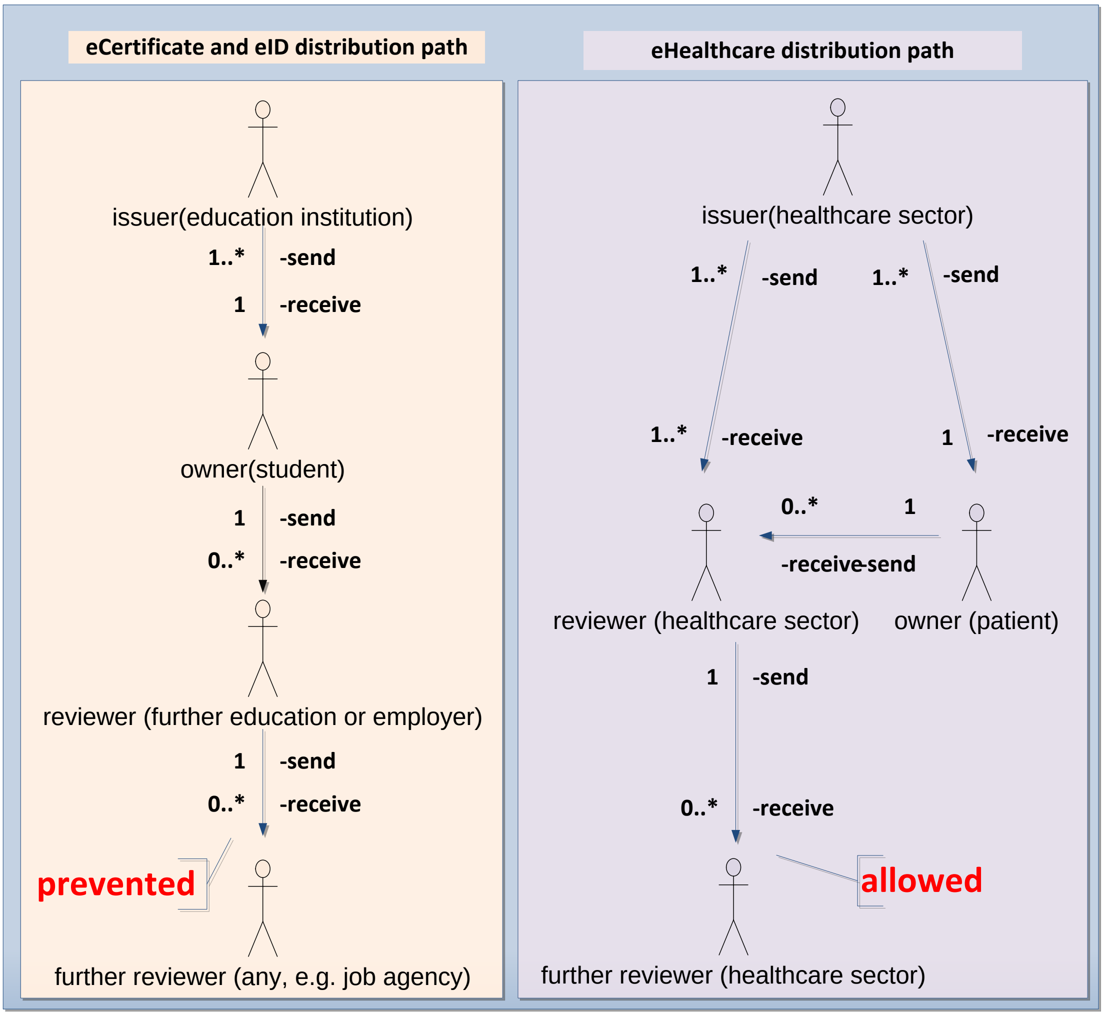

eCertificate and eID distribution path
issuer(education institution)
1..*
-send
1
-receive
owner(student)
1
-send
0..*
-receive
reviewer (further education or employer)
1
-send
0..*
-receive
prevented
further reviewer (any, e.g. job agency)
eHealthcare distribution path
issuer(healthcare sector)
1..*
-send
1..*
-send
1..*
-receive
1
-receive
0..*
1
-receive-send
reviewer (healthcare sector)
owner (patient)
1
-send
0..*
-receive
allowed
further reviewer (healthcare sector)

Figure 8-4 Document transmission paths

8.3.9 The Design

The eHealthcare application will be formed from two subsystems: issuing, and reviewing. These two subsystems will be installed locally in registered healthcare providers, and linked to the central eCert server. While these installed subsystems will only be accessed by authorized staff, there will also be an online publicly-accessed central reviewing subsystem for patients to view, set controls, and distribute their own documents.

The issuing subsystem will collect the required information from the PRS according to the specified input criteria, and will then sign and encrypt the document using the eCert protocol.

The reviewing subsystem will take the uploaded eHealth-eCert file as input, decrypt and verify the document against content modification, status validation, signing key revocation, access time limit, and then display the enabled visible sections. The user is allowed to set further access controls on the document after a successful verification process.

By applying the eCert protocol to eHealthcare, a digitally-signed eHealthcare document, an eHealth-eCert, can be created according to the specified criteria. Such an eHealth-eCert will follow the eCert user-centric approach, and will be secure to ensure confidentiality, integrity and availability during its issue, distribution, management, and verification processes. This is shown as use cases in Figure 8-5, published in [36].

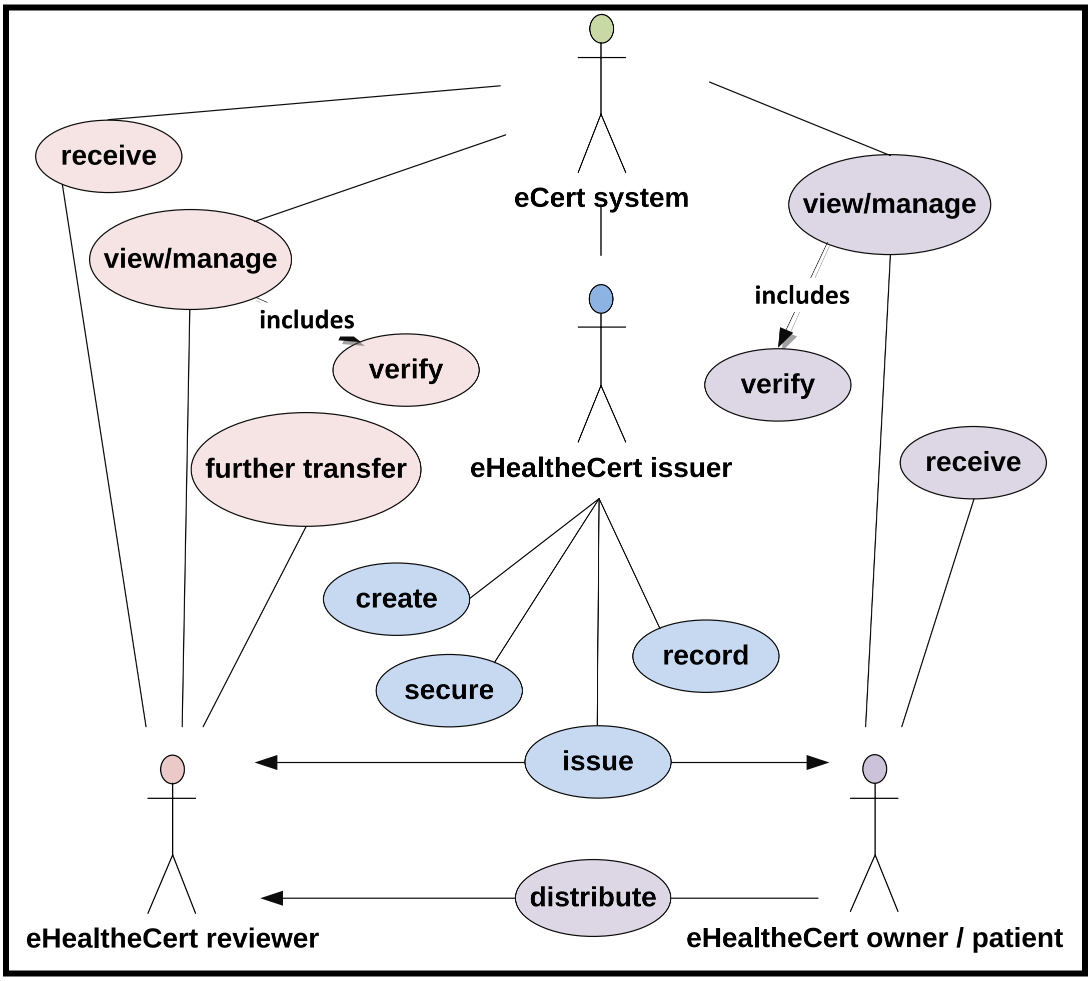


Figure 8-5 eHealthcare system use cases

Confidentiality is also called secrecy or privacy. It ensures that computer-related assets are accessed only by authorized parties. To address the information confidentiality issue in the case of the sharing of healthcare records, senders need to be able to select the required data that will be made available to which receiver and for how long. As all stakeholders can be both sender and receiver, they will all have the right to set access control values.

To ensure that no one can access more information than that which they have on receipt, they will not be able to make visible any optional non-display sections, and non-display files will not be included in further transfer. However, the title(s) of the hidden section(s) will be indicated, and the original document issuer can be traced. Therefore, the hidden information can be requested from the document issuer if needed.

Staff members will all have their own unique key pairs within the system. When transferring eHealth-eCert documents between healthcare sectors, unique encryption keys will be employed for each document to ensure that only the specified reviewer can access them.

When issuing the initial eHealth-eCert document to the patient, the system default encryption key will be employed to enable all stakeholders to access it. This appears to militate against privacy, but provides availability in an emergency situation when the information must be provided by an incapable patient. Patients can set a unique key to their documents through the reviewing subsystem when preferred. To backup the security issue, a log of access IPs will be maintained. In addition, a list of encrypting options could be provided for advanced users with specified privacy requirements. This use of keys is indicated in Table 8-4, published in [36].

Integrity in computing security implies that assets can be modified only when they are under authorized control, specifying who or what can access which resources and in what ways. In applying the eCert technique, the eCert signature method was employed with the corresponding system structure design so that the document access key would be verified, together with its signing key status, content status, expiry time, and access time. These should all be validated, with any unauthorized modifications being detected.

For an individual healthcare history, an eHealth-eCert can be created and made available to the patient. This can act as a backup to the PRS, in that it will not only address the availability issues in the case of loss of records, but will also benefit some patients. This is especially so for those who know they may require emergency treatment. They can even carry it with them, such as a bracelet style USB, to provide their certified identity and healthcare history. What is more, issuing an eHealth-eCert to a patient also gives them back control of their data. It addresses the information ownership right, since patients are now free to choose where, to whom, and how to present their personal data. They can even afford to choose “not to have their healthcare information collected and recorded in the healthcare information system”[143], as the eCert technique enables the document to be owner-controllable, verifiable, securely transferred, with lifetime validation, and easily backed up.

Table 8-4 eHealthcare system keys

Signing and verifying process		
Signing key	Issuer private key	
Verifying key	Issuer public key	
Encrypt and decrypt on issuing process		
Issuing path options	Encrypt key	Decrypt key
Within healthcare sector	Receiver public key	Receiver private key
Healthcare sector to patient with open access	System default public key	System default private key
Healthcare sector to patient with controlled access	Patient public key	Patient private key
Encrypt and decrypt on access control process for further transfer		
Transfer path options	Encrypt key	Decrypt key
Within healthcare sector	Receiver public key	Receiver private key
Healthcare sector to patient	System default public key	System default private key
Patient to any reviewers (Open access)	System default public key	System default private key
Patient to already known receiver	Receiver public key	Receiver private key
Patient to unknown specified receiver	Newly generated unique private key	The unique corresponding public key

8.3.10 Issues

The balance between data confidentiality and availability under security control in healthcare is extreme: on the one hand, the patients' data is considered as highly sensitive, and requires a high level of security; on the other hand, the information needs to be available in emergency events without any trapdoors.

The eHealthcare system was designed to maintain high level security when the document is transferred between healthcare sectors (signed, encrypted, and required unique access key), and low level security when issuing to the patient (with open access by default), but providing functions for the patients to upgrade the security level if required. This is aimed at availability, especially if the document is the only available verifiable information that is provided on an incapable patient in an emergency situation. Whether this approach is suitable or not could become the main security argument.

8.3.11 Evaluation

Through the eCert for eHealthcare study, the issues around eCertification in eHealth documents were identified. As a result, the eCert protocol was again reviewed, and a detailed eHealthcare system design was proposed. From the design, the file structure of the eCert protocol had been improved to suit various types of eCert document, and additional support functions are added to provide security control options. Although there is currently no system demonstrator to take the eHealthcare design forward, the changes could be easily made following this design once the implementation takes place.

By employing the eCert protocol, the eHealth-eCert document can be used standalone or in parallel with the PRS, as a secured and independently verifiable backup to the existing PRS. It could be the answer to the current healthcare information system security problems. It also provides advantages over the existing system, as it satisfies the information ownership right, and enables the owner to have control of their data. The design is independent of any particular implementation.

The outcome of the eHealthcare study indicates that the eCert protocol can be applied in a wide eDocument transmitting domain.

This study was evaluated by domain experts and published as a conference paper at the International Conference on Information Society (i-Society 2011)[36]

However, the proposed system was only developed at the theoretical level, and no system implementation and testing have been carried out at a technical level yet. Issues when theory is applied to practice still need to be explored.

8.4 The Abstracted eCert Protocol

After being evaluated in three different applied domains, the eCert protocol was improved to suit a wide range of file structure that may be required, for all types of user (including all ages, IT levels, and capabilities), in various environments.

8.4.1 Features

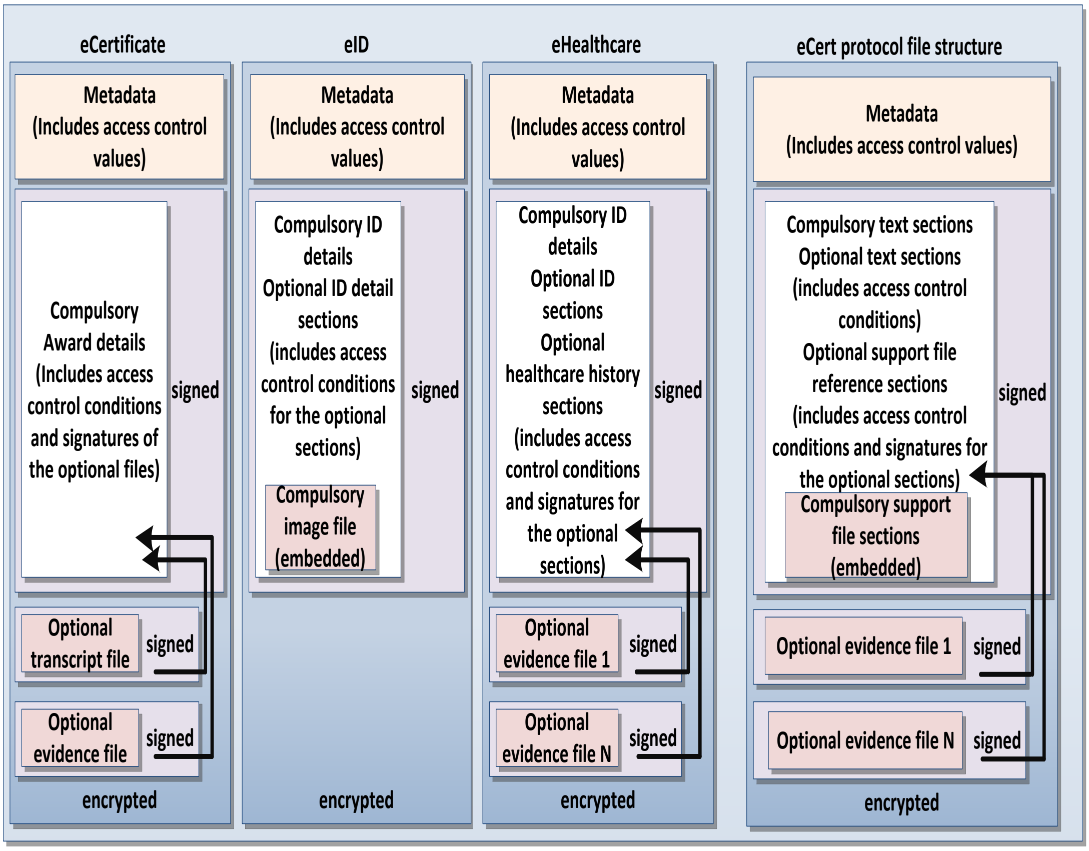
File structure: an eCert file will contain three types of data: metadata, text outputs, and file outputs (that can be in any format). These are constructed in three sections: metadata, main content section, and detached supported files section. Both the text content and the support files can be subdivided into two types: compulsory and optional. The text output will form the main content, whether compulsory or optional; the compulsory file outputs will be embedded within the main content, while the optional files will be attached. The improved file structure of the eCert protocol is shown in Figure 8-6, along with the comparison of the earlier designs.

Signing method: optional files will be signed individually using a detached signature. Their signature values and the reference URI will then be embedded within the main content under the corresponding display conditions. The document will then be signed using an enveloped signature, and encrypted before being distributed.

Keys management: the system will use the issuer's private key to sign the document, and use the system's default public key, or the receiver's public key to encrypt the document, depending on the applied situations or specified selected options. On review, the corresponding decrypt key, and the issuer's public key will be used for verification.

System structure: all supported systems will be installed locally in registered institutions, and linked to the eCert central server. In addition, an online central service will provide public access for the required management and verification service. In some cases, an identity management system will be involved in access control.

Usage control: the owner can choose who can see what and for how long by setting usage control on section display and access time limits with a unique access token.



eCertificate
Metadata (Includes access control values)
Compulsory Award details (Includes access control conditions and signatures of the optional files)
signed
Optional transcript file
signed
Optional evidence file
signed
encrypted
eID
Metadata (Includes access control values)
Compulsory ID details
Optional ID detail sections (includes access control conditions for the optional sections)
Compulsory image file (embedded)
signed
encrypted
eHealthcare
Metadata (Includes access control values)
Compulsory ID details
Optional ID sections
Optional healthcare history sections
(includes access control conditions and signatures for the optional sections)
signed
Optional evidence file 1
signed
Optional evidence file N
signed
encrypted
eCert protocol file structure
Metadata (Includes access control values)
Compulsory text sections
Optional text sections (includes access control conditions)
Optional support file reference sections (includes access control conditions and signatures for the optional sections)
Compulsory support file sections (embedded)
signed
Optional evidence file 1
signed
Optional evidence file N
signed
encrypted

Figure 8-6 eCert protocol file structure design

8.4.2 Advantages and Innovation

Secure: The eCert approach is based on digital signing, but also addresses what is called the "eCertificate squared" problem. Not only must the non-repudiation and the authenticity of the document be ensured, but the current validity to cover the potential revocation of the data must be detected as well as the classical case of the revocation of the signing key. This means it is more secure than conventional digital signing.

User-centric: By taking this approach, the ownership rights are addressed. The owner can not only store, manage, share and track their personal data, but can also tailor their documents to best support their needs. In this way, the information is "under their control, with their consent, and for their benefit [133]."

Lifetime Validation: The eCert signing method and system structure design ensure that all issued eCert files are independent of the issuing body. They can therefore be validated for life even if the issuing body ceases to exist.

Verifiable distributed data: The eCert signing method also enables the distributed eDocument to be verified through a supported service, without the need for storing the data. This provides the advantage of saving huge storage and dramatically avoids database attacks.

8.5 Proof of Hypotheses

From this research, it has been shown that Hypothesis 1 (the current technology has the required features that can be used or adapted to support the design and implementation of the eCertificate system, so that an eCertificate can be secured, rendered permanently verifiable and allow the student owner to have control over its use independently from its issuing body.) has been met. It has been described in Chapter 6 and has been tested and evaluated in Chapter 7:

1. Adapting the digital signature CRL method, maintaining the revocation lists for both the signer's key and the issued eCertificate, together with an automatic checking service against both of them. This not only solved the

eCertificate squared issue but also improved the security of the traditional digital signing with the verification process.

2. Employing a new file structure and a new signing method, allows the owner to set controls on the signed eCertificate through its metadata without invalidating the signature. This addressed the security issues of the new eCert system and satisfied the owner control requirement.
3. Applying number 1 and 2, together with a new system structure design, and providing a central management and verification system independent from the issuing body, solved the lifelong availability nationwide usage issues.

This research has also shown that the Hypothesis 2 (the concept of the eCertificate solution can be applied to related domains, such as other eDocuments that face similarly complex situations, to solve their security and ownership issues.) has been met. It has been demonstrated in Chapter 8:

4. Applying the eCert protocol to Mobile eID demonstrated that the concept of the eCertificate solution can be applied in a mobile environment
5. Applying the eCert protocol to the eHealthcare domain demonstrated that the concept of the eCertificate solution can be applied to the complex situations of patient data transmission

From the designs, demonstrators, and approval processes that have taken place, the hypothesis has been proved not only from the theoretical level, but also in practice.

8.6 Chapter Summary

The initial eCert protocol was formed through the development of the eCertificate system. It was tested through the eCert for ePortfolio subproject, and was evaluated through the Mobile eID subproject and the eHealthcare study. Step-by-step, the protocol was adjusted to suit the applicability requirements in various environments. The evaluation outcome indicated that the improved eCert protocol can be applied successfully in a wide range of eDocument transmitting domains.

Chapter 9 Summary, Conclusion, and Future Work

This chapter summarizes the research, outlines the journeys to achieving the outputs and outcomes, along with the lessons learned and the impacts. The dissertation ends with the conclusion, and proposals for future work.

This chapter is entirely the researcher’s own work. Some sections have been published in the eCert project website [28].

9.1 Research Summary

Through this research, a solution for a secured and user-centric eCertificate management system has been proposed. It has successfully addressed the eCertificate squared problem that exists within the traditional digital signing method when it is applied to non-static content eDocuments. It has defined an eCertificate file structure, so that it contains not only the qualification award information, but also the transcript information and any supporting evidence files, which can be in any format. It has proposed a new digital signing method to cooperate with the file structure and to meet the eDocuments’ ownership rights. The new signing method not only binds the related files together, but also allows the eCertificate owners to set access control on who can see the signed eDocument for what and for how long. Meanwhile it retains the integrity of the signature, without the need of re-signing by the initial issuing body; an additional encryption key is added after the signing to ensure that only the receiver with the corresponding decryption key can access the file. The research 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 expiry time, access period, ownership, signing key status, qualification award status, and owner controlled section display. The whole design works together to ensure the issued eCertificates can be securely distributed and verified independently from the issuing body and satisfy ownership rights, without requiring storage in the verification system. This method also provides huge advantages of lifetime validation and the avoidance of database attacks.

The protocol was tested and evaluated through its demonstrator by following the selected research methodology. The design principle was tested through a subproject, integrating eCert in ePortfolios, to evaluate the usage of eCertificates in other applications. The concept of the eCert solution was tested through a subproject, the Mobile eID, and a study of eCert for eHealthcare, to evaluate the applicability of this concept in wider situations. All the test and evaluation results were successful, indicating that the proposed eCert protocol will not only meet the eCertificate challenge, but also solve the eDocument transmission security issues, and can be applied to a wider domain.

9.2 Journeys to Achieving the Outcomes

The research topic was raised initially from personal interest in online certification for ePortfolios. After the background research, a secured eCertificate system was identified as the research focus. Two years into the research, a call for a government-funded project matched the research topic exactly, and with successfully winning the bid, the project named eCert enabled the researcher to lead a development team to visualise and construct a user-centric solution to the problem of maintaining confidentiality in a world of linked data. As the research has generated interest and gained momentum, it has become possible to explore the initial concept in more depth, to define more clearly what is at the heart of the “eCert” concept, and to develop examples of how the protocol may be applied in widely varying contexts. It has also been possible to develop some of these examples as practical demonstrators, which has led to a great depth of understanding the issues that arise when the theory is applied in practice.

The research has generated global interest from Australia to the USA and Canada, and led to 10 publications. Whilst focusing on dissemination in the UK, interaction with expert audiences worldwide has been extremely helpful in assessing and refining the eCert concept.

9.3 Hypotheses and Contributions

The eCertificate study is a new field in research worldwide. Through this research, the researcher proposed an eCertificate system, and proved that (hypothesis 1) the current technology has the required features that can be used or adapted to support the design and implementation of the eCertificate system, so that an eCertificate can be secured, rendered permanently verifiable and allow the student owner to have control over its use independently from its issuing body.

The researcher has also proposed the abstracted eCert protocol, and proved that (hypothesis 2) the concept of the eCertificate solution can be applied to related domains, such as other eDocuments that face similarly complex situations, to solve their security and ownership issues. This includes:

- identifying and addressing the $(\text{eCertificate})^2$ problem, which is a content validation issue raised in the verification process of digitally signed documents that contains non static content;
- defining the file structure of a complex eDocument that involved non static content, contained a wide range of file types, needed to be digitally signed and enabling authorized modification to access control values;
- designing a new signing method to enable owner control over the access of a digitally signed document without the need for digital re-signing;
- designing a new system structure to accompany the new signing method, which provides a centralized verification framework for digitally signed and owner-controlled distributed eDocuments;

The eCert protocol, which was proved through two evaluation studies, can provide a number of innovation advantages when it is applied to other eDocument transmission and verification domains, such as eGovernment, and eBusiness, this includes:

Security: The new signing method is based on digital signing while improving its security through addressing the (eCertificate)^2 problem. It validates the current status of the document content as well as the revocation of the signing key, which means it is more secure than conventional digital signing.

User-centric: The ownership rights are addressed such that the owner of the document can not only store, manage, share and track their personal data, but can also tailor their documents to best support their needs, so that it is "under their control, with their consent, and for their benefit [133]."

Lifetime Validation: The eCert signing method and system structure design ensure that all issued eCert files are independent of the issuing body. They can therefore be validated for life even if the issuing body ceases to exist.

Verifiable distributed data: The eCert signing method also enables the distributed eDocument to be verified through a supported service, without the need for storing the data. This provides the advantage of saving huge storage and dramatically avoids database attacks.

9.4 Research Methodologies

Two research methodologies were employed in this research: Service Orientated Reference Model (SORM) [173] and Delphi [88].

The SORM methodology was used to investigate the eCertificate system as it can help to better understand how services fit together to provide the required functionalities within the eFramework. The eCertificate research was developed following the four layers of the SORM methodology:

- In Chapter 3 and 4, literature review and domain research were carried out for the first layer, Domain Definition, to look into eCertificate-related areas to find out what is being studied in the field and explore what systems/projects are already available besides literature, what can be adapted, and what limitations need to be overcome. The outcome of identified issues and useful information were summarised and passed on to the next layer as the required Common Usage Patterns of the new system;

- With the usage patterns defined, the second layer of Use Cases study was carried out in Chapter 5 to formalise user activities; the corresponding gap analysis was also performed to identify if any of the use cases required services need to be addressed
- Based on the gap analysis result, a series of Service Profiles for each required use case were generated in Chapter 6. At this third layer, existing services that could be used or adapted, and the techniques to address the issues of required services were investigated.
- With the above preparation and the ideas of approaching the requirements, the fourth layer of Reference Implementation was finally carried out to implement the eCertificate system in Chapter 6 and evaluated in Chapter7.

The Delphi methodology is a “high accuracy forecasting tool” that can provide professional opinions efficiently. As the eCertificate is a new field of research, so at this starting point, the development and evaluation of the system was focused on the theoretical level, such as whether the related issues have been understood and the design is appropriate, rather than on the production level of how well the demonstration system performs. With this focus in mind, the Delphi methodology was employed, step-by-step alongside the SORM methodology, to guide the decision making and evaluate whether the proposed design meets all system requirements. These include:

- A panel of domain experts, include employment managers, IT security experts, ePortfolio experts, and exam board officers have be selected at national level to represent the eCertificate stakeholders;
- Two workshops were run during two stages of the development to collect professional opinions from these experts

  - The first workshop was run at the system design stage to evaluate and adjust the design at the strategic level. Comments, disagreements, and suggestions from the domain experts were collected, analysed, fed back, and the system design was also adjusted accordingly.
  - The second workshop was run at the system demonstrator completion stage to evaluate and adjust the design not only at the theoretical level but also at the technical level. Again, comments, disagreements, and suggestions from the domain experts were collected, analysed, fed back, and the system design was also adjusted accordingly.
- In addition to the two workshops with the selected domain experts, a few more presentations also took place at national and international computing security-related conferences to collect the opinions from a wider range of domain experts. After each round, feedback was reflected upon, and the system was adjusted accordingly.
- Towards the end of this research, positive feedback was received from conferences and workshops internationally while negative feedback was mainly related to the future work that could not be completed within the current project. So the Delphi method was effective in achieving a convergence of opinions.

9.5 Lessons Learned

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

The evaluation subprojects were initiated to implement the eCert concept, and they looked to be something that would provide valuable alternative tests. In the event, they proved not only successful, but also generated lots of interests.

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

At a different level, lessons have also been learnt about how to manage changes in plan, especially when dealing with a project. The eCert project has had its fair share of problems, including the departure of the main code developer halfway through the development cycle. This has been an object lesson in noting that risk assessment is not an arbitrary exercise done to meet requirements, but an essential part of pre-project planning.

9.6 Future Work

As a result of running the eCert project alongside the research, it is now known that the eCert protocol will work in practice in a variety of contexts, giving users control over who may see their data and for how long, thus giving them improved protection against identity theft, for example. The eCert code library was tested by two different groups of developers through the two subprojects, and refined to ensure it is easy to use.

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

1. A carefully-monitored trial with a specific group of students in a local institution (e.g. on a single course), with the paper-based system as a fallback scenario.
2. An institution-wide roll-out, again with students located within the institution.
3. A roll-out that crosses institutions, for example covering a local area, and with FE/HE cross-over, focussing on, say, the HE admissions boundary.

4. Alongside the ePortfolio roll-outs, it would be good to see a prototype system set up to evaluate the potential for student data to be kept on smartphones, so that university smartcards could be replaced by a smartphone app. The eCert project has demonstrated how this may be achieved securely and operated simply.
5. The eCert for ePortfolio implementation subproject indicated that there are issues relating to the implementation of eCert within different ePortfolio systems. This could be worth evaluating, although it does not relate to the value of the eCert protocol itself, but on the design of the ePortfolio system.
6. A further development of the eCert protocol would be to use it to cover areas of student-related documentation that are currently problematic, such as files relating to disability, periods of ill-health, and matters relating to "Special Considerations". The eCert protocol gives a solution to enable time-limited access for restricted groups to sensitive information. Thus a member of a "Special Considerations" panel could be granted access to a student's personal information for the duration of the panel meeting only. This application is currently only at the design stage, so it needs to be built and tested first to ensure that it works before it can be evaluated in practice.

9.7 Conclusions

There is a tension in the world of security between a desire to keep control of data centrally, and putting control into the hands of the user. In the world of ePortfolios, confirmation of award data is currently only possible via a centralised service. Following the SORM and Delphi methodologies, this research has proposed a new eDocument signing method, along with other supported functions and new system designs, has solved what is called the "eCertificate squared" problem, and has developed a test system to investigate the issues that arise when control of award data is put in the hands of users.

With further evaluation subprojects of eCert for ePortfolio, Mobile eID, and the study of eHealthcare, the abstracted requirements for secured eDocument transmitting have been captured. Step-by-step, the eCert protocol has been adjusted and improved accordingly.

The eCert protocol is an entirely new concept. Both the use of eCert in an ePortfolio context, and the use of eCert in a mobile eID context have created considerable interest. Interest has been expressed by eWork, the Australian Flexible Learning Framework project, with regard to ePortfolio usage, interest from the University of Sapienza with regard to developing the mobile eID aspect of eCert, and interest in eCert with regard to the secure transfer of documents. From the results of this research, it is clear that the eCert protocol is not just a solution to the problem of putting control of ePortfolio award data into the hands of the user, which was its initial intention; it is now a useful solution to a wide range of problems. The outcome indicated that the improved eCert protocol can be applied successfully in a wide range of eDocument transmitting domains.

The eCert protocol design has been published, together with the applied example systems, source code, and related documentation. It is therefore available for anyone to use and to implement an eCert solution in their own applications.

References

1. Abrami, P.C. 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, 2005. **31**(3 Fall/Automne).
2. Acquisti, A. and J. Grossklags, *Privacy and rationality in individual decision making.* IEEE Security and Privacy, 2005. **3**(1): p. 26-33.
3. activ8.org. *Fun stuff - eCertificates*. 13/01/2009]; Available from: http://www.activ8.org/funStuff_eCertificates.cfm.
4. Adams, A. and A.L. Cox, *Questionnaires, in-depth interviews and focus groups*, in *Research Methods for Human Computer Interaction*, P. Cairns and A.L. Cox, Editors. 2008, Cambridge University Press. p. 17-34.
5. Adams, A., P. Lunt, and P. Cairns, *A qualititative approach to HCI research*, in *Research Methods for Human-Computer Interaction*. 2008, Cambridge University Press. p. 138-157.
6. Adams, A. and A. Sasse, *The user is not the enemy*, in *Security and Usability: Designing secure systems that people can use*, Cranor Lorrie Faith and Garfinkel Simson, Editor. 2005, USA: O'Reilly. p. 610-630.
7. Ahn, J. (2004) *Electronic portfolios: Blending technology, accountability and assessment*. Transforming education through technology [18/08/2007]; Available from: http://thejournal.com/articles/2004/04/01/electronic-portfolios-blending-technology-accountability--assessment.aspx
8. Sufyan, T., and A. Adb-alrazzaq. *Combining mediated and identity-based cryptography for scecuring email*. in *International Conference on Digital Enterprise and Information Systems (DEIS 2011)*. E.E.-Q. Ezendu Ariwa, Editor. 2011, Springer Berlin Heidelberg: London, UK. p. 1-15
9. Albisser, A.M., J.B. Albisser, and L. Parker, *Patient confidentiality, data security, and provider liabilities in diabetes management.* Diabetes Technology & Therapeutics, 2003. **5**(4): p. 631-640.
10. Anderson, R. and S. Fuloria. *Certification and evaluation: A security economics perspective*. in *IEEE Conference on Emerging Technologies & Factory Automation (ETFA 2009)*. 2009. Mallorca, Spain: IEEE. p. 1-7
11. Argles, D., L. Chen-Wilson, and T. Guan. *Solving the e-Portfolio Certificate Problem*. in *AACE World Conference on Educational Multimedia, Hypermedia and Telecommunications (EdMedia 2010)*. 2010. Toronto, Canada.Copyright by AACE
12. Austin, L.M., *Is Consent the foundation of fair information practices? Canada's Experience Under PIPEDA.* University of Toronto Law Journal, 2006. **56**(2): p. 181-215.

13. Bangerter, E., D. Gullasch, and S. Krenn, *Cache games – bringing access-based cache attacks on AES to practice*, in *IEEE Symposium on Security and Privacy* 2011: California, USA. p. 490-505.
14. Basu, S. and R.G. Schroeder, *Incorporating judgments in sales Forecasts: Application of the Delphi method at American Hoist & Derrick.* Interfaces, 1977. **7**(3): p. 18-27.
15. Bernstein, D.J. *Cache-timing attacks on AES*. 2005 22 May 2012]; Available from: http://cr.yp.to/papers.html#cachetiming.
16. Biryukov, A., O. Dunkelman, N. Keller, D. Khovratovich, A. Shamir, (2009) *Key recovery attacks of practical complexity on AES variants with up to 10 rounds*.
17. Biryukov, A. and D. Khovratovich, *Related-key cryptanalysis of the full AES-192 and AES-256*, in *Advances in Cryptology - ASIACRYPT*. 2009, Springer: Berlin Heidelberg. p. 1-18.
18. Bishop, M., *What is computer security?* IEEE Security & Privacy, 2003. **1**(1): p. 3.
19. Bloustein, E.J., *Privacy as an aspect of human dignity: An answer to Dean Prosser*, in *NYUL Review*. 1964, HeinOnline. p. 962.
20. Blowers, R., *Individual development project (IDP) Report on ePortfolio Research*. 2008, University of Southampton.
21. Bogdanov, A., D. Khovratovich, and C. Rechberger. *Biclique cryptanalysis of the full AES*. in *Advances in Cryptology - ASIACRYPT*. 2011. Berlin Heidelberg: Springer
22. Boyle, J.M., E.S. Maiwald, and D.W. Snow, *Apparatus and method for providing multi-level security for communication among computers and terminals on a network*, 1996, Washington, DC: U.S. Patent and Trademark Office, 5,577,209, issued Nov 19, 1996
23. BREGLOBAL. *Certification*. 2007 10/03/2011]; Available from: http://www.bre.co.uk/page.jsp?id=1762.
24. Butler, P. (2006) *eCDF ePortfolio project: A review of the literature on portfolios and electronic portfolios*.
25. Canada, M. (2002) *Assessing e-folios in the on-line class*. New Directions for Teaching and Learning, p. 69-75.
26. Cavoukian, A. (2006) *Seven Laws of Identity: The case for privacy-embedded laws of identity in the digital age*.
27. Challis, D., *Towards the mature ePortfolio: Some implications for higher education*. Canadian Journal of Learning and Technology, 2005. **31**(3).
28. Chen-Wilson, L. *The eCert Project*. 2010 [cited 2010; Available from: http://ecert.ecs.soton.ac.uk/.
29. Chen-Wilson, L., and Argles, D. *Towards a framework of a secure e-Qualification certificate system*. in *2nd International Conference on Computer modeling and simulation (ICCMS)*. 2010. SanYa, China: IEEE. p. 493-500
30. Chen-Wilson, L., R. Blowers, A. Gravell, and D. Argles, *Towards a secured e-Certificate system for use in e-Portfolios*. in *International conference on Multimedia and Information and Communication Technologies in Education (m-ICTE)*. 2009. Lisbon, Portugal
31. Chen-Wilson, L., L. Gilbert, G. Wills, A. Gravell, and D. Argles, *A user-centric approach for secured eDocument transmission: Digital signing practical issues*

and the eCert solution. International Journal for Information Security Research, 2011. **1**(3). p. 94-105

32. Chen-Wilson, L., 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)*. 2011. London, UK.Copyright by IEEE. p. 93-99
33. Chen-Wilson, L., T. Guan, and D. Argles. *E-qualification certificate system for E-Portfolio*. in *17th International Conference of the Association for Learning Technology (ALT-C 2010)*. 2010. Nottingham, UK
34. Chen-Wilson, L., P. Royce, P. Newcombe, S. Ong, T. Wonnacott, G. Wills, and D. Argles, *Secure certification for e-Portfolios*. in *World Conference on Educational Multimedia, Hypermedia and Telecommunications (ED-MEDIA)*. 2008. Vienna, Austria: Joseph Luca & Edgar R. Weippl
35. Chen-Wilson, L., P. Royce, P. Newcombe, S. Ong, T. Wonnacott, G. Wills, and D. Argles, *Secure certification for e-Portfolios*. in *8th International Conference on Advanced Learning Technologies (ICALT)*. 2008. Santander, Spain: IEEE
36. Chen-Wilson, L., X. Wang, G. Wills, D. Argles, and C. Shoniregun, *Healthcare data management issues and the eCert solution*. in *International Conference on Information Society (i-Society 2011)*. 2011. London, UK: IEEE.Copyright by IEEE. p.114-119
37. CHESICC. *The certificate information verification services in China*. 2005 02 September 2008]; Available from: http://www.chsi.com.cn/about_en/.
38. Cohen, J., *What privacy is for.* Harvard Law Review, 2013. **126**.
39. Coppersmith, D., *Small solutions to polynomial equations, and low exponent RSA vulnerabilities.* Journal of Cryptology, 1997. **10**(4). p.233-260
40. Custer, R.L., J.A. Scarcella, and B.R. Stewart, *The modified Delphi technique-A rotational modification.* Journal of Vocational and Technical Education, 1999. **15**(2).
41. Davis, J., *Digital signatures application guidelines on digital signature practices for common criteria security*, in *MSDN Magazine*. 2009.
42. digiproofs. *Definition*. 2007; Available from: http://www.digiproofs.com/.
43. Digitary. *Secure electronic documents*. 2008 12 August 2008]; Available from: http://www.digitary.net/aboutus.htm.
44. Doddrell, G.R., *Information security and the Internet.* Internet Research, 1996. **6**(1): p. 5-9.
45. DSA. *FIPS-186, the first version of the official DSA specification*. 1991; Available from: http://www.itl.nist.gov/fipspubs/fip186.htm.
46. DSA. *FIPS-186-3, the third and current revision to the official DSA specification*. 2009; Available from: http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf.
47. El Gamal, A., *A public key crytosystem and signature scheme for based on discrete logarithms.* IEEE Transactions on Information Theory, 1985. **IT-31**(4): p. 469-472.
48. Etzioni, A., *A communitarian perspective on privacy.* Conn. Law Review, 1999. **32**: p. 897.
49. Etzioni, A., *Are new technologies the enemy of privacy?* Knowledge, Technology & Policy, 2007. **20**(2): p. 115-119.
50. EU Directive, *95/46/EC of the European parliament and of the council of 24 October 1995 on the protection of individuals with regard to the processing of*

personal data and on the free movement of such data. Official Journal of the European Communities, 1995. **281**: p. 31-50.

51. European Communities, *Ceritficate supplement: Advanced certificate craft - electrical*. 2007, European Communities.
52. European Communities. *Information on Europass Certificate Supplement navigate action*. 2008 [28 January 2008]; Available from: http://europass.cedefop.europa.eu/europass/home/vernav/
53. European Union. *Opening doors to learning and working in Europe: Information On Europass Certificate Supplement*. 2004 [28 January 2010]; Available from: http://europass.cedefop.europa.eu/europass/home/hornav/Introduction.csp.
54. FDA, *FDA electronic submissions gateway (ESG) user guide*, FDA, Editor. 2010.
55. National Communications System (US). Technology & Standards Division, and United States. General Services Administration Information Technology Section. *Telecommunications: Glossary of Telecommunication Terms*. Rowman & Littlefield, 1997.
56. Ferguson, N., B. Schneier, M. Stay, D. Wagner, and D. Whiting *Improved cryptanalysis of rijndael, fast software encryption*, in *Fast software encryption*. 2001, Springer Berlin Heidelberg. p. 213-230.
57. FISMA, *Federal information security management Act of 2002 (Title III of E-Gov)*. 2002, National Institution of Standards and Technology - information technology Laboratory.
58. Ford, M.D., *Identity authentication and 'e-commerce'*. The Journal of Information, Law and Technology, 1998. **3**(3).
59. Council, Financial Reporting. "Key facts and trends in the accountancy profession." *Financial Reporting Council, London* (2013).
60. Furr, A. *eFolio: University of Southampton ePortfolio system*. [cited 2009; Available from: http://www.efolio.soton.ac.uk/.
61. Gibbs, P., *Work-based quality: a collusion waiting to happen?* Quality in Higher Education, 2013. **19**(1): p. 1-6.
62. Gilbert, H. and T. Peyrin, *Super-Sbox cryptanalysis: Improved attacks for AES-like permutations*, in *Fast Software Encryption*. 2010, Springer Berlin Heidelberg. p. 365-383.
63. Gladney, H.M., *Durable evidence*. Preserving Digital Information, 2007: p. 219-234.
64. Gleichauf, R.E., W. A. Randall, D.M. Teal, S.V. Waddell, and K.J. Ziese., *Method and system for adaptive network security using network vulnerability assessment*, 2001, Washington, DC: U.S. Patent and Trademark Office, 6,301,668, issued October 9, 2001
65. Goldwasser, S., S. Micali, and R. Rivest, *A digital signature scheme secure against adaptive chosen-message attacks*. SIAM Journal on Computing, 1988. **17**(2): p. 281-308.
66. Grant, S. *Clear e-portfolio definitions: a prerequisite for effective interoperability*. in *ePortfolio conference*. 2005. Cambridge, UK
67. Grey, L. (2007) *e-Portfolios - An overview of JISC activities*. JISC.
68. Grimaila, M.R. and L.W. Fortson. *Towards an information asset-based defensive cyber damage assessment process*. in *IEEE Symposium on*

Computational Intelligence in Security and Defense Applications (CISDA 2007). 2007: IEEE

69. Grossman, S.J. and O.D. Hart, *The costs and benefits of ownership: A theory of vertical and lateral integration.* Journal of Political Economy, 1986. **94**(4): p. 691-719.
70. Grove, A., *What I've learned*, in *Esquire*. 2000. Available from: http://www.esquire.com/features/what-ive-learned/learned-andy-grove-0500
71. Hartnell-young, E., A. Smallwood, S. Kingston, P. Harley, (2007) *The impact of eportfolios on learning*.
72. Hartnell-Young, E., A. Smallwood, S. Kingston, P. Harley, *Joining up the episodes of lifelong learning: A regional transition project.* British Journal of Educational Technology, 2006. **37**(6): p. 853-866.
73. H åstad, J. *N using RSA with low exponent in a public key network*. in *Advances in Cryptology - CRYPTO 85*. 1986. Santa Barbara, California, USA: Springer Berlin Heidelberg
74. Hathaway, L., *National policy on the use of the advanced encryption standard (AES) to protect national security systems and national security information*, 2003, NSA,
75. Hershey, P.C., D.B. Johnson, A.V. Le, S.M. Matyas, J.G. Waclawsky, and J.D. Wilkins, *Network security system and method using a parallel finite state machine adaptive active monitor and responder*, 1995, Washington, DC: U.S. Patent and Trademark Office, 5,414,833, issued May 9, 1995
76. Higgs, P., J. Smith, A. Miller, K. Edgar, E. Bailey, P. Blee, and K. Gooding, *Trust federation user consultation and use-case collation*, 2010, University of Southern Queensland's Link Affiliates,
77. Hilbert, M., I. Miles, and J. Othmer, *Foresight tools for participative policy-making in inter-governmental processes in developing countries: Lessons learned from the eLAC Policy Priorities Delphi.* Technological Forecasting and Social Change, 2009. **76**(7): p. 880-896.
78. Hiltz, S.R. and M. Turoff, *Network nation, Revised edition: Human communication via computer*. 1993: Mit Press.
79. IMS Global Learning Consortium. *IMS ePortfolio best practice and implementation guide*. Version 1.0 Final Specification 2008 2008]; http://www.imsglobal.org/ep/epv1p0/imsep_bestv1p0.html.
80. Ireland, D. *RSA algorithm*. 2011; Available from: http://www.di-mgt.com.au/rsa_alg.html#weaknesses.
81. Johnson, T.R., *Book III: Retrenchment and reform, 1972-1980*. American Cryptology during the Cold War, 1945-1989. 2009: NSA. 232.
82. Kaliski, B. *Raising the standard for RSA signatures: RSA-PSS*. 2003; RSA Laboratories]. Available from: http://www.rsa.com/rsalabs/node.asp?id=2005.
83. Kaur, H. and M.A. Alm, *Implementation of portion approach in distributed firewall application for network security framework.* arXiv preprint arXiv:1201.4555, 2012.
84. Klenowski, V., S. Askew, and E. Carnell, *Portfolios for learning, assessment and professional development in higher education.* Assessment and Evaluation in Higher Education, 2006. **31**(3): p. 267-286.
85. Le Gendre, O., *Synthesis and structural modification of the MDMA antagonist nantenine: A naturally occuring aporphine alkaloid*. 2010, City University of New York.

86. Lee, E.S., Essays About Computer Security, 1999, *Centre for communications systems research*, Cambridge, Available from: http://www.cl.cam.ac.uk/~mgk25/lee-essays.pdf
87. Lessig, L., *Code: And other laws of cyberspace, Version 2.0*. 2006: Basic Books.
88. Linstone, H.A. and M. Turoff, *The Delphi method: Techniques and applications*. 2002. p. 618.
89. Lorenzo, G. and J. Ittelson (2005) *An overview of e-portfolios*.
90. Loshin, D. (2004) *Knowledge integrity: Data ownership*.
91. Lysyanskaya, A., *Signature schemes and applications to cryptographic protocol design*, in *Electrical Engineering and Computer Science*. 2002, Massachusetts Institute of Technology (MIT): United States.
92. Macnamara, D., C. Drury, and N. Ward, *Verifying VET learner attainment data - An investigation of learner verification services and third party verification needs,* 2010, University of South Queensland Link Affiliates, Available from: http://www.voced.edu.au/content/ngv45627
93. Macnamara, D., N. Nicholas, and A. Miller (2011) *Accessing VET learner attainment data: an investigation to enable learner-facilitated electronic access to their VET learner attainment data*. The Tertiary Education Research Database - education for work and beyond, 68.
94. Majchrzak, T.A. and C.A. Usener. *Evaluating e-Assessment for exercises that require higher-order cognitive skills*. in *System Science (HICSS), 2012 45th Hawaii International Conference on*. 2012: IEEE
95. Mao, W., *Modern cryptography: Theory & Practice*. 2004, New Jersey: Prentice Hall Professional Technical Reference. 308.
96. Martinovic, D. and V. Ralevich, *Privacy issues in educational systems.* International Journal for Internet Technology and Secured Transactions, 2007. **1**: p. 132-150.
97. Mayhew, R., *The communism of property: A note on aristotle.* The Classical Quarterly, 1995. **45**(2): p. 566.
98. McCrea, J.-A., Q. Hanich, and M. Tsamenyi, *Discussion paper: Australia's ability to meet the requirements of European Commission Regulation No. 1005/2008'establishing a community system to prevent, deter and eliminate illegal, unreported and unregulated fishing.* Faculty of Law-Papers (Archive), 2009.
99. McKinley, B. (2001) *The ABCs of PKI: Decrypting the complex task of setting up a public-key infrastructure*.
100. Microsoft. *Microsoft certified professional and office specialist exams*. 2008 02/03/2008]; Available from: http://www.microsoft.com/learning/mcpexams/default.mspx.
101. Microsoft, *Microsoft TechNet product documentation - Technical reference for cryptographic controls used in configuration manager*, 2012, Available From: http://technet.microsoft.com/en-us/library/hh427327.aspx
102. Microsoft.com. *Microsoft certifications overview*. 2008 02/03/2008]; Available from: http://www.microsoft.com/learning/mcp/default.mspx.
103. Naedele, M., *Standards for XML and web services security*. Computer, 2003. **36**(4): p. 96-98.

104. National Institute of Standards and Technology, *Recommendation for the Triple Data Encryption Algorithm (TDEA) block cipher* Version 1.1, NIST Special Publication 800-67

105. Network Working Group, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, 2008, RFC5280

106. NIST, *Announcing the advanced encryption standard (AES)*, 2001, United States National Institute of Standards and Technology (NIST), Federal Information Processing Standards Publication 197

107. NIST, *Recommendation for key management*, 2007,

108. Nottingham University. *Nottingham University ePortfolio project*. 2007 28/01/08]; Available from: http://www.nottingham.ac.uk/eportfolio/.

109. Novell. *How do I certify?* 2008 13/04/2008]; Available from: http://www.novell.com/training/certinfo/howdoi.html.

110. O'Donnell, M.L., *FERPA: Only a piece of the privacy puzzle.* Journal of College and University Law, 2003. **29**(3): p. 679-717.

111. O'Reilly, T. *What is Web 2.0?* 2005 05 March 2008]; Available from: http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html.

112. Olivier, B., T. Roberts, and K. Blinco. *The e-framework for education and research: an overview*. 2005 [cited 2013 July]; Available from: www.eframework.org.

113. Pacific, K. *Mahara: Open source eportfolios*. 2013; Available from: http://mahara.org/.

114. Papazoglou, M., *Service-orientated computing: Concepts, characteristics and directions*, in *International Conference on Web Information Systems Engineering*. 2003, IEEE: Rome.

115. PEPPOL. *Pan-European public procurement online*. Making procurement better 12 Feb 2011]; Available from: http://www.peppol.eu/.

116. Perlman, R., *An overview of PKI trust models.* IEEE Network, 1999. **13**: p. 38-43.

117. Pfleeger, C., and S.L. Pfleeger, *Security in computing*. 4th ed. 2007: Prentice Hall.

118. Pomin, T. and J.P. Stern. *Digital signatures do not guarantee exclusive ownership*. in *Applied Cryptography and Network Security: 3rd International Conference (ACNS 2005)*. 2005. New York, NY, USA

119. Pronichkin, *Certificate revocation list (CRL) verification - an application choice*. 2012 12 Jan 2013]; 29 Jul 2012:[Available from: http://social.technet.microsoft.com/wiki/contents/articles/964.certificate-revocation-list-crl-verification-an-application-choice.aspx.

120. PROQUIS. *ISO/IEC 17799: Information technology/security techniques/code of practice for information security management*. 2005 08/11/2008]; Available from: http://www.proquis.com/RESOURCES/standards/ISO-IEC_17799/.

121. Razavi, M. and L. Iverson. *A grounded theory of information sharing behaviour in a personal learning spaces*. in *20th Anniversary conference on Computer Supported Cooperative Work*. 2006. Alberta: ACM

122. Redman, J., M. Warren, and W. Hutchinson, *System survivability: A critical security problem.* Information management & computer security, 2005. **13**(3): p. 182-188.

123. Rees-Jones, P. *Building a Reference Model for ePortfolio*. 2007 28/01/08]; Available from: http://www.elframework.org/refmodels/epll/.
124. Rees-Jones, P., A. Smallwood, and S. Kingston, *e-Portfolio for Lifelong Learning Reference Model Project (eP4LL)*, 2006, University of Nottingham, JISC Development Project Report
125. Rees-Jones, P., A. Smallwood, and S. Kingston, *Specifying an e-Portfolio: a personal view*, 2006, *CETIS/JISC*, University of Nottingham.
126. Regan, P.M., *Legislating privacy: Technology, social values, and public policy*. 1995: Univ of North Carolina Press.
127. Rice, R.A., *Teaching and learning first-year composition with digital portfolios*. 2002: Indiana. p. 276.
128. Rivest, R., A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems.* Communications of the ACM, 1978. **21** (2): p. 12-126.
129. Roberts, G. W. Aalderink, J. Cook, M. Feijen, J. Harvey, S. Lee, and V. P. Wade, *Reflective learning, future thinking: digital repositories, e-portfolios, informal learning and ubiquitous computing*. in *ALT/SURF/ILTA Spring Conference*. 2005. Dublin
130. Rosen, J., *The web means the end of forgetting*, in *The New York Times*. 2010. Available from: http://www.lucasvg.com/buzz/The%20Web%20Means%20the%20End%20of%20Forgetting.pdf
131. Rowe, G. and G. Wright, *Expert opinions in forecasting. Role of the Delphi technique*, in *Principles of Forecasting*. 2001, J. Armstrong. p. 125-144.
132. Royce, P., P. Newcombe, S. Ong, T. Wonnacott, *Report on on-line authentication of qualification records*, 2008, MSc Computer Science Group Development Project, University of Southampton,
133. Sadd, G., *What do you think I am: Trusted relationship management*, in *London Learning Forum*. 2010: London, UK.
134. Sale, J.E.M., L.H. Lohfeld, and K. Brazil, *Revisiting the quantitative-qualitative debate: Implications for mixed-methods research.* Quality and Quantity, 2002. **36**(1): p. 43-53.
135. Saunders, M., P. Lewis, and A. Thornhill, *Research methods for business students*. 5th ed. Pearson Education 2009: Trans-Atlantic Publications Inc.
136. Schneier, B., *Liars and Outliers: Enabling the trust that society needs to thrive*. 2012: Wiley.
137. Schneier, B., N. Ferguson, and T. Kohno, *Cryptography engineering - Design principles and practical applications*. 2010: John Wiley & Sons. 384.
138. Schneier, B., J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, T. Kohno, M. Stay, (2000) *The twofish team's final comments on AES selection*. AES Round 2 Information - AES Development Effort.
139. searchsecurity. *SearchSecurity research library*. 2007 07/08/2008]; Available from: http://searchsecurity.bitpipe.com/.
140. Security Associates. *The information security glossary*. 2001; Available from: http://www.yourwindow.to/information-security/gl_informationowner.htm.
141. Selkirk, A., *Using XML security mechanisms.* BT Technology Journal, 2001. **19**(3): p. 35-43.
142. Shade, L.R., *Reconsidering the right to privacy in Canada.* Bulletin of Science, Technology & Society, 2008. **28**(1): p. 80-91.

143. Shoniregun, C.A., *Security comprehension of healthcare information systems*, in *IEEE World Congress on Internet Security (WorldCIS)*. 2011: London, UK.

144. Shore, J.H. and S.C. Schreiber, *Certification, recertification, and lifetime learning in psychiatry*. 1st ed. 1994: American Psychiatric Press, Inc. 224.

145. SmartDraw.com. *Powerful Business Graphics*. 08 July 2008]; Available from: www.SmartDraw.com.

146. Smith, A. and R.P. Hanley, *The theory of moral sentiments*. 2010: Penguin Classics.

147. SPOCS. *Building the next generation points of single contact*. 2012 [18 Feb 2013]; SPOCS is an EU co-funded project CIP-ICT PSP-2008-2 no238935]. Available from: http://www.eu-spocs.eu/.

148. Sridhar, M.S. *Research Methodology: PART 1 Introduction to research & research methodology*. 2009 [18 October 2009]; Available from: http://sciencestage.com/uploads/text/AOHpZs2hDHvMeYDhHCm5.pdf.

149. Stallings, W., *Cryptography and network security: principles and practice*. 2006: Prentice Hall. p73.

150. Stevens, J.F., R.A. Caralli, and B.J. Willke, *Information asset profiling*, 2005, Carnegie-Mellon University of Pittsburgh, PA, Software Engineering Institute, CMU/SEI-2005-TN-021

151. Strudler, N. and K. Wetzel, *Electronic portfolios in teacher education: Issues of initiation and implementation.* Research on Technology in Education, 2005. **37**(4): p. 411-433.

152. Sturcke, J., *Government offers reward in hunt for lost data*, in *Guardian*. 2007.

153. Sunday, O. and E.A. Popo-ola, *Accessing e-Banking based on resilient transaction*. 2008.

154. Tanenbaum, A., *Computer networks*. 4th ed. 2002: Pearson Education.

155. TechTarget, *Definitions* 2007, SearchSoftwareQuality.com

156. Terziovski, M., D. Samson, and D. Dow, *The business value of quality management systems certification. Evidence from Australia and New Zealand.* Journal of Operations Management, 1997. **15**(1): p. 18.

157. Toch, E., Y. Wang, and L.F. Cranor, *Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems.* User Modeling and User-Adapted Interaction, 2012. **22**(1-2): p. 203-220.

158. Toorani, M. and A. Beheshti. *LPKI - A lightweight public key infrastructure for the mobile environments*. in *11th IEEE International Conference onCommunication Systems (ICCS 2008)*. 2008. Singapore

159. Tosh, D. and B. Werdmuller. *ePortfolios and weblogs: One vision for ePortfolio development*. 2004; Available from: http://64.233.179.104/scholar?num=100&hl=en&lr=&q=cache:tnNxIF3piUYJ:eduspaces.net/dtosh/files/7371/16864/ePortfolio_Weblog.pdf+e-portfolio+security.

160. Trček, D., *Managing information systems security and privacy*. 2006: Birkhauser. 69.

161. Tsahuridu, E. (2012) *Document ownership: The rules of a broken engagement*. Manage your clients' SMSFs from one place, [06 March 2010]; Available from: http://www.itbdigital.com/tools-of-the-trade/2012/09/24/document-ownership-the-rules-of-a-broken-engagement/.

162. UK Parliament, *Data Protection Act*. 1998.

163. United Nations, *Universal declaration of human rights*. 1948.

164. Vacca, J.R., *Public key infrastructure: building trusted applications and web services*. 2004: CRC Press. 8.

165. VeriSign. *Introduction to digital certificates*. 2008 12/11/2008]; Available from: http://www.verisign.com.au/repository/tutorial/digital/intro1.shtml.

166. Chandra, P., M. Messier, and J. Viega, *Network security with OpenSSL*. 2002: O'Reilly Media. 61-62. Available from: http://www.weibnc.com/wp-content/uploads/brkpdfs/Network-Security-with-OpenSSL-by-Pravir-Chandra-Happy-With-My-Purchase.pdf

167. W3C recommendation (2002) *XML signature syntax and processing*.

168. Warren, S.D. and L.D. Brandeis, *The right to privacy*. Harvard Law Review, 1890. **4**(5): p. 193-220.

169. Webb, J.M. *Trade Secret Law Reporter: A practitioner's guide to confidentiality agreement*. 1985 08 April 2013; Available from: http://uk.search.yahoo.com/r/_ylt=A7x9QbwshadR3DIA7AVLBQx.;_ylu=X3oDMTE1NnJjbjg0BHNlYwNzcgRwb3MDMQRjb2xvA2lyZAR2dGlkA01TWVVLMDRfNzc-/SIG=12g0othhh/EXP=1369961900/**http%3a//www.stoel.com/files/ConfidentialityAgreementGuide.pdf.

170. Wesinger Jr, R.E. and C.D. Coley, *Firewall providing enhanced network security and user transparency*, 1999, Washington, DC: U.S. Patent and Trademark Office, 5,898,830, issued April 27, 1999.

171. Westin, A.F., *Privacy and freedom.* Washington and Lee Law Review, 1968. **25**(1): p. 166.

172. Westlund, H.B., *NIST reports measurable success of Advanced Encryption Standard.* Journal of Research of the National Institute of Standards and Technology, 2002(May 2002).

173. Wills, G., 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),* . 2007. Loughborough University, UK

174. Wills, G., D. Millard, S. Chennupati, E.R. Jam, I. Tulloch, L. Gilbert, and Y. Howard *FREMA: e-learning framework reference model for assessment*. FREMA Project Journal 2006; Available from: http://www.frema.ecs.soton.ac.uk/projectJournal/.

175. Yancey, K.B., *General patterns and the future*, in *Electronic portfolios: Emerging practices in student, faculty, and institutional learning*, Cambridge, B.L., S. Kahn, D.P. Tompkins & K.B. Yancey, Editors. 2001, American Association for Higher Education: Washington. p. 83-87.

176. Yeun, C.Y. and T. Farnham. *Secure m-commerce with wpki*. in *1st International Workshop for Asian PKI*. 2001. Korea: Citeseer

177. Yoder, J. and J. Barcalow, *Architectural patterns for enabling application security*. Urbana, 1998. **51**: p. 61801.

178. Zenise, M., A. Vitaletti, and D. Argles. *A user-centric approach to eCertificate for electronic identities (eIDs) management in mobile environment*. in *IEEE World Congress on Internet Security (WorldCIS)*. 2011. London, UK

179. Zenise, M., A. Vitaletti, L. Chen-Wilson, L. Gilbert, and D. Argles, *eIDeCert: A user-centric solution for mobile identification.* International Journal for Infonomics, 2011. **4**(3/4): p. 527-536.

180. Zimmermann, P.R., *The official PGP user's guide*. 1995: MIT Press.

Appendix A: Supporting Documents

The supporting documents for this research are about the experiments (the eCert project and its sub-projects), which can be found on the eCert project website. These include:

eCert Project documents

- Project Plan: http://ecert.ecs.soton.ac.uk/publications/eCertProjectPlan.pdf
- Final Report: http://ecert.ecs.soton.ac.uk/publications/eCertProjectFinalReport.pdf
- First Workshop Report: http://ecert.ecs.soton.ac.uk/publications/eCert-1stWorkshop.pdf
- Second Workshop Report: http://ecert.ecs.soton.ac.uk/publications/eCert-2ndWorkshop.pdf

eCert Code library

- Source code: http://ecert.ecs.soton.ac.uk/development/source/eCert.zip
- JavaDoc: http://ecert.ecs.soton.ac.uk/development/ecertdoc/

eCert Demonstrator

- Source code: http://ecert.ecs.soton.ac.uk/development/source/eCert.war
- Online demo system: http://152.78.189.130:8080/eCert/
- Video: http://www.youtube.com/watch?v=LlrETHZeHeA
- Documentation: http://ecert.ecs.soton.ac.uk/development/document/eCert.pdf

eCert in ePortfolio

- Source code: http://ecert.ecs.soton.ac.uk/development/source/eport.zip
- Video: http://www.youtube.com/watch?v=c9lc9vS3Eyg
- Report: http://ecert.ecs.soton.ac.uk/development/document/eport.pdf

eCert for Mobile eID

- Source code: http://ecert.ecs.soton.ac.uk/development/source/eID.zip
- Video: http://www.youtube.com/watch?v=yYn7c6uVFl8

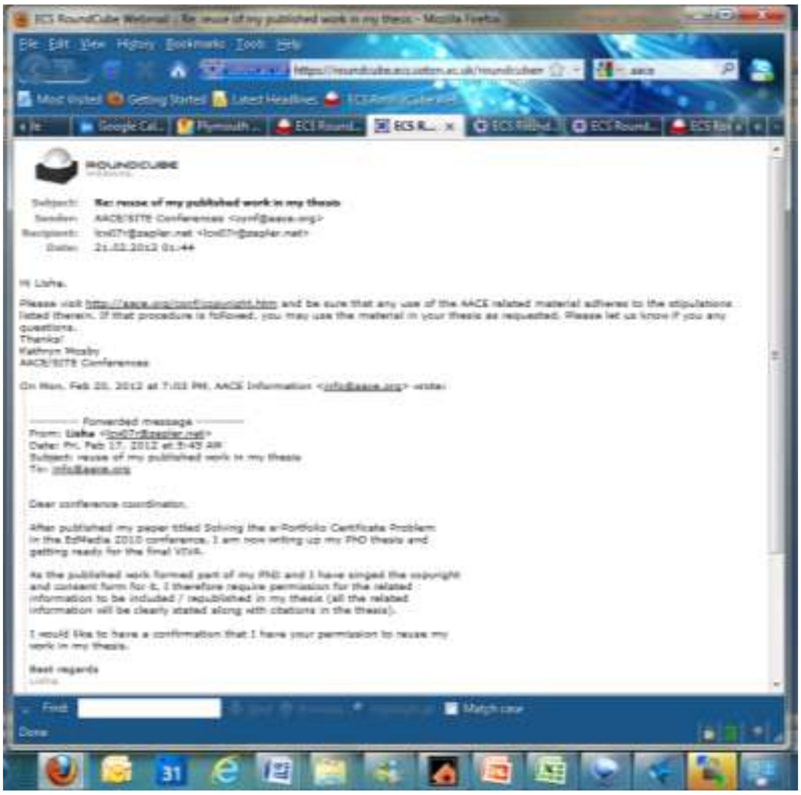
Appendix B: Copyright

Part of the work summarized in this thesis has been published and the copyright has been transferred to the publishers. The items involved are:

- Reference paper NO 11, Copyright by AACE, copyright policy can be accessed from http://www.aace.org/conf/copyright.htm
- Reference papers No 32 and 36, Copyright by IEEE, copyright policy can be accessed from http://www.ieee.org/documents/ieeecopyrightform.doc
- Reference papers No 168 and 31, Copyright by Infonomics Society, copyright policy can be accessed from http://www.infonomics-society.org/IJI/IJI%20Copyright%20Form.pdf and http://www.infonomics-society.org/IJISR/IJISR%20Copyright%20Form.pdf

Part of the work was carried out during the JISC-funded project eCert, and has been published on the eCert project website.

In order to address these, permissions for re-using the published materials have been obtained, and copyright procedures have been followed according to the individual publisher's requirements, such as the provided citations, notice of copyright, and acknowledgement of publishers. Below are the permission examples: Figure B-1 shows the permission from AACE; and Figure B-2 shows the permission from Chris Brown, the JISC program manager.



Subject: Re: reuse of my published work in my thesis
Sender: AACE/SITE Conferences <conf@aace.org>
Recipient: lcw07r@zepler.net <lcw07r@zepler.net>
Date: 21.02.2012 01:44

Hi Lisha,

Please visit http://aace.org/conf/copyright.htm and be sure that any use of the AACE related material adheres to the stipulations listed therein. If that procedure is followed, you may use the material in your thesis as requested. Please let us know if you any questions.
Thanks!
Kathryn Mosby
AACE/SITE Conferences

On Mon, Feb 20, 2012 at 7:03 PM, AACE Information <info@aace.org> wrote:

---------- Forwarded message ----------
From: Lisha <lcw07r@zepler.net>
Date: Fri, Feb 17, 2012 at 5:45 AM
Subject: reuse of my published work in my thesis
To: info@aace.org

Dear conference coordinator,

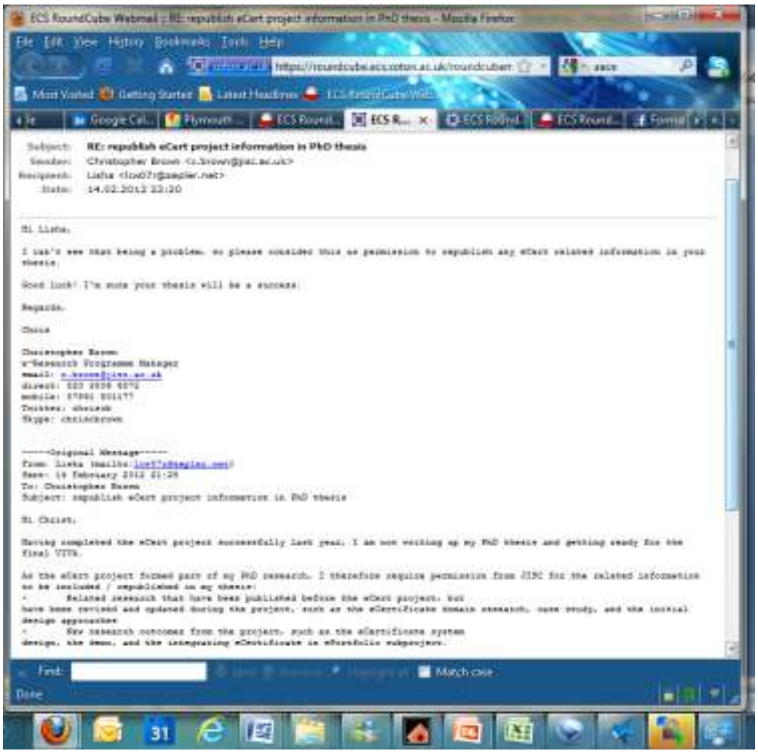
After published my paper titled Solving the e-Portfolio Certificate Problem in the EdMedia 2010 conference, I am now writing up my PhD thesis and getting ready for the final VIVA.

As the published work formed part of my PhD and I have singed the copyright and consent form for it, I therefore require permission for the related information to be included / republished in my thesis (all the related information will be clearly stated along with citations in the thesis).

I would like to have a confirmation that I have your permission to reuse my work in my thesis.

Best regards
Lisha

Figure B-0-1 Permission from AACE



Subject: RE: republish eCert project information in PhD thesis
Sender: Christopher Brown <c.brown@jisc.ac.uk>
Recipient: Lisha <lcw07r@zepler.net>
Date: 14.02.2012 22:20

Hi Lisha,

I can't see that being a problem, so please consider this as permission to republish any eCert related information in your thesis.

Good luck! I'm sure your thesis will be a success.

Regards,

Chris

Christopher Brown
e-Research Programme Manager
email: c.brown@jisc.ac.uk
direct: [illegible]
mobile: [illegible]
Twitter: chrisbrown
Skype: chrisdcbrown

-----Original Message-----
From: Lisha [mailto:lcw07r@zepler.net]
Sent: 14 February 2012 21:28
To: Christopher Brown
Subject: republish eCert project information in PhD thesis

Hi Chris,

Having completed the eCert project successfully last year, I am now writing up my PhD thesis and getting ready for the final VIVA.

As the eCert project formed part of my PhD research, I therefore require permission from JISC for the related information to be included / republished in my thesis:
- Related research that have been published before the eCert project, but have been revised and updated during the project, such as the eCertificate domain research, case study, and the initial design approaches
- New research outcomes from the project, such as the eCertificate system design, the demo, and the integrating eCertificate in ePortfolio subproject.

Figure B-0-2 Permission from JISC

Appendix C: System Development with SORM Methodology

The process of eCertificate system development with the SORM methodology is summarized in Table C-1 below.

- First, system requirements (SR) were raised from Domain definition and Common usage patterns
- Second, technical requirements (TR) were raised from Use cases and Gap analysis
- Third, design approaches (DA) were raised from Service profiles
- Finally, system implementation (SI) was raised from Reference implementation

Table C-0-1 eCertificate system development process IDs

System requirement ID	Technical requirement ID	Design approach ID	System implementation ID
SR-01	TR-01	DA-01	SI-01
SR-02	TR-02	DA-02	SI-02
	TR-03	DA-03	SI-03
			SI-04
	TR-04	DA-04	SI-05
			SI-06
SR-03	TR-05	DA-05	SI-07
	TR-06	DA-06	SI-08
	TR-07	DA-07	SI-09
	TR-08	DA-08	SI-10
		DA-09	SI-11
		DA-10	SI-12
SR-04	TR-09	DA-11	SI-13
		DA-12	SI-14
SR-05	TR-10	DA-13	SI-15
			SI-16
		DA-14	SI-17
	TR-11	DA-15	SI-18
	TR-12	DA-16	SI-19
	TR-13	DA-17	SI-20
	TR-14	DA-18	SI-21

System requirements (SR)

SR-01 can be used stand alone or served within an ePortfolio

SR-02 security control throughout the whole eCertificate lifecycle: from generation, issue, distribution, to verification; involves hardware, software, database, information, and human control

SR-03 can be verified in a legal context, support withdrawal of eCertificate and the content status validation as well as the signing key status validation

SR-04 ensure that the owner can have control over the usage of their eCertificates

SR-05 effective usage: easy to use, support lifetime validation, and can be widely verified and recognized throughout the UK

Technical requirements (TR)

TR-01 system adaptability and compatibility so that the system can be embedded as a plug-in within other systems, e.g. eFolio

TR-02 Security control: includes hardware, database, and network

TR-03 system access control for students, reviewers, and any third parties

TR-04 eCertificate access control for students, reviewers, and any third parties

TR-05 support content modification validation

TR-06 support withdrawal of an eCertificate

TR-07 support revocation of signing key

TR-08 can be verified and proof of issuer

TR-09 the student owner of the eCertificate can have control over who can see it and for how long, without the need for re-signing by the issuer

TR-10 stimulate large-scale uptake, enable eCertificate to be widely verified and recognized throughout the UK

TR-11 support lifetime validation, can be independent from the issuing body

TR-12 easy to use, suit low IT skill users, both students and reviewers

TR-13 minimize system storage

TR-14 establish stakeholder trust between all involved parties

Design approaches (DA)

DA-01 Use XML to enable easy transaction between systems with different platforms

DA-02 for the eCertificate generation and issuing process, the hardware, database, and network security, and human control for both staff and students, will be guarded by the issuing body

DA-03 adapt Federated Identity system technique; access control to eCertificate system will be based on system roles

DA-04 access control to eCertificate will be restricted to authorized users only

DA-05 employ digital signing technique to support the content modification validation

DA-06 design a new function for eCertificate content status validation, address the unique eCertificate squared problem, support withdrawal of an eCertificate

DA-07 design a new function to support the auto verification of signing key CRL

DA-08 design a new structure for eCertificate so that it can contain the various information files which can be legally accepted and verified

DA-09 adapt the XML signature technique to support the verification of the various information types involved in an eCertificate

DA-10 employ timestamp technique to enhance the signature integrity

DA-11 employ XML metadata for eCertificate access control values

DA-12 design a new signing method that allows the modification of eCertificate metadata while maintaining the integrity of the digital signature, so that the owner can set access controls on an eCertificate without the need for re-signing by the issuer

DA-13 adapt SOA to provide an architecture for participation which will enable large-scale uptake

DA-14 adapt a national unique number system to enable the eCertificate system to be rolled out throughout the UK

DA-15 an independent system to provide the required services

DA-16 provide functions with user friendly interface to deal with complicated technical requirements, such as key management

DA-17 avoid storing sensitive data, minimize system storage to reduce the attraction of database attacks

DA-18 employ PKI, establish stakeholder trust between all involved parties

System implementation (SI)

SI-01 The system was developed using XML to enable easy transaction between systems with different platforms

SI-02 The security control of hardware, database, and network for the eCertificate generation and issuing processes is handled by the issuing institution

SI-03 As explained in the Federation Management vs. eCert System Management section, a locally built access control system was implemented instead of a federated identity system.

SI-04 Based on their system role, only authorized staff can access the issuing system and only authorized students can access the management system, but everyone can access the verification system.

SI-05 Students can only set controls on their own eCertificates through the management system.SI-06 Only reviewers with correct access key can access the corresponding eCertificate

SI-07 Traditional digital signing technique is used as the foundation of the signing process to support the content modification validation

SI-08 Took the signing key CRL as an example, a new qualification CRL was created and its validation process was added to the traditional digital signing process to solve the eCertificate squared problem

SI-09 A function was added to call for the verification of the signing key and display the result every time an eCertificate is accessed,

SI-10 A new file structure for eCertificate was defined, which contains all elements that a paper-based certificate has, as well as the new elements that meet the eCertificate and ePortfolio requirements, such as the evidence file.

SI-11 The XML signature was adopted with a new wrapping method for the various file types structured in the eCertificate to increase the signature security in the verification process

SI-12 A timestamp has been added to the signature so that an eCertificate will be digitally signed, certified signature time, and therefore, tamper evident and non-repudiation

SI-13 Owner controlled access token, access section, and access time limit values have been placed in metadata

SI-14 A new signing method, eCert signature, has been proposed and implemented, which allows eCertificate owners to modify the metadata of a signed eCertificate without invalidating the signature

SI-15 The system was implemented with SOA

SI-16 Standards and policies have been set up for all institutions who use the system

SI-17 As explained in the Unique Student ID and eCertificate ID section, a self maintained numbering system was implemented

SI-18 An online centralised system has been implemented to provide eCertificate management and verification services. As the newly designed file structure and signing method enable the modification of access control values without re-signing, the system can be used independent of the issuers (with the last updated CRLs).

SI-19 Implemented support functions to handle the complicated requirements from the back end, such as signing and key management; therefore, front end web user friendly interface development can be easily set up by calling the support functions

SI-20 The system only proves the service, no personal sensitive information is stored, and only stores the CRLs for the validation purpose

SI-21 As the implementation is based on traditional digital signature, the PKI is maintained to provide trust between the stakeholders

Appendix D: A Comparison between eCert and Digitary

System architecture

The main difference between Digitary and eCert is the system architecture. From the point of the system usage, Digitary provides a distributed solution because each institution accesses a separate system for document issuing and verification, while eCert is a centralized solution because it is supposed to be a national system that is responsible for document creation, distribution, and verification (since there is no stand-alone program for issuers to issue the e-certification). From the storage model of signed documents, Digitary is centralized because the signed documents are only kept in the institutions; eCert is distributed because the signed documents are distributed to their owners (students). The difference in system architecture decides the difference in system implementation, maintenance and update. Generally speaking, Digitary is more convenient for the e-certificate issuing process, but is a little "clumsy" for reviewers who need to verify e-certificates from a wide range of institutions. Also, Digitary needs the institutions to store all issued e-certificates, placing more burden on system maintenance.

Technical elements

Digital signatures: digital signature is the fundamental technology for the system implementation of the eCert and Digitary system. However, as implementation of the digital signature alone is insufficient to address the issue of long-lived graduation documents, additional elements must be incorporated. In Digitary, a facility for the creation of long-lived digitally signed and timestamped documents compliant with the

XAdES standard has been used. In the eCert approach, only a timestamp is added to the digital-signed documents at this moment. Since the eCert system is still in the development stage, it can be improved with a similar facility in the Digitary approach.

Services for distribution: there is no distribution service in Digitary because signed documents are kept in the location where they were signed. In the eCert approach, the signed documents will be sent to students by email.

System access control: In Digitary, three groups are defined: issuers, students, employers, for users signing into the system to access required functions. eCert provides a similar approach for user access control: three sub-systems with different URLs are built for issuers, students and reviewers respectively. Users can only log into the sub-system to which they are allowed.

E-document access control: In Digitary, random URIs, including the document information and its access control are transmitted to reviewers. The reviewers are able to access online documents through secure hyperlinks. In eCert, the access control information is added onto the signed e-certificates, and students are able to set up access control in the central system and send processed e-certificates to reviewers.

Verification of documents: In Digitary, reviewers are able to get the verification information through the URIs from students. In eCert, reviewers need to upload the files received onto the central verification system. The verification system will analyze the files, and display the verification results to the reviewers.

System maintenance

Key management: In Digitary, since the signed documents are not distributed to owners, only issuers' keys (not sure if it is a key pair or a symmetric key) are used. In eCert, the issuer private key is used to sign the digest of the document, and the student public key is used to signed the whole e-Certificate document (including original documents, access control information, digital signature, and timestamp).

Document backup: Digitary does not store any copies of all issued e-Certificates for all institutions. It is the responsibility of institutions to make issued e-Certificates secure. In eCert, as the issued e-Certificates are distributed to students, institutions do not need to back up issued e-Certificates. If students lose their e-Certificates accidently, institutions are able to re-issue them through the eCert system.

Appendix E: The eCert Approach for eWork Use Cases

The eCert system is designed with a user centric approach. An issued eCertificate is an independent, verifiable, and owner controllable application. It can be accessed through an organization, serviced within any ePortfolio, or used in standalone mode. Therefore, eCert enables one solution to be employed for all the eWork use cases.

1. RTOs issue eCertificates to the VET learners using the eCert system. Each of these eCertificates includes the award certificate, the skill assessment that the certification was based on, and the qualification transcript with course information.
2. The issued eCertificate will be either:
    a. issued to the learner through a secured mailing system; or
    b. stored by the RTO. The learner can download copies of the eCertificate through the RTO and store them in his/her preferred repository, e.g. a personal ePortfolio system or PC.
3. The learner can set new access control values for their eCertificate in the RTO or the preferred repository.
4. The learner can provide the eCertificate as the qualification information to the reviewer, by either:
    a. providing the relevant eCertificate (and access keys if set) along with the application form or ePortfolio to the reviewer; or

   b. giving permission to the RTO to provide the relevant eCertificate; and following the process as mentioned in the use case scenario (varying from use case to use case) to provide the access path for the reviewing party.

5. The reviewer can verify the eCertificate by either using the eCert central system or the downloaded eCert application, and progress forward once confirmation is received that the learner meet the requirements.

Appendix F: The Usage of a Standalone eCertificate

Figure F-1 shows the process of an eCertificate from issue, to set control, distribute, and verify, when used standalone.

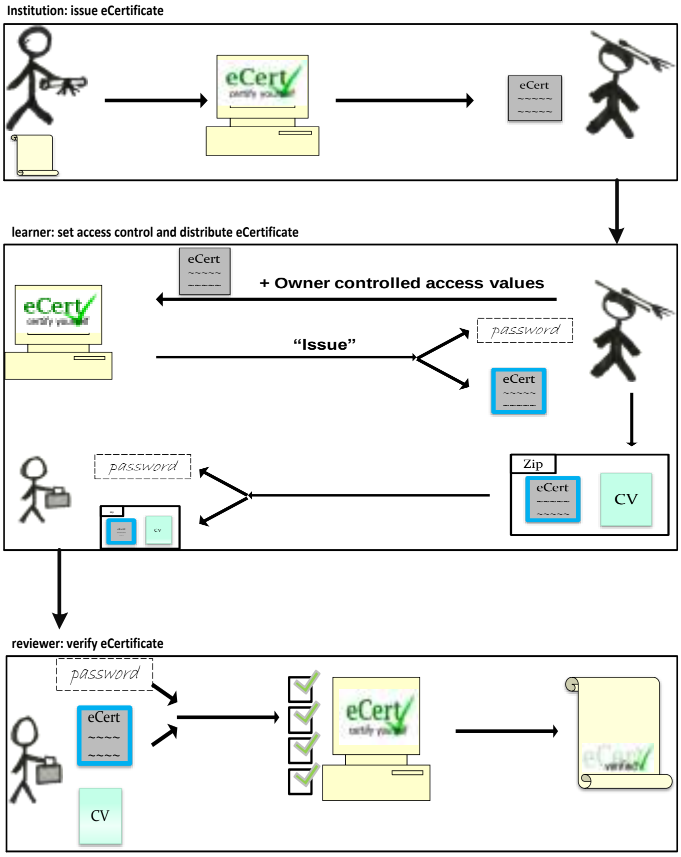
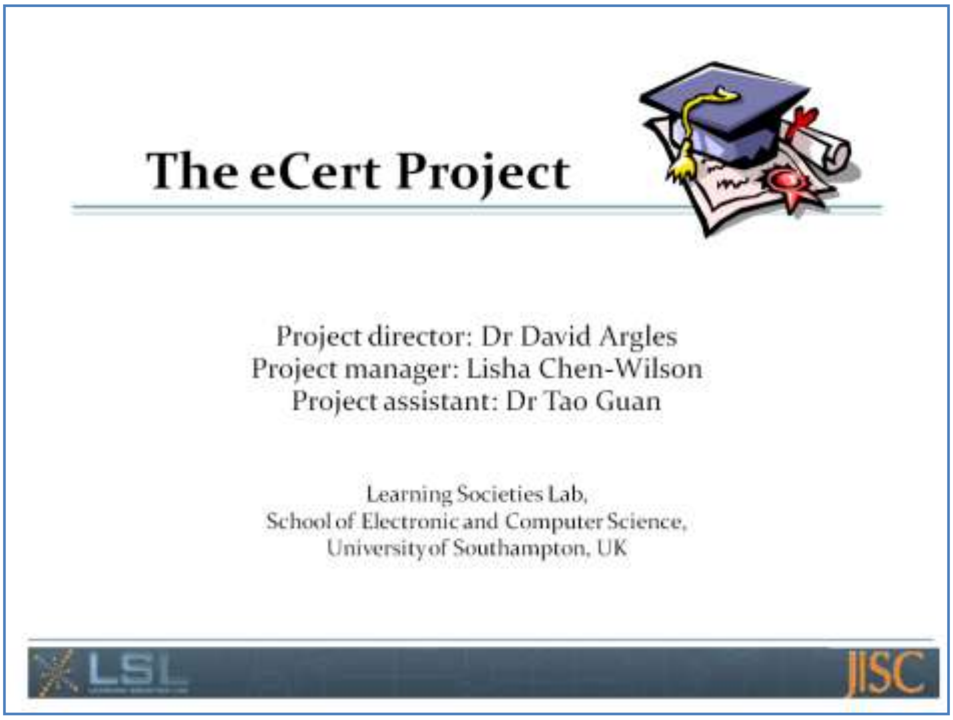

Institution: issue eCertificate
eCert
eCert
learner: set access control and distribute eCertificate
eCert
+ Owner controlled access values
eCert
"Issue"
password
eCert
password
Zip
eCert
CV
reviewer: verify eCertificate
password
eCert
CV
eCert
eCert

Figure F-0-1 An eCertificate used in standalone mode

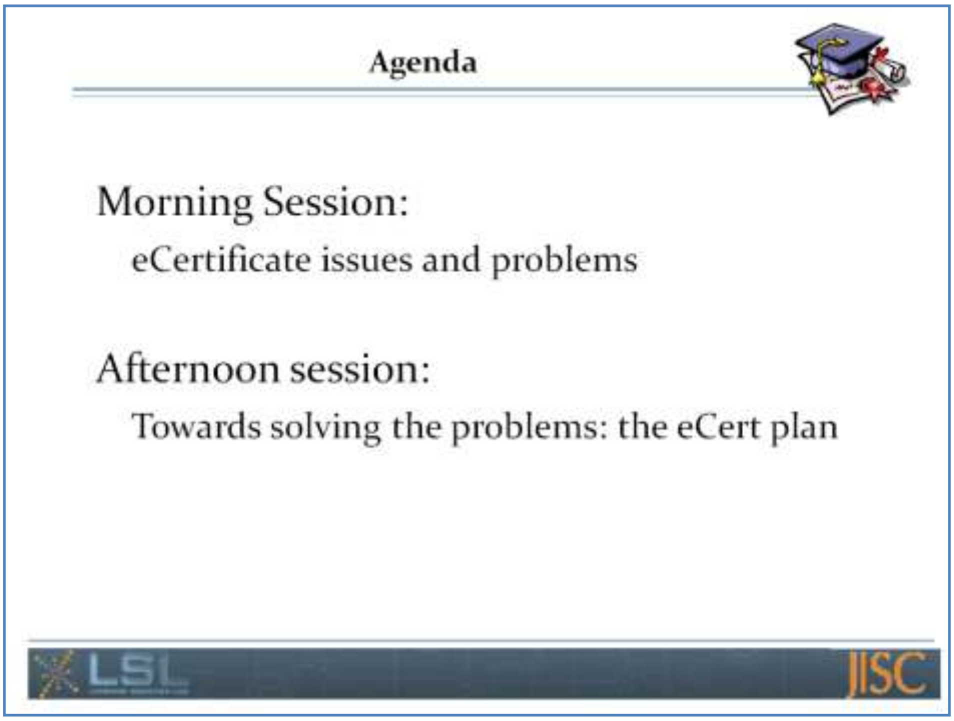
Appendix G: eCert First Workshop Presentation



The eCert Project

Project director: Dr David Argles
Project manager: Lisha Chen-Wilson
Project assistant: Dr Tao Guan

Learning Societies Lab,
School of Electronic and Computer Science,
University of Southampton, UK



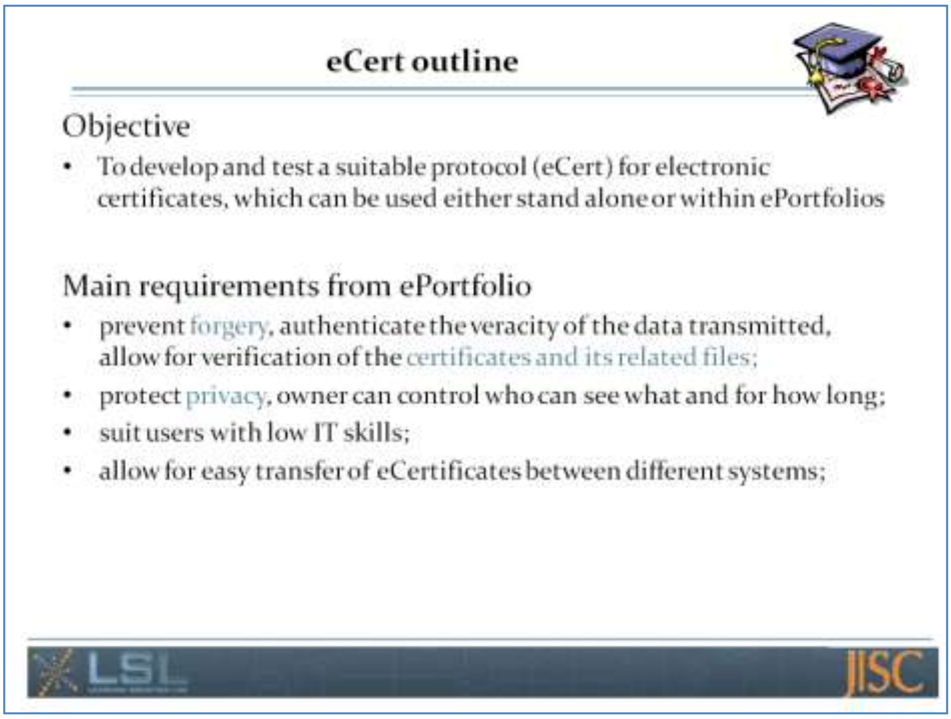
Agenda

Morning Session:

eCertificate issues and problems

Afternoon session:

Towards solving the problems: the eCert plan



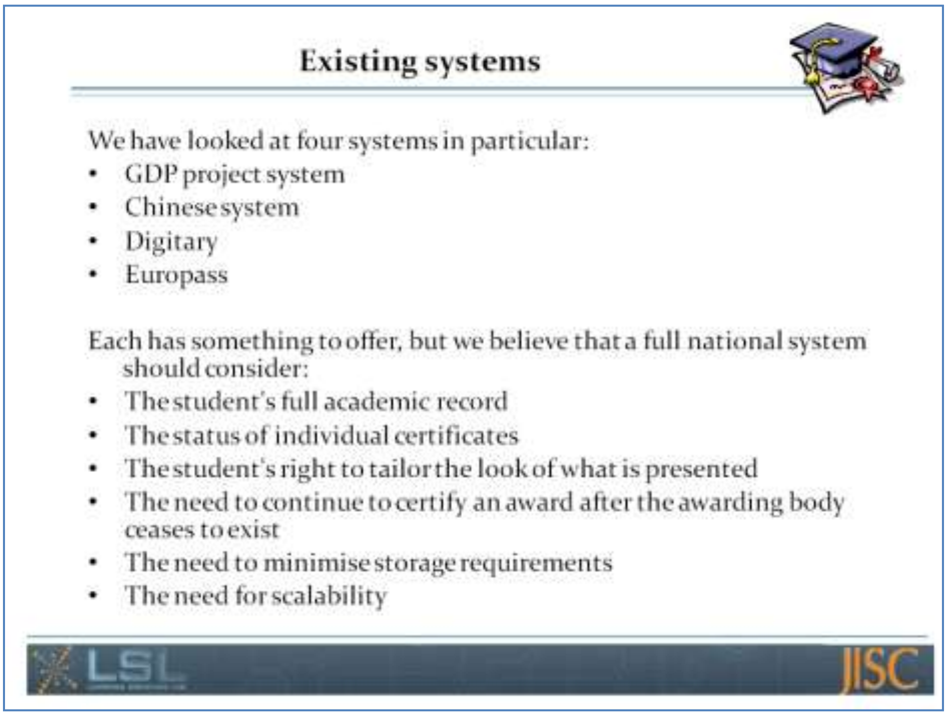
eCert outline

Objective

- To develop and test a suitable protocol (eCert) for electronic certificates, which can be used either stand alone or within ePortfolios

Main requirements from ePortfolio

- prevent forgery, authenticate the veracity of the data transmitted, allow for verification of the certificates and its related files;
- protect privacy, owner can control who can see what and for how long;
- suit users with low IT skills;
- allow for easy transfer of eCertificates between different systems;



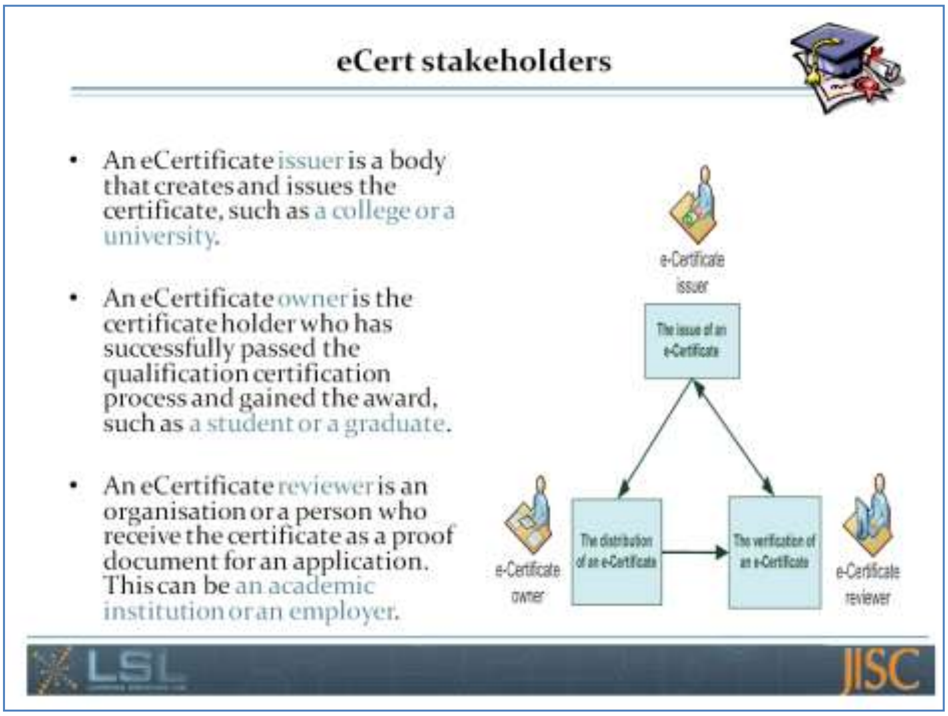
Existing systems

We have looked at four systems in particular:

- GDP project system
- Chinese system
- Digitary
- Europass

Each has something to offer, but we believe that a full national system should consider:

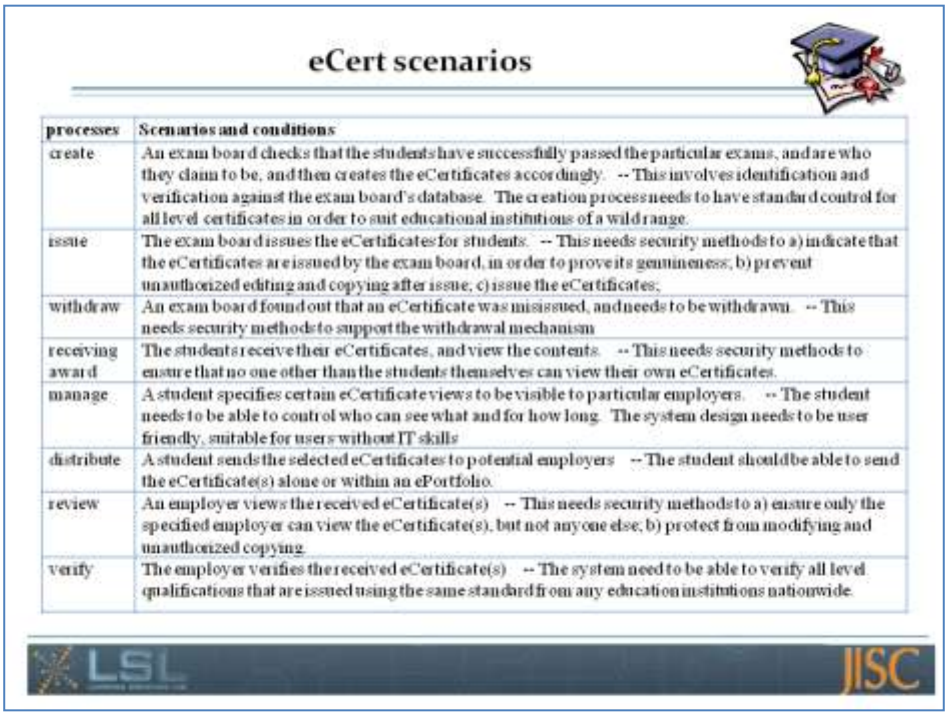
- The student's full academic record
- The status of individual certificates
- The student's right to tailor the look of what is presented
- The need to continue to certify an award after the awarding body ceases to exist
- The need to minimise storage requirements
- The need for scalability



eCert stakeholders

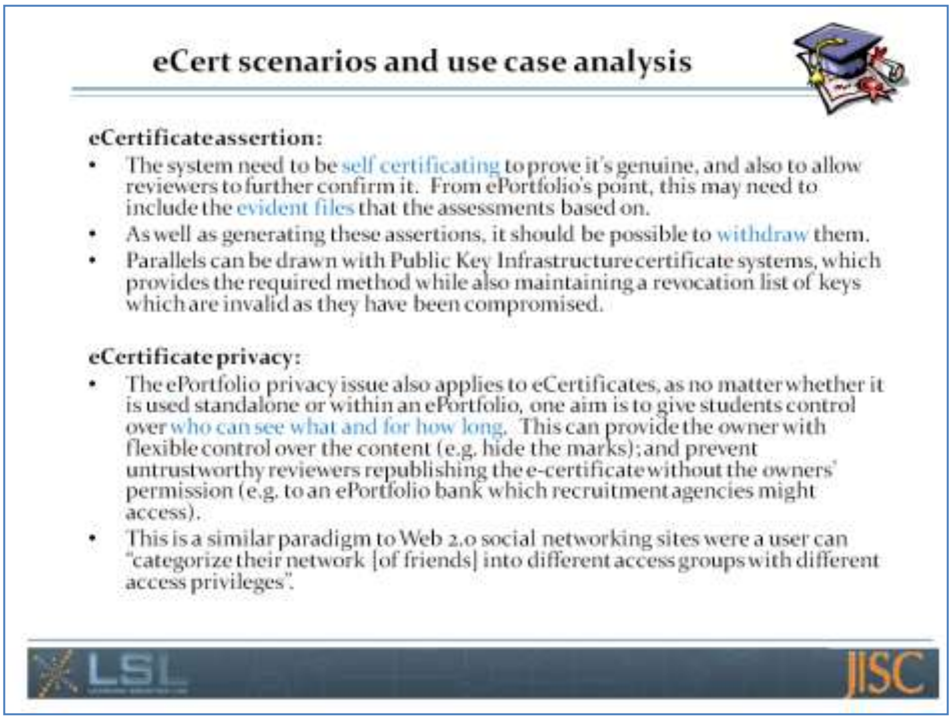
- An eCertificate issuer is a body that creates and issues the certificate, such as a college or a university.
- An eCertificate owner is the certificate holder who has successfully passed the qualification certification process and gained the award, such as a student or a graduate.
- An eCertificate reviewer is an organisation or a person who receive the certificate as a proof document for an application. This can be an academic institution or an employer.

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



eCert 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 eCertificates accordingly. -- This involves identification and verification against the exam board's database. The creation process needs to have standard control for all level certificates in order to suit educational institutions of a wild range.
issue	The exam board issues the eCertificates for students. -- This needs security methods to a) indicate that the eCertificates are issued by the exam board, in order to prove its genuineness; b) prevent unauthorized editing and copying after issue; c) issue the eCertificates;
withdraw	An exam board found out that an eCertificate was misissued, and needs to be withdrawn. -- This needs security methods to support the withdrawal mechanism
receiving award	The students receive their eCertificates, and view the contents. -- This needs security methods to ensure that no one other than the students themselves can view their own eCertificates.
manage	A student specifies certain eCertificate views to be visible to particular employers. -- The student needs to be able to control who can see what and for how long. The system design needs to be user friendly, suitable for users without IT skills
distribute	A student sends the selected eCertificates to potential employers -- The student should be able to send the eCertificate(s) alone or within an ePortfolio.
review	An employer views the received eCertificate(s) -- This needs security methods to a) ensure only the specified employer can view the eCertificate(s), but not anyone else; b) protect from modifying and unauthorized copying.
verify	The employer verifies the received eCertificate(s) -- The system need to be able to verify all level qualifications that are issued using the same standard from any education institutions nationwide.



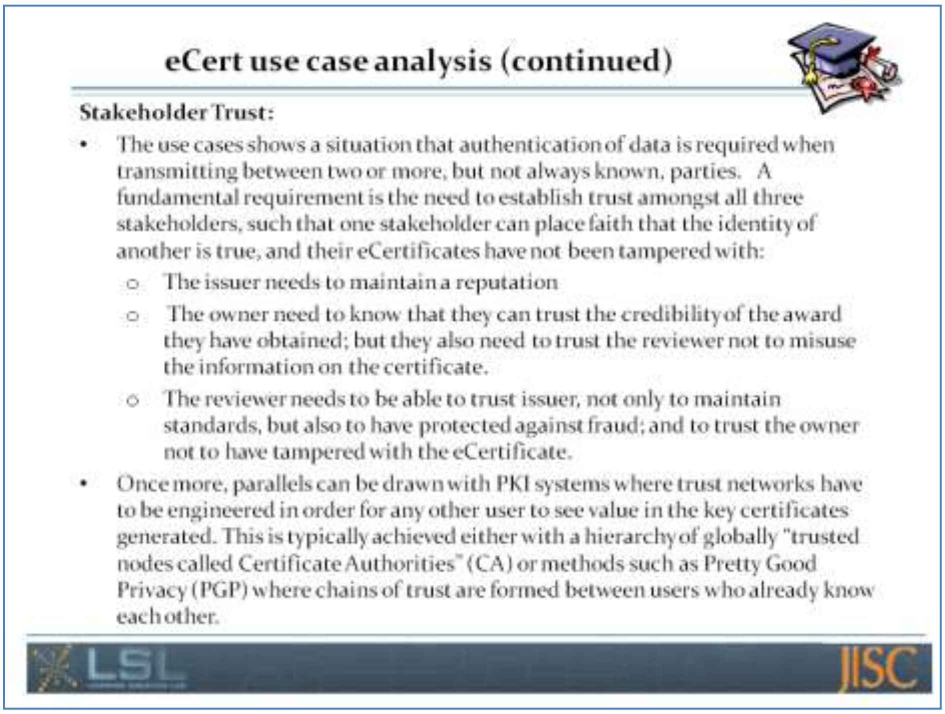
eCert scenarios and use case analysis

eCertificate assertion:

- The system need to be self certificating to prove it's genuine, and also to allow reviewers to further confirm it. From ePortfolio's point, this may need to include the evident files that the assessments based on.
- 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.

eCertificate privacy:

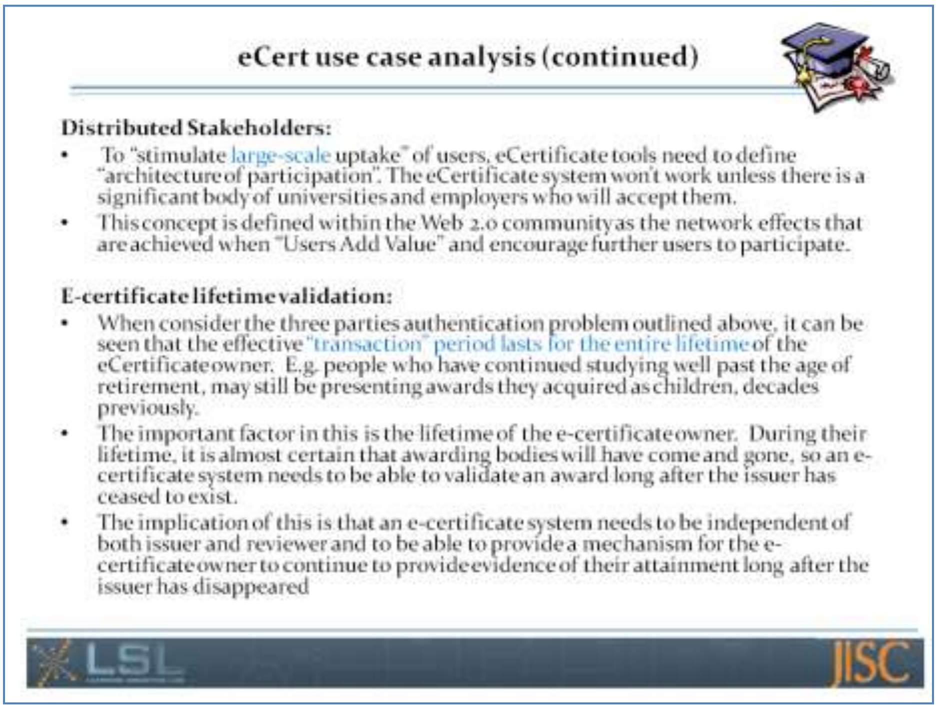
- The ePortfolio privacy issue also applies to eCertificates, as no matter whether it is used standalone or within an ePortfolio, one aim is to give students control over who can see what and for how long. This can provide the owner with flexible control over the content (e.g. hide the marks); and prevent untrustworthy reviewers republishing the e-certificate without the owners' permission (e.g. to an ePortfolio 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".



eCert use case analysis (continued)

Stakeholder Trust:

- The use cases shows a situation that authentication of data is required when transmitting between two or more, but not always known, parties. A fundamental requirement is the need to establish trust amongst all three stakeholders, such that one stakeholder can place faith that the identity of another is true, and their eCertificates have not been tampered with:
  - The issuer needs to maintain a reputation
  - The owner need to know that they can trust the credibility of the award they have obtained; but they also need to trust the reviewer not to misuse the information on the certificate.
  - The reviewer needs to be able to trust issuer, not only to maintain standards, but also to have protected against fraud; and to trust the owner not to have tampered with the eCertificate.
- 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 methods such as Pretty Good Privacy (PGP) where chains of trust are formed between users who already know each other.



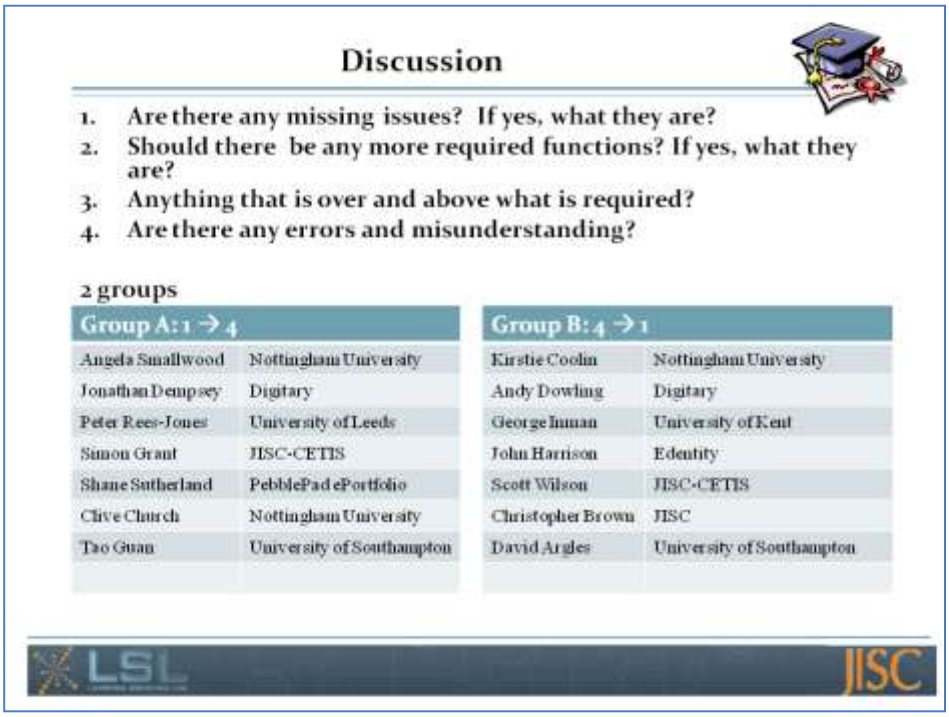
eCert use case analysis (continued)

Distributed Stakeholders:

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

E-certificate lifetime validation:

- When consider the three parties authentication problem outlined above, it can be seen that the effective "transaction" period lasts for the entire lifetime of the eCertificate owner. E.g. people who have continued studying well past the age of retirement, may still be presenting awards they acquired as children, decades previously.
- The important factor in this is the lifetime of the e-certificate owner. During their lifetime, it is almost certain that awarding bodies will have come and gone, so an e-certificate system needs to be able to validate an award long after the issuer has ceased to exist.
- The implication of this is that an e-certificate system needs to be independent of both issuer and reviewer and to be able to provide a mechanism for the e-certificate owner to continue to provide evidence of their attainment long after the issuer has disappeared



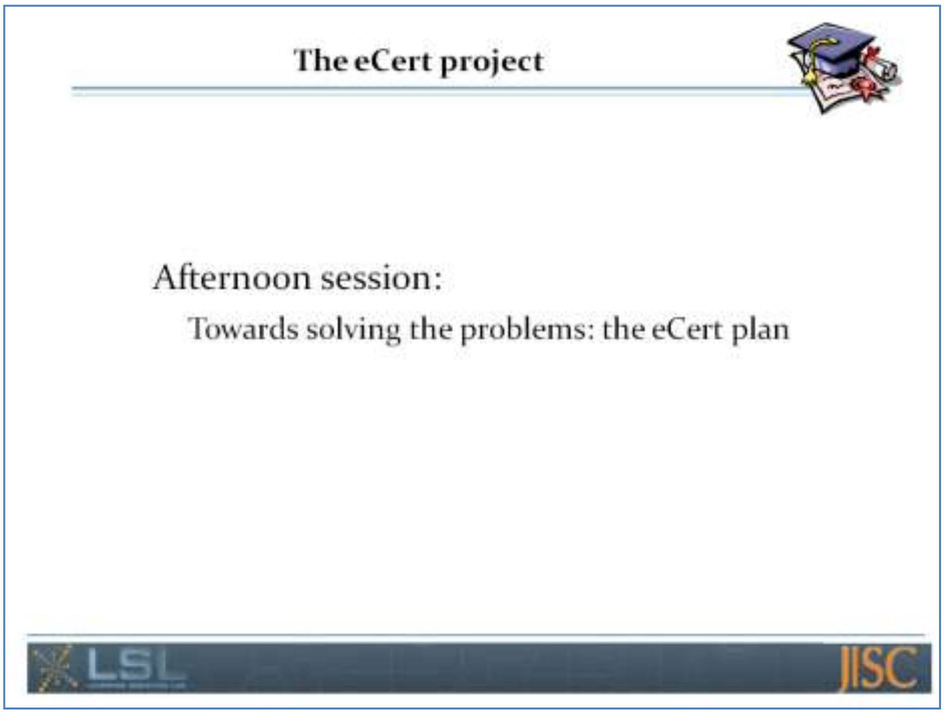
Discussion

1. Are there any missing issues? If yes, what they are?
2. Should there be any more required functions? If yes, what they are?
3. Anything that is over and above what is required?
4. Are there any errors and misunderstanding?

2 groups

Group A: 1 → 4	
Angela Smallwood	Nottingham University
Jonathan Dempsey	Digitary
Peter Rees-Jones	University of Leeds
Simon Grant	JISC-CETIS
Shane Sutherland	PebblePad ePortfolio
Clive Church	Nottingham University
Tao Guan	University of Southampton

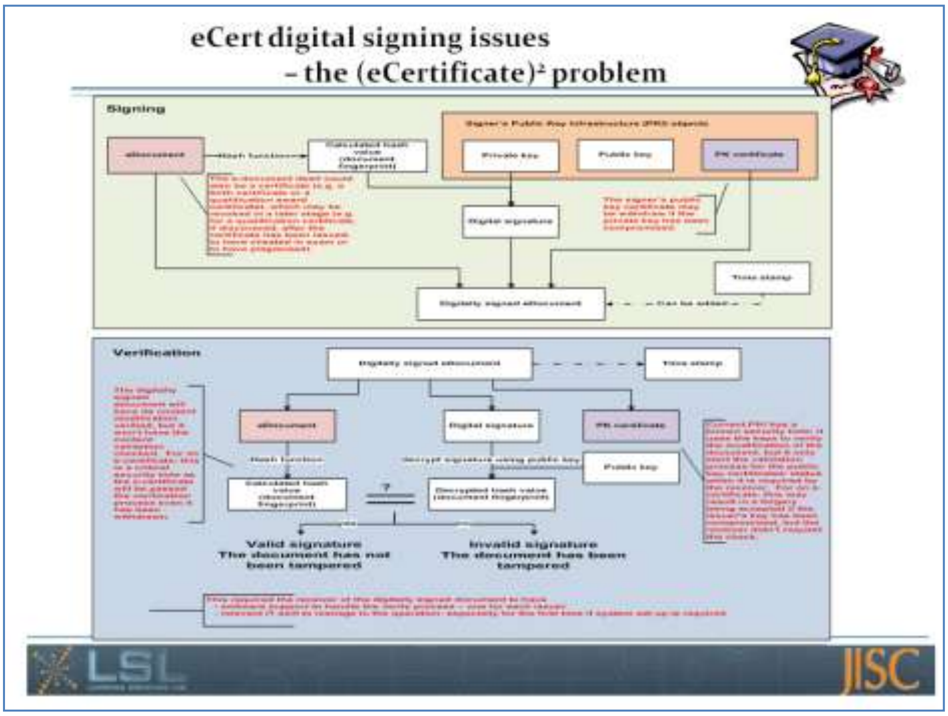
Group B: 4 → 1	
Kirstie Coolin	Nottingham University
Andy Dowling	Digitary
George Inman	University of Kent
John Harrison	Edentity
Scott Wilson	JISC-CETIS
Christopher Brown	JISC
David Argles	University of Southampton



The eCert project

Afternoon session:

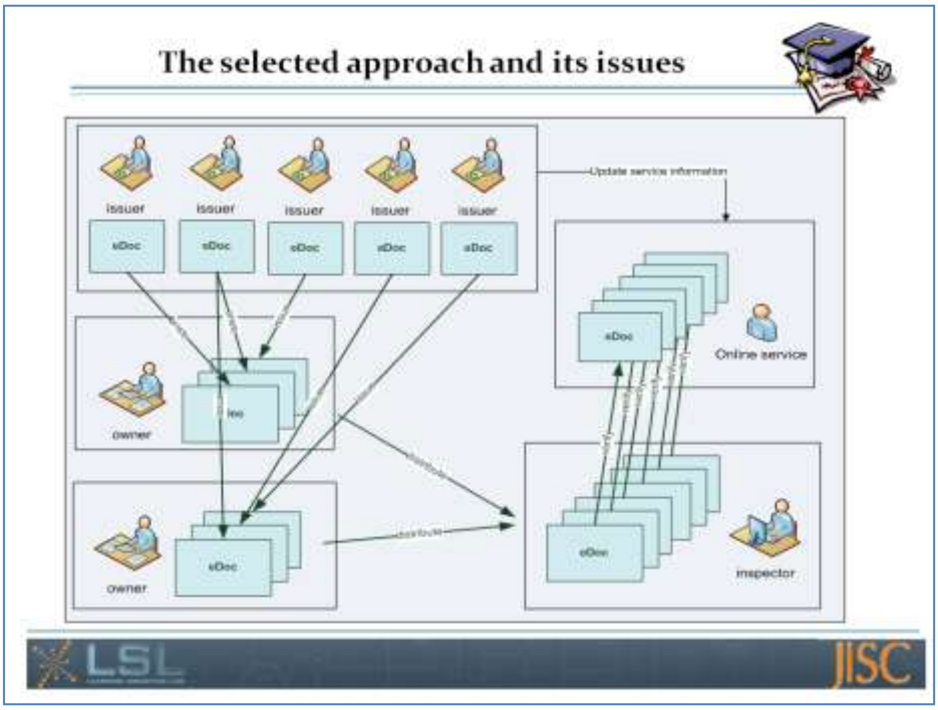
Towards solving the problems: the eCert plan



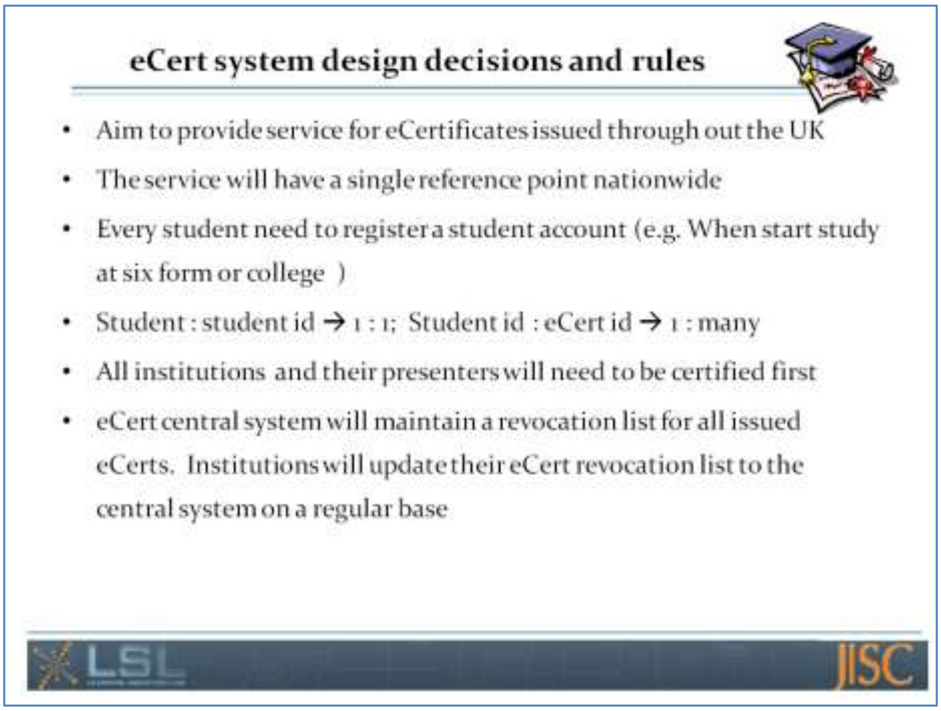
eCert digital signing issues – the (eCertificate)² problem

Signing
eDocument
Hash function
Calculated hash value (document fingerprint)
Signer's Public Key Infrastructure (PKI) objects
Private key
Public key
PK certificate
Digital signature
Time stamp
Digitally signed eDocument
Can be added
Verification
Digitally signed eDocument
Time stamp
eDocument
Digital signature
PK certificate
Hash function
Decrypt signature using public key
Public key
Calculated hash value (document fingerprint)
?
Decrypted hash value (document fingerprint)
Valid signature The document has not been tampered
Invalid signature The document has been tampered

[illegible]



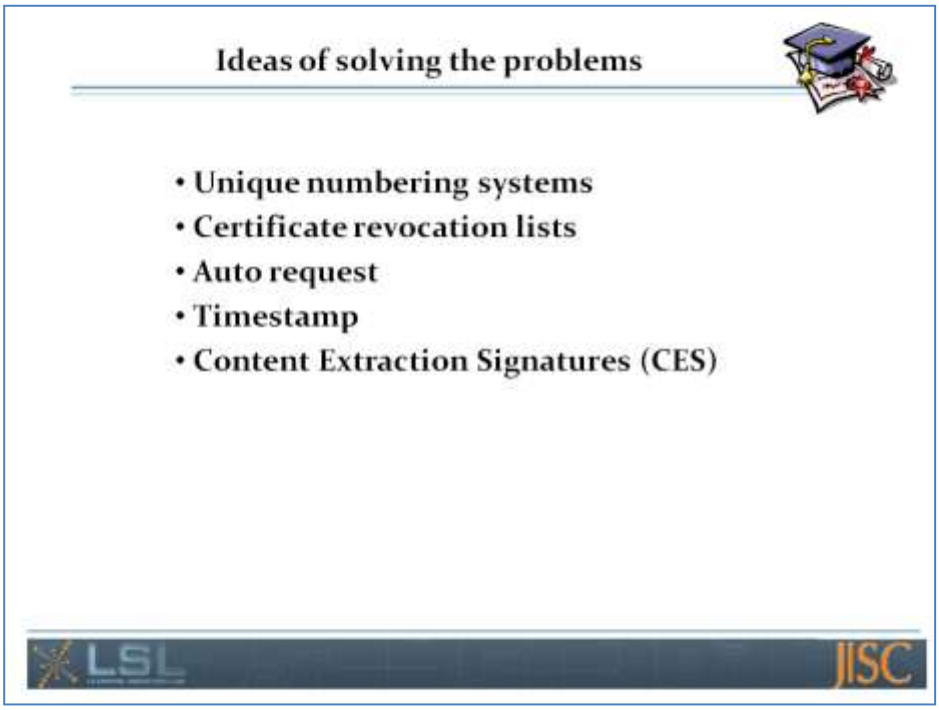
The selected approach and its issues



eCert system design decisions and rules

- Aim to provide service for eCertificates issued through out the UK
- The service will have a single reference point nationwide
- Every student need to register a student account (e.g. When start study at six form or college)
- Student : student id → 1 : 1; Student id : eCert id → 1 : many
- All institutions and their presenters will need to be certified first
- eCert central system will maintain a revocation list for all issued eCerts. Institutions will update their eCert revocation list to the central system on a regular base

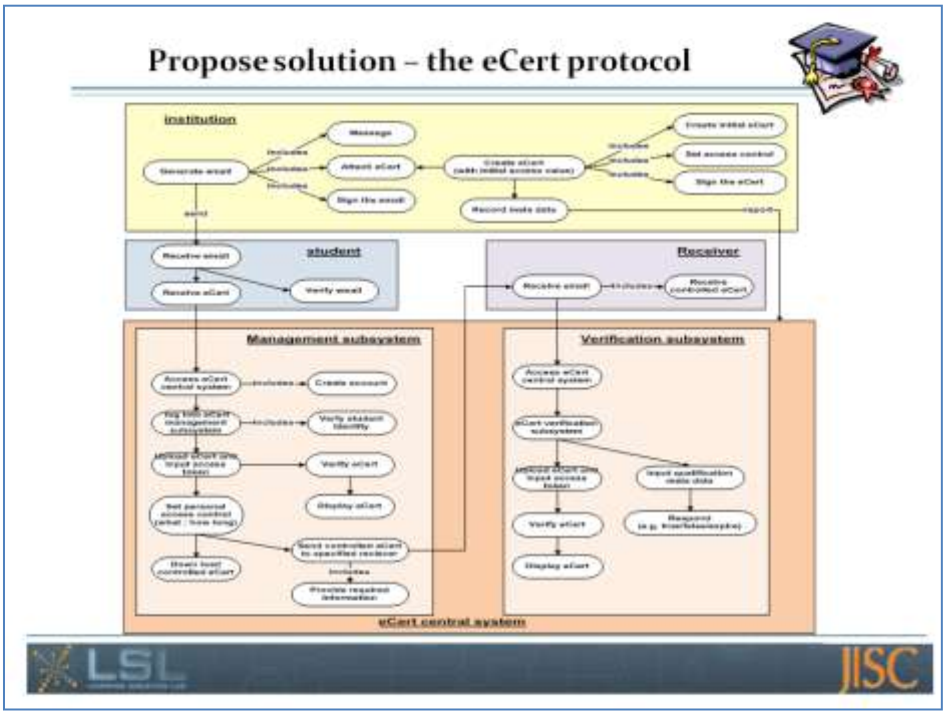
LSL
JISC



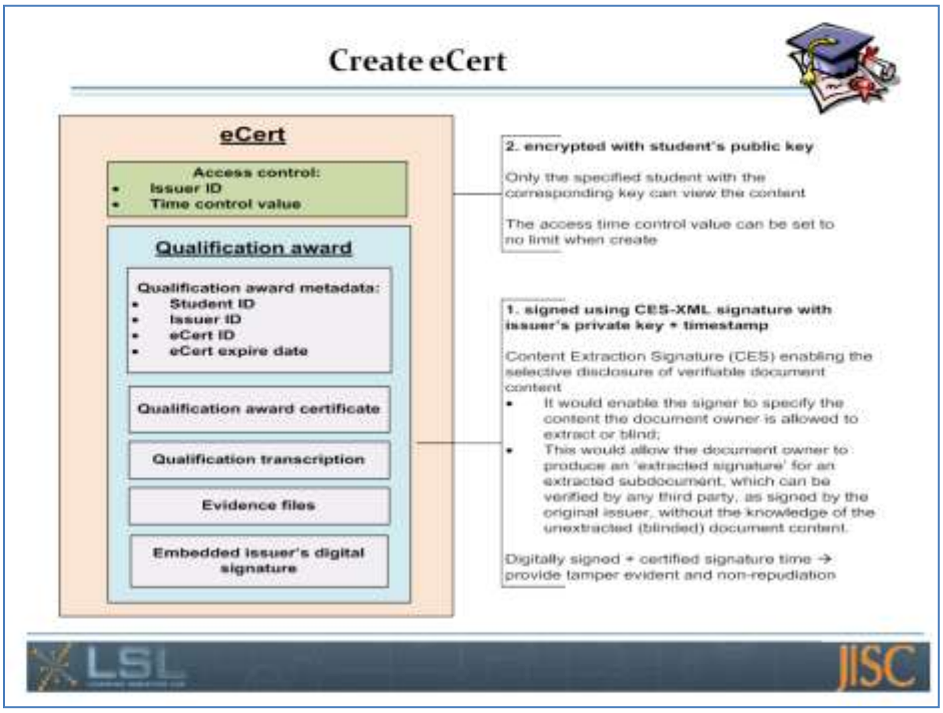
Ideas of solving the problems

- Unique numbering systems
- Certificate revocation lists
- Auto request
- Timestamp
- Content Extraction Signatures (CES)

LSL
JISC



Propose solution – the eCert protocol



Create eCert

2. encrypted with student's public key

Only the specified student with the corresponding key can view the content

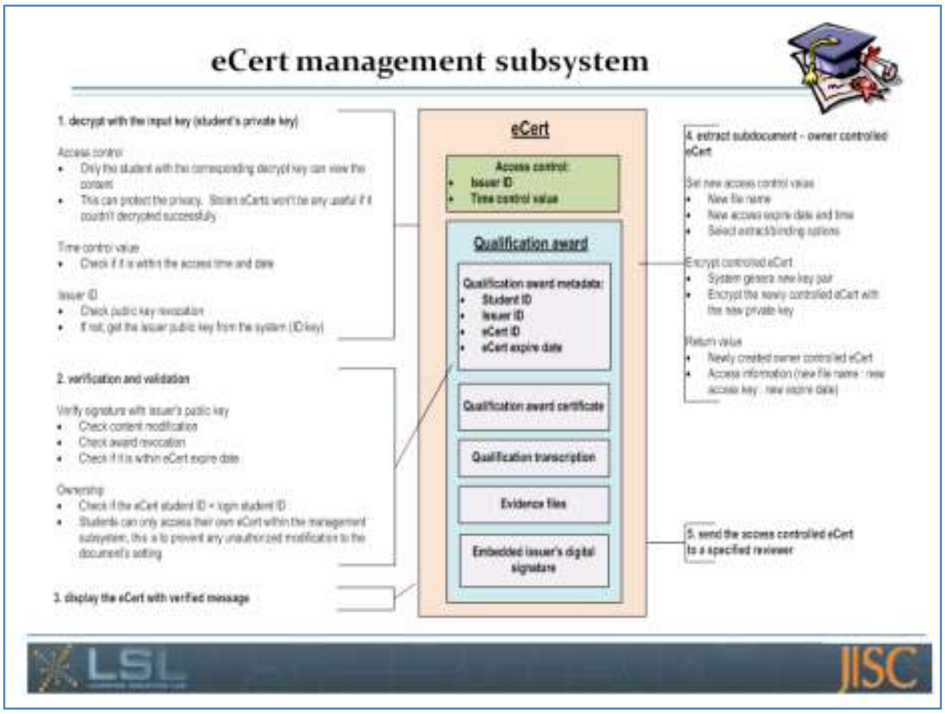
The access time control value can be set to no limit when create

1. signed using CES-XML signature with issuer's private key + timestamp

Content Extraction Signature (CES) enabling the selective disclosure of verifiable document content

- It would enable the signer to specify the content the document owner is allowed to extract or blind;
- This would allow the document owner to produce an 'extracted signature' for an extracted subdocument, which can be verified by any third party, as signed by the original issuer, without the knowledge of the unextracted (blinded) document content.

Digitally signed + certified signature time → provide tamper evident and non-repudiation



eCert management subsystem

1. decrypt with the input key (student's private key)

Access control
- Only the student with the corresponding decrypt key can view the content
- This can protect the privacy. Stolen eCerts won't be any useful if it couldn't decrypted successfully

Time control value
- Check if it is within the access time and date

Issuer ID
- Check public key revocation
- If not, get the issuer public key from the system (ID key)

2. verification and validation

Verify signature with issuer's public key
- Check content modification
- Check award revocation
- Check if it is within eCert expire date

Ownership
- Check if the eCert student ID = login student ID
- Students can only access their own eCert within the management subsystem; this is to prevent any unauthorized modification to the document's setting

3. display the eCert with verified message

eCert

Access control:
- Issuer ID
- Time control value

Qualification award

Qualification award metadata:
- Student ID
- Issuer ID
- eCert ID
- eCert expire date

Qualification award certificate

Qualification transcription

Evidence files

Embedded issuer's digital signature

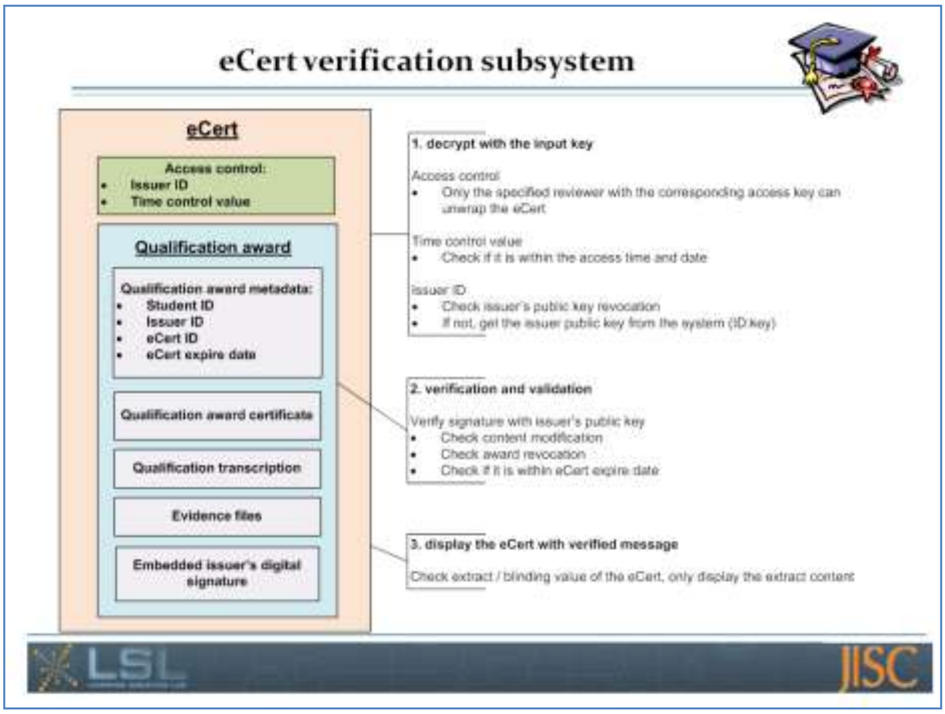
4. extract subdocument – owner controlled eCert

Set new access control value
- New file name
- New access expire date and time
- Select extract/binding options

Encrypt controlled eCert
- System genera new key pair
- Encrypt the newly controlled eCert with the new private key

Return value
- Newly created owner controlled eCert
- Access information (new file name : new access key : new expire date)

5. send the access controlled eCert to a specified reviewer



eCert verification subsystem

eCert

Access control:
- Issuer ID
- Time control value

Qualification award

Qualification award metadata:
- Student ID
- Issuer ID
- eCert ID
- eCert expire date

Qualification award certificate

Qualification transcription

Evidence files

Embedded issuer's digital signature

1. decrypt with the input key

Access control
- Only the specified reviewer with the corresponding access key can unwrap the eCert

Time control value
- Check if it is within the access time and date

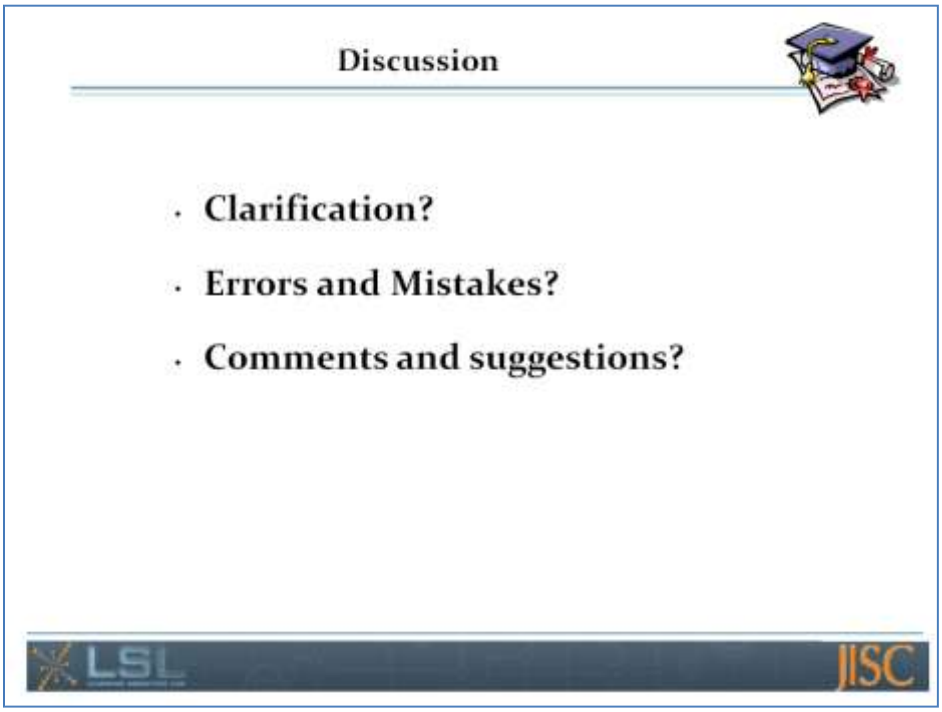
Issuer ID
- Check issuer's public key revocation
- If not, get the issuer public key from the system (ID key)

2. verification and validation

Verify signature with issuer's public key
- Check content modification
- Check award revocation
- Check if it is within eCert expire date

3. display the eCert with verified message

Check extract / blinding value of the eCert, only display the extract content



Discussion

- Clarification?
- Errors and Mistakes?
- Comments and suggestions?

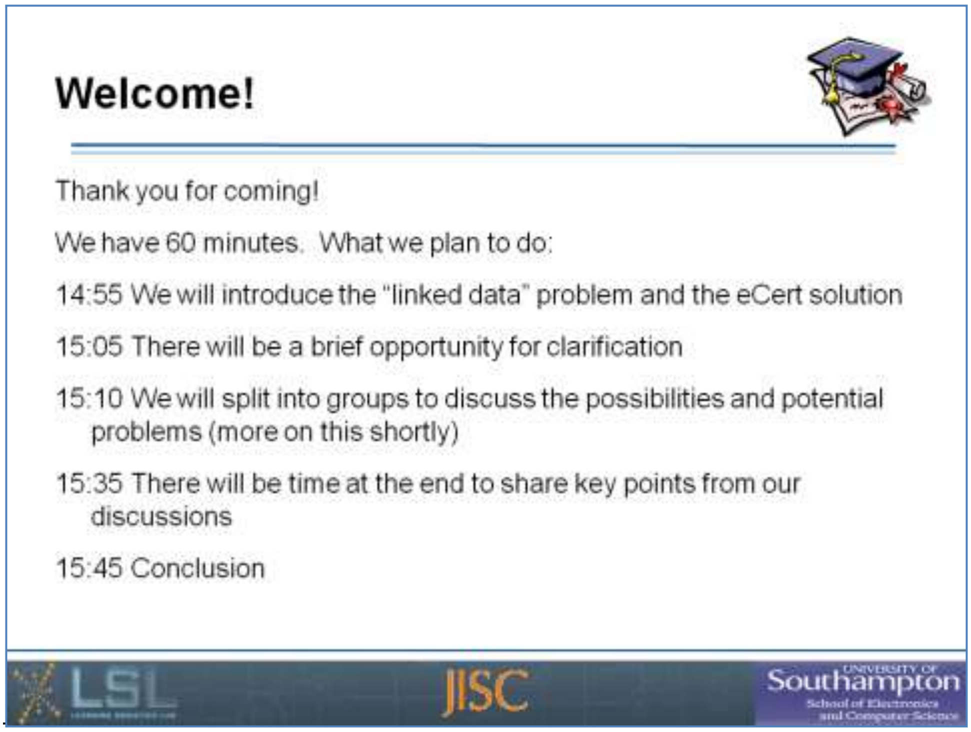
Appendix H: eCert Second Workshop Presentation

Giving you back control of your data:

E-qualification system for E-portfolios

Learning Societies Laboratory,
School of Electronic and Computer Science,
University of Southampton, UK

LSL
JISC
ALT-C 2010 7/09/2010 14:38
UNIVERSITY OF Southampton
School of Electronics and Computer Science



Welcome!

Thank you for coming!

We have 60 minutes. What we plan to do:

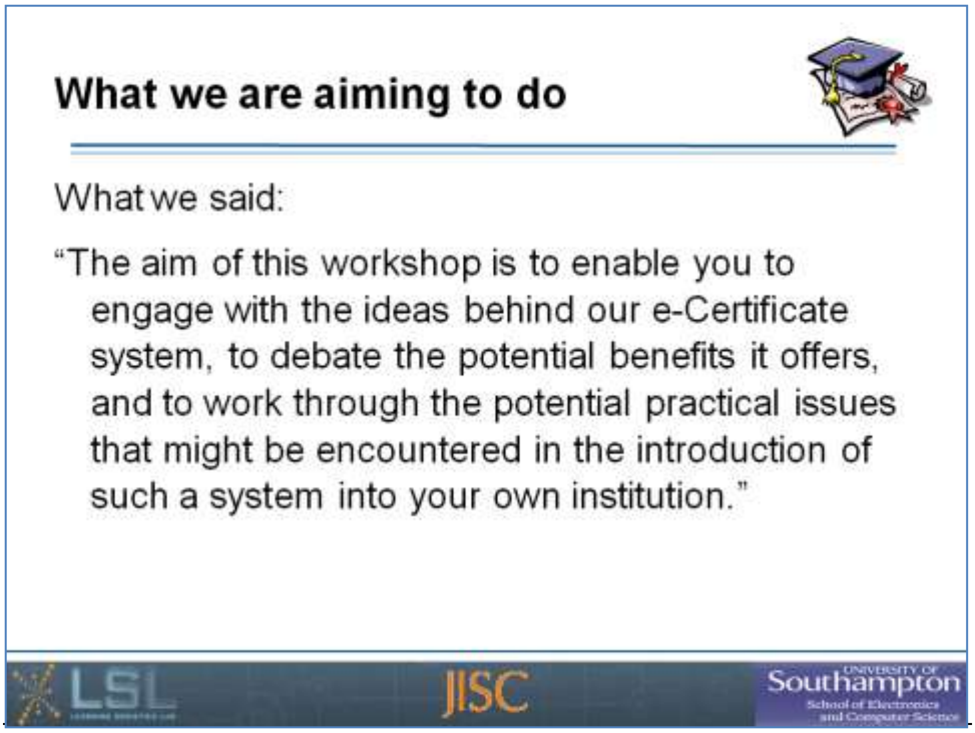
14:55 We will introduce the "linked data" problem and the eCert solution

15:05 There will be a brief opportunity for clarification

15:10 We will split into groups to discuss the possibilities and potential problems (more on this shortly)

15:35 There will be time at the end to share key points from our discussions

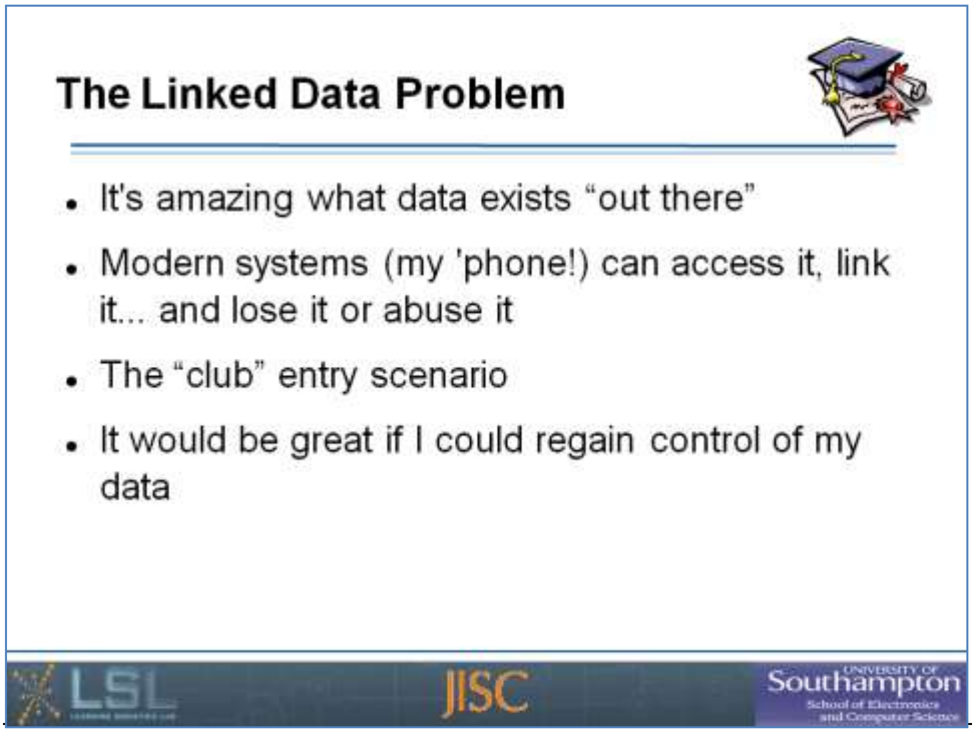
15:45 Conclusion



What we are aiming to do

What we said:

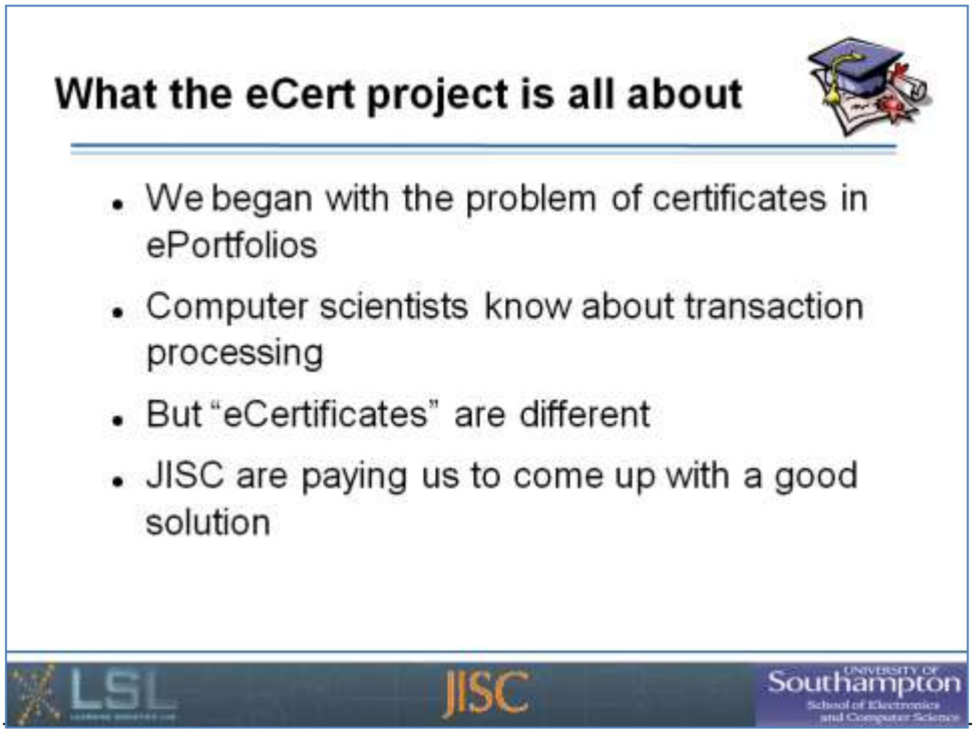
"The aim of this workshop is to enable you to engage with the ideas behind our e-Certificate system, to debate the potential benefits it offers, and to work through the potential practical issues that might be encountered in the introduction of such a system into your own institution."



The Linked Data Problem

- It's amazing what data exists “out there”
- Modern systems (my 'phone!) can access it, link it... and lose it or abuse it
- The “club” entry scenario
- It would be great if I could regain control of my data

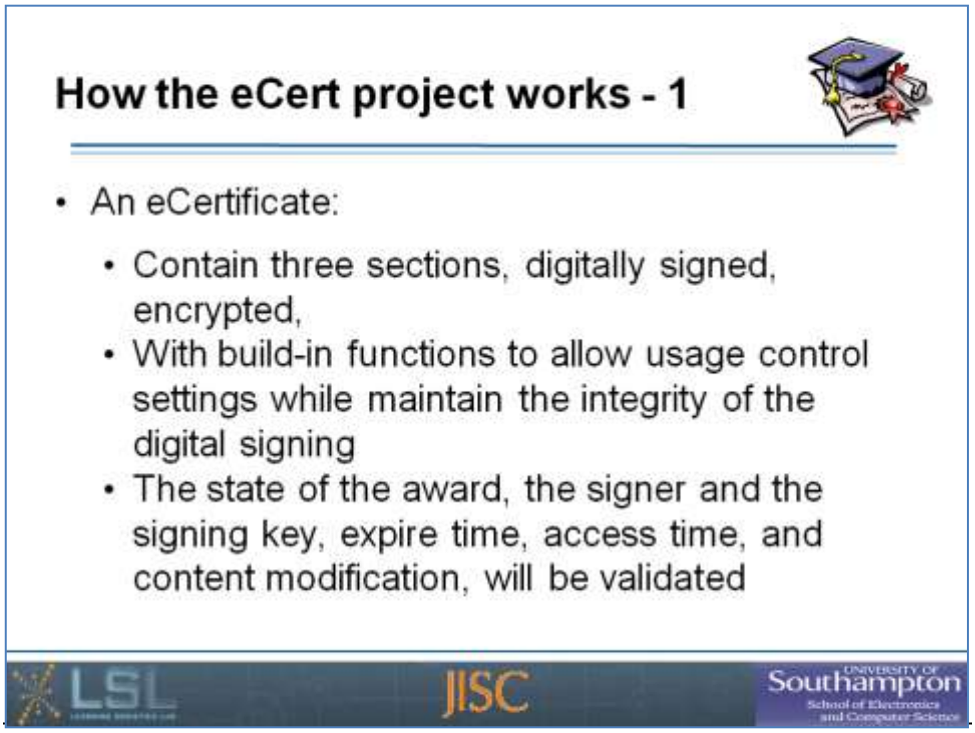
LSL
JISC
UNIVERSITY OF Southampton
School of Electronics and Computer Science



What the eCert project is all about

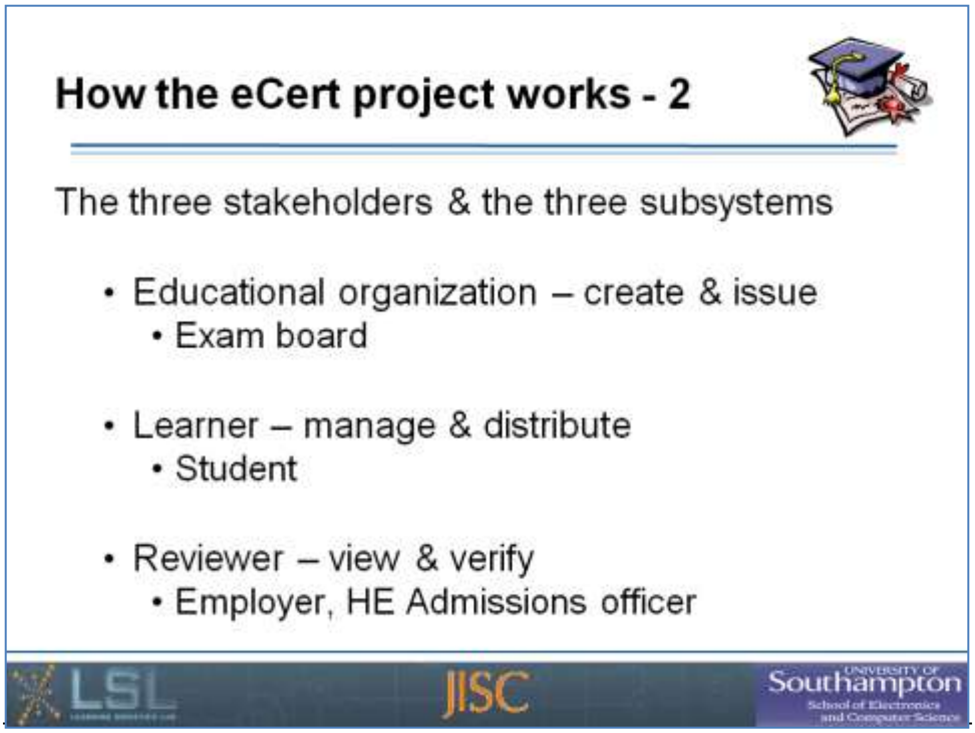
- We began with the problem of certificates in ePortfolios
- Computer scientists know about transaction processing
- But “eCertificates” are different
- JISC are paying us to come up with a good solution

LSL
JISC
UNIVERSITY OF Southampton
School of Electronics and Computer Science



How the eCert project works - 1

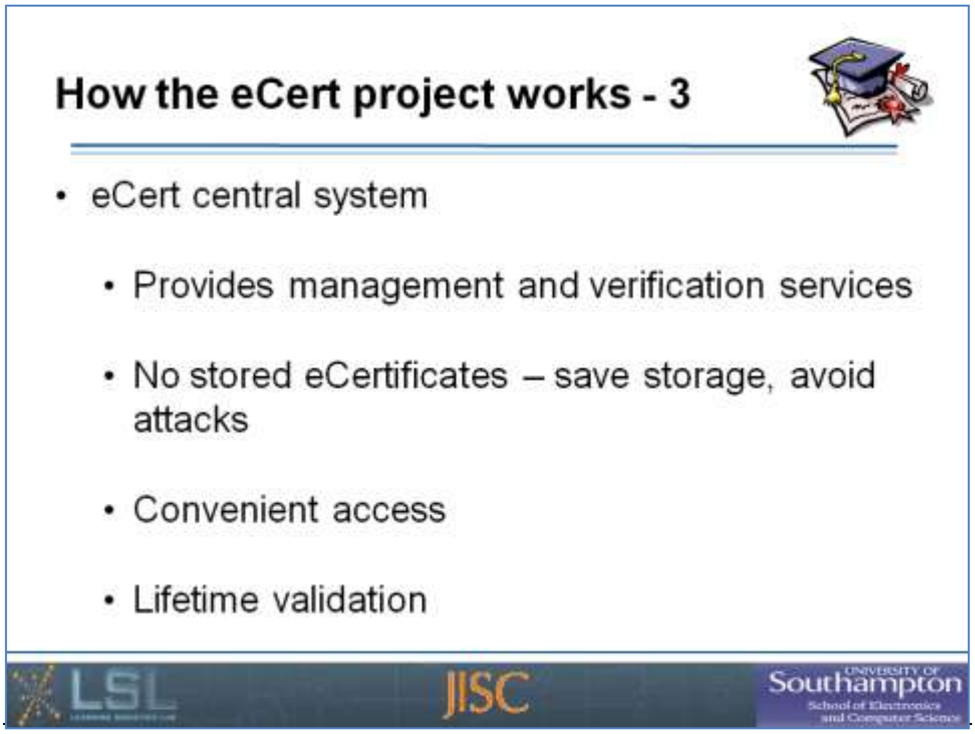
- An eCertificate:
  - Contain three sections, digitally signed, encrypted,
  - With build-in functions to allow usage control settings while maintain the integrity of the digital signing
  - The state of the award, the signer and the signing key, expire time, access time, and content modification, will be validated



How the eCert project works - 2

The three stakeholders & the three subsystems

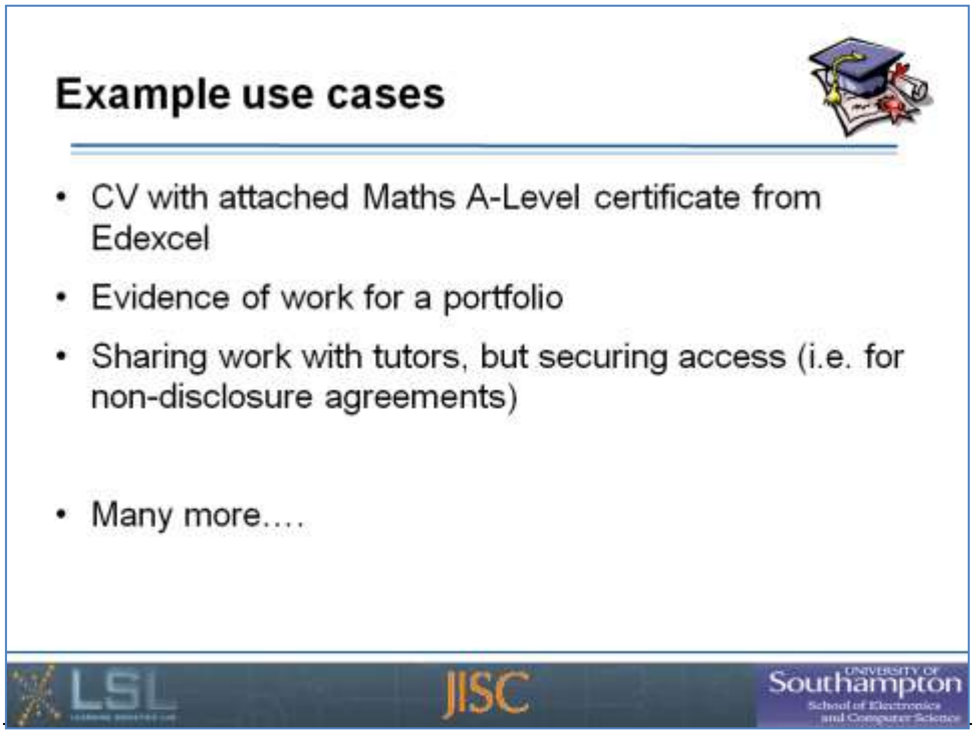
- Educational organization – create & issue
  - Exam board
- Learner – manage & distribute
  - Student
- Reviewer – view & verify
  - Employer, HE Admissions officer



How the eCert project works - 3

- eCert central system
  - Provides management and verification services
  - No stored eCertificates – save storage, avoid attacks
  - Convenient access
  - Lifetime validation

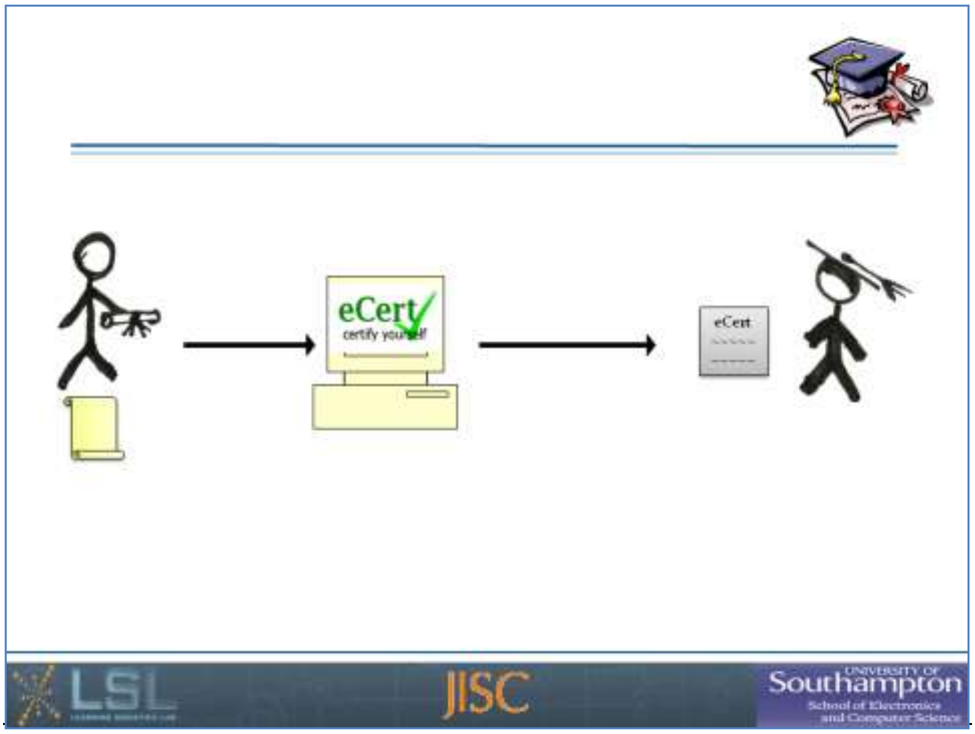
LSL
JISC
UNIVERSITY OF Southampton
School of Electronics and Computer Science

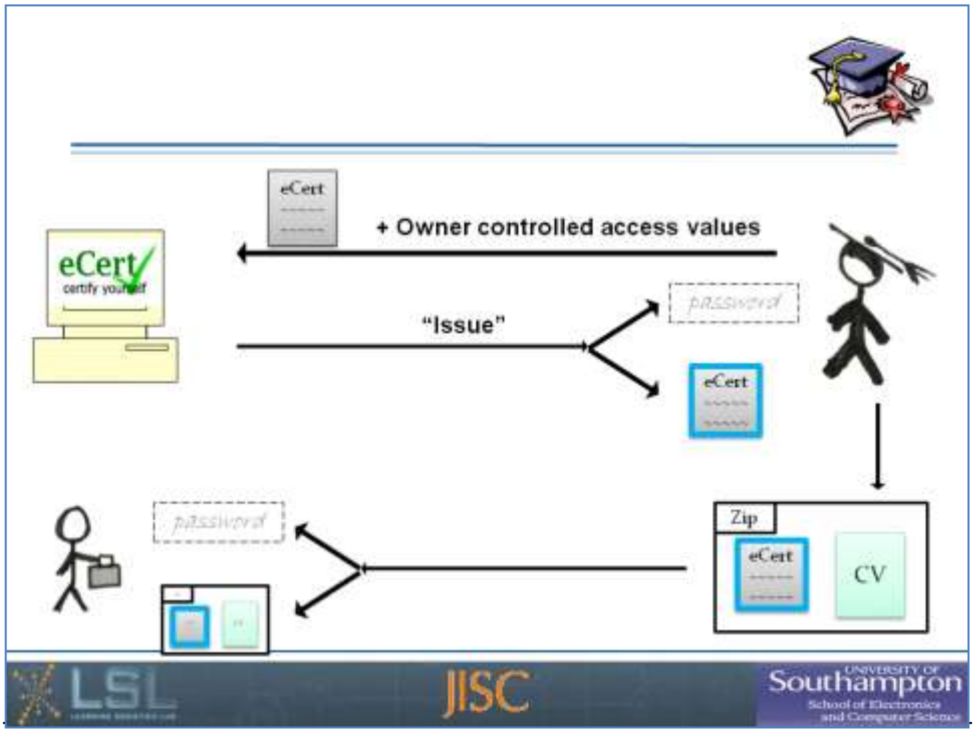


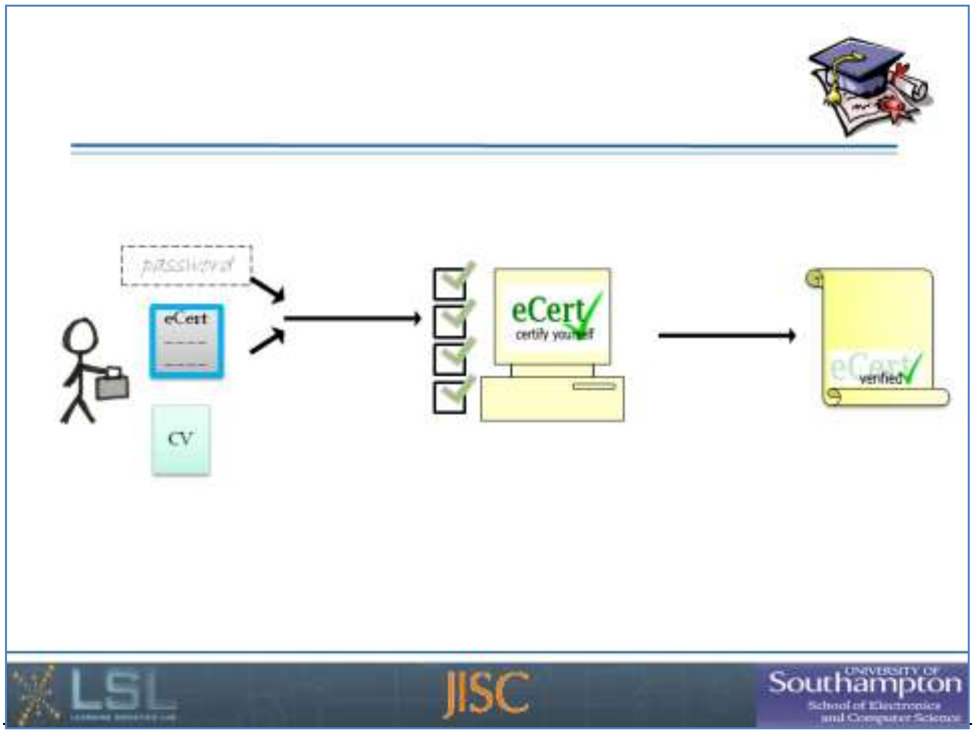
Example use cases

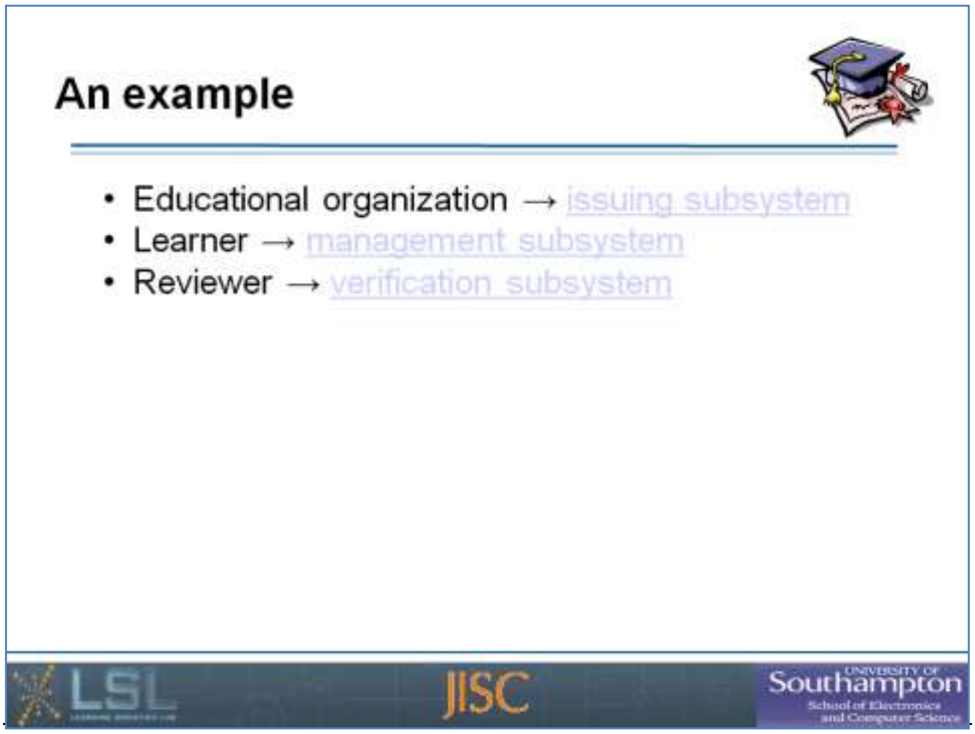
- CV with attached Maths A-Level certificate from Edexcel
- Evidence of work for a portfolio
- Sharing work with tutors, but securing access (i.e. for non-disclosure agreements)
- Many more….

LSL
JISC
UNIVERSITY OF Southampton
School of Electronics and Computer Science


eCert
certify yourself
eCert
LSL
JISC
UNIVERSITY OF Southampton
School of Electronics and Computer Science


eCert
+ Owner controlled access values
eCert
certify yourself
"Issue"
password
eCert
Zip
eCert
CV
password
LSL
JISC
UNIVERSITY OF Southampton
School of Electronics and Computer Science

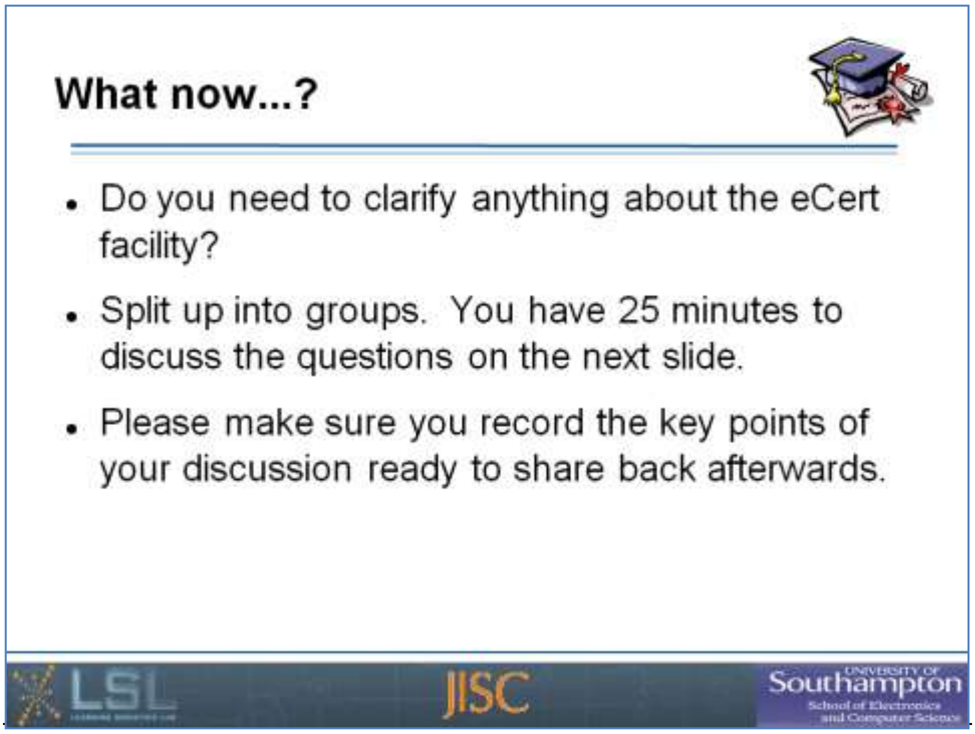

password
eCert
CV
eCert
certify yourself
eCert
verified
LSL
JISC
UNIVERSITY OF Southampton
School of Electronics and Computer Science



An example

- Educational organization → issuing subsystem
- Learner → management subsystem
- Reviewer → verification subsystem

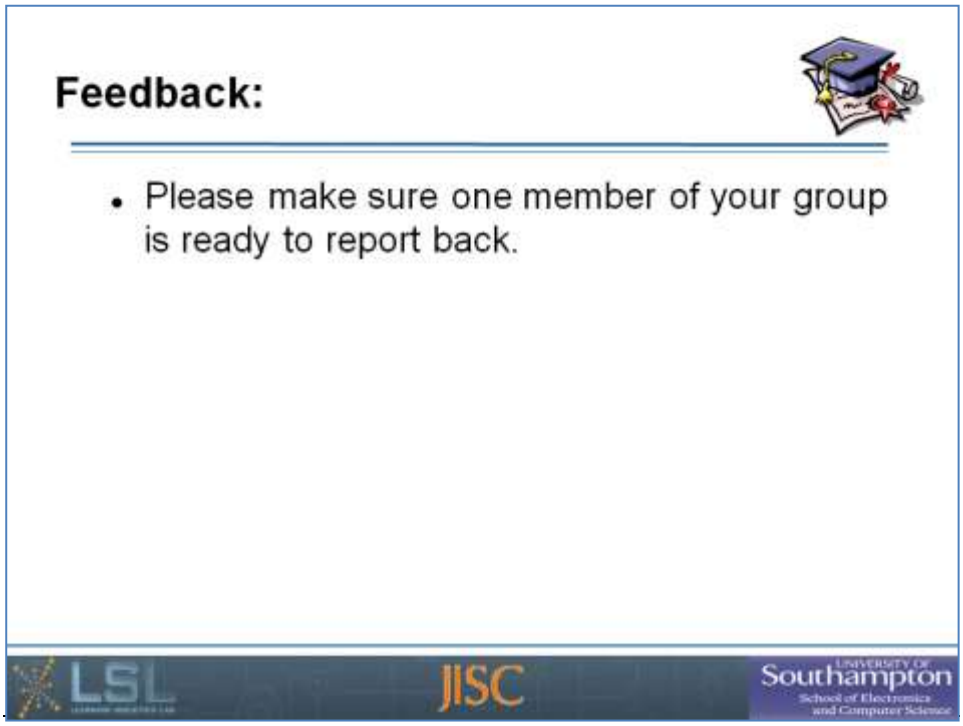
LSL
JISC
UNIVERSITY OF Southampton
School of Electronics and Computer Science



What now...?

- Do you need to clarify anything about the eCert facility?
- Split up into groups. You have 25 minutes to discuss the questions on the next slide.
- Please make sure you record the key points of your discussion ready to share back afterwards.

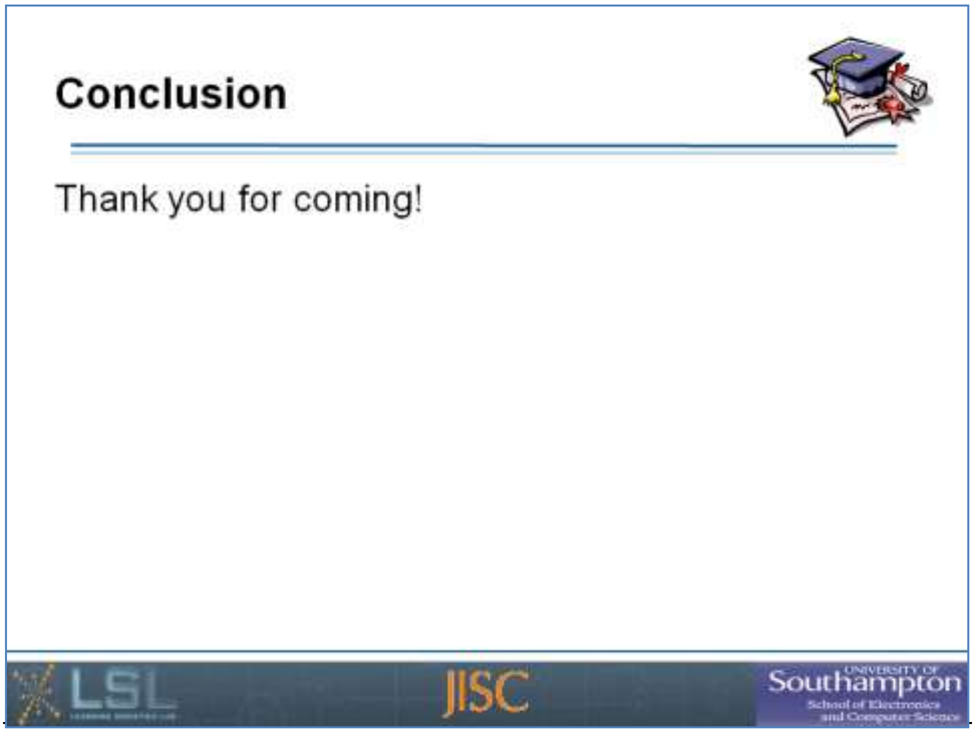
LSL JISC UNIVERSITY OF Southampton School of Electronics and Computer Science



Feedback:

- Please make sure one member of your group is ready to report back.

LSL JISC UNIVERSITY OF Southampton School of Electronics and Computer Science



Conclusion

Thank you for coming!

LSL
JISC
UNIVERSITY OF Southampton
School of Electronics and Computer Science

Appendix I: eCert workshops information

First workshop information

- Venue: Centre for International ePortfolio Development, University of Nottingham
- Date: Thursday 15th April 2010
- Participants:
    - Christopher Brown – JISC Program Manager
    - Angela Smallwood – Associate Professor, ePortfolio expert in Centre for International ePortfolio Development, University of Nottingham
    - Kirstie Coolin – eBusiness analyst in Centre for International ePortfolio Development, University of Nottingham
    - Scott Wilson – HE, security, and ePortfolio expert in JISC-CETIS
    - Simon Grant – HE, security, and ePortfolio expert in JISC-CETIS
    - John Harrison – owner of Edentity
    - Clive Church – Development Manager at EdExcel
    - Shane Sutherland – owner of PebblePad ePortfolio
- Format:
    - 10:30 Arrive, Register, coffee & biscuits
    - 11:00 Welcome to the day
    - 11:10 Morning presentation: “eCertificate issues and problems”
    - 11:25 Discussions (in groups) – defining the problem areas
    - 11:45 Report back

  - 12:15 Lunch
  - 13:15 Coffee and reassemble
  - 13:30 Introduction to the afternoon
  - 13:35 Afternoon presentation: "Towards solving the problems: the eCert plan"
  - 13:55 Round Table discussion on the proposed design and related issues
  - 14:30 Plan for the future; follow-on event, Monday 6th September 2010 (immediately before ALT-C); what do the delegates want from this project?
  - 15:00 Coffee and cakes
  - 15:30 Workshop closes

Second workshop information

- Venue: 17th International Conference of the Association for Learning Technology (ALT-C2010)
- University: of Nottingham
- Date: 7th September 2010
- Participants:
  - John Clayton – workshop facilitator, Manager of Wintec
  - Katharine Iles – Training Manager of JANET
  - Andrew Davey – technical developer of eLanguages
  - Kirstie Coolin – eBusiness analyst at the University of Nottingham
  - Matt Haigh – Project Manager of Cambridge Assessment
  - Joe Wilson – head of New Ventures at the Scottish Qualifications Authority
  - Annette Odell – Learning Technology Advisor at the University of East London
  - Peter Silvester – Web Applications Programmer at the University of Southampton

  - Iwi Ugiagbe-Green – Senior Lecturer at the Leeds Metropolitan University
  - Alex Furr – eLearning consultant and developer at the University of Southampton
  - Plus several others (names not recorded)

- Format: The workshop lasted for 60 minutes
  - 5 minutes of welcome and introduction
  - 15 minutes of introducing the “linked data” problem and the eCert solution
  - 5 minutes for a brief clarification
  - 25 minutes of group discussions for possibilities and potential problems
  - 10 minutes of feedback and conclusion

Appendix J: Terms of eCertificate

The relationships of the terms and processes for the proposed eCertificate system are analyzed and displayed in the system structure design in Figure J-1.

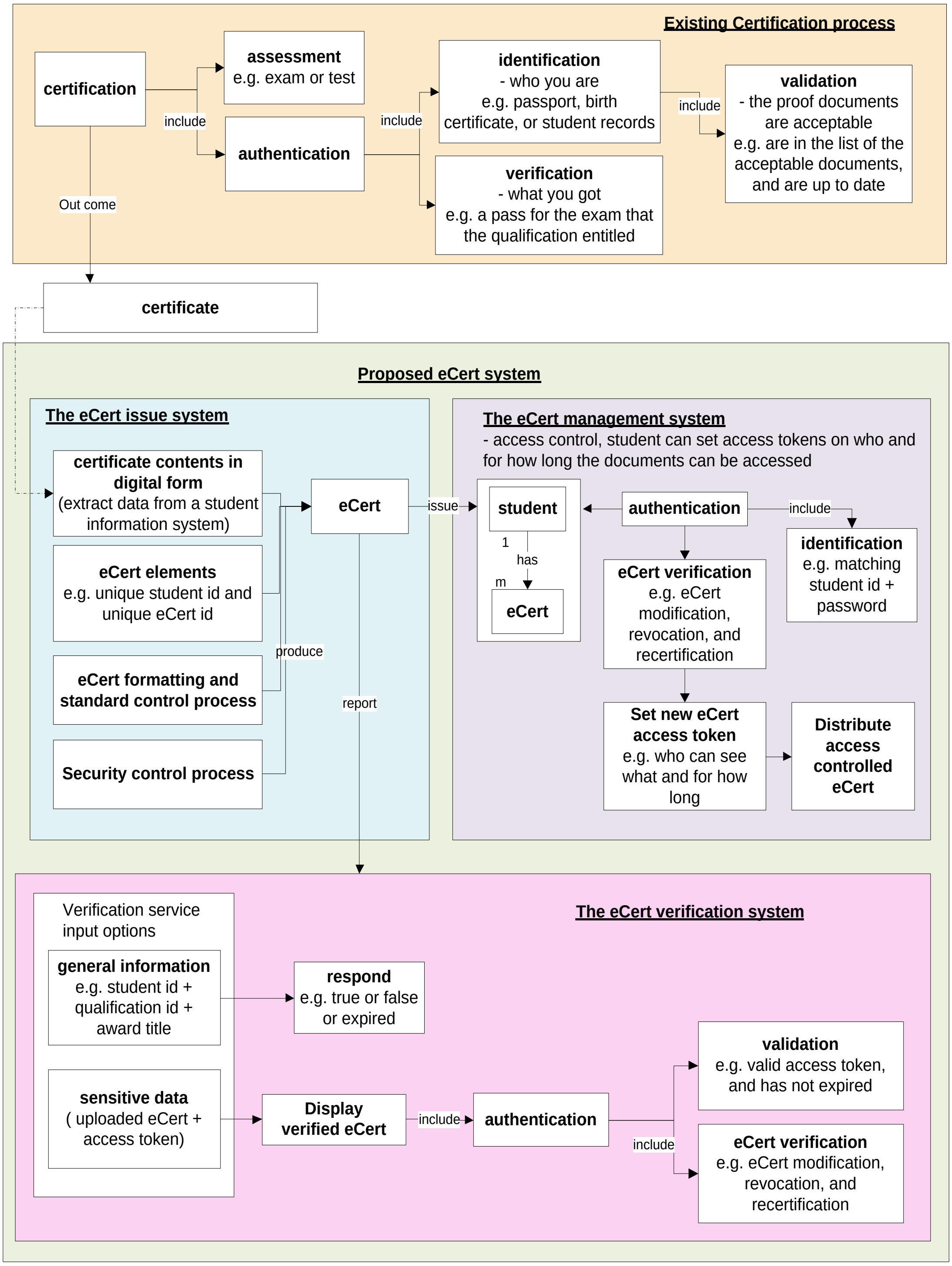

Existing Certification process
certification
include
assessment
e.g. exam or test
authentication
include
identification
- who you are
e.g. passport, birth certificate, or student records
verification
- what you got
e.g. a pass for the exam that the qualification entitled
include
validation
- the proof documents are acceptable
e.g. are in the list of the acceptable documents, and are up to date
Out come
certificate
Proposed eCert system
The eCert issue system
certificate contents in digital form
(extract data from a student information system)
eCert elements
e.g. unique student id and unique eCert id
eCert formatting and standard control process
Security control process
produce
eCert
issue
report
The eCert management system
- access control, student can set access tokens on who and for how long the documents can be accessed
student
1
has
m
eCert
authentication
include
identification
e.g. matching student id + password
eCert verification
e.g. eCert modification, revocation, and recertification
Set new eCert access token
e.g. who can see what and for how long
Distribute access controlled eCert
The eCert verification system
Verification service input options
general information
e.g. student id + qualification id + award title
sensitive data
(uploaded eCert + access token)
respond
e.g. true or false or expired
Display verified eCert
include
authentication
include
validation
e.g. valid access token, and has not expired
eCert verification
e.g. eCert modification, revocation, and recertification

Figure J-0-1 The relevant terms in the eCertificate system

Appendix K: Comparison of Shortlisted Research Methodologies

During the research methodology selection process, four appropriate research methodologies have been shortlisted. The methods are summarised and compared in the appendix. More details of the final selected methodologies (SORM and Delphi) can be found in Chapter 2 of the thesis.

Compare Category 1 – Design and Decision Making Methodologies

Design-based research (DBR) methodology[19] is a set of analytical techniques with "*iterative analysis, design, development, and implementation*" that based on "*collaboration among researchers and practitioners in real-world settings*", and hence "*leading to contextually-sensitive design principles and theories*".

[19] Wang, F., and M. Hannafin, *Design-Based Research and Technology-Enhanced Learning Environments* in Educational Technology Research and Development, 2005. 53(4): p. 5-23

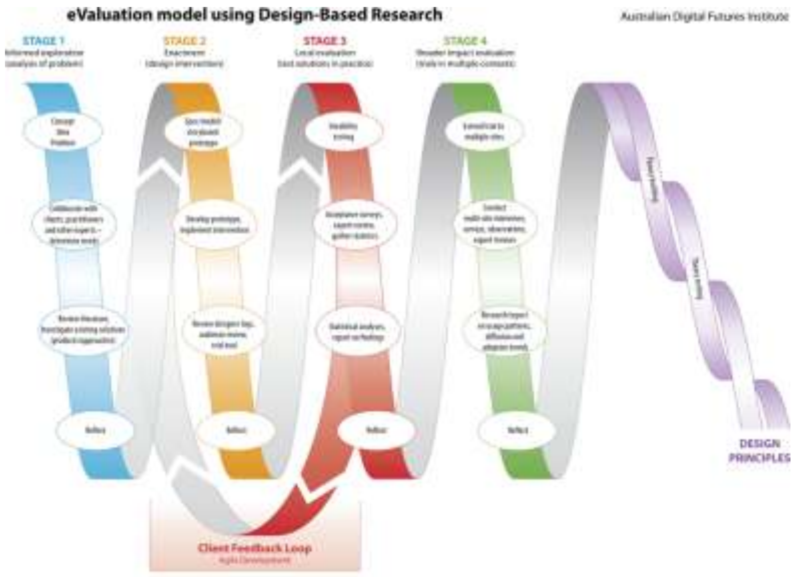


Figure K-0-1 The Design-based research methodology [20]

The Delphi methodology [21] is a "*structured communication technique that originally developed as a systematic, interactive forecasting method which relies on a panel of experts*".

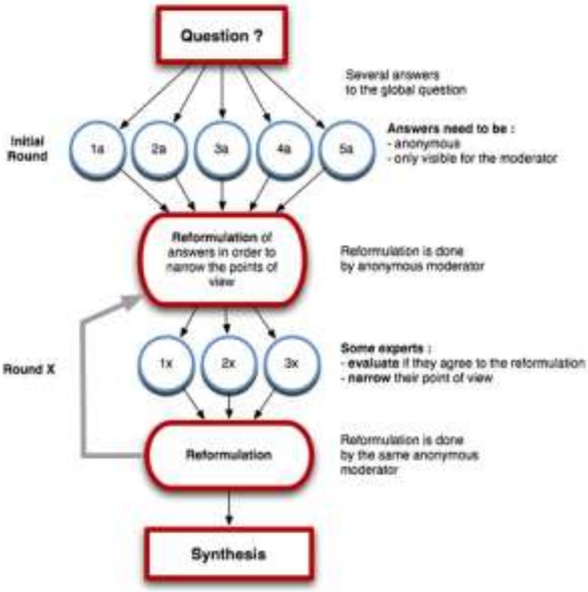


Figure K-0-2 The Delphi Methodology [22]

[20] Image reprint from http://www.emeraldinsight.com/content_images/fig/2400400104001.png

[21] Linstone, H.A. and M. Turoff, *The Delphi Method: Techniques and Applications*. 2002. p. 618.

Table K-0-1 Delphi vs. DBR

	Delphi	DBR
Comment	Evaluate design through participants' opinions	
	Have a number of iterative activities	
	Viewpoints from the feedbacks will be identified, filtered, and analysed	
	The design will be adjusted according to the analysis result at each round.	
Differences	Participants are the experts in the field	Any level of users, do not have to be experts
	Experts will review their opinions in light of the others after each round	No related information found
Benefit	Can gain the latest opinions from experts in the field As the experts can take into account of the others' opinions, the variety of answers/opinions will decrease after each round and tend towards one direction	Participants can be easily selected and organized Better ties between researchers and practitioners, and hence the research theory and practices
Limitation	Not easy to engage experts to take the activity for all the required rounds	Quality of feedback may various and hence affect the outcome

Compare Category 2 – Development Methodologies

Software Development Life Cycle (SDLC) [23] is a conceptual model, commonly used in project management. Various SDLC methodologies have been developed to

[22] Image reprint from http://www.emeraldinsight.com/content_images/fig/2400400104001.png

[23] Blanchard, B. S., & Fabrycky, W. J. (2006) *Systems engineering and analysis* (4th ed.) New Jersey: Prentice Hall.

suit different purposes. The initial SDLC involved six stages: from an initial feasibility study through maintenance of the completed application.

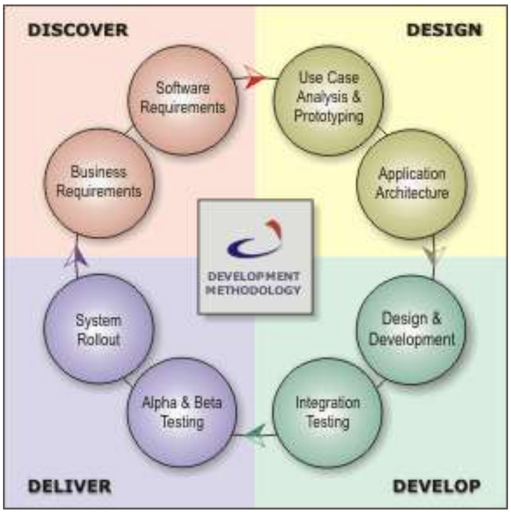


Figure K-0-3 A extended SDLC methodology [24]

The Service-Oriented Reference Model (SORM) [25] is a "*community-driven*" methodology for "*understanding how services fit together to provide functionality for a particular domain*". It was initially invented to develop the e-learning framework reference model for assessment in 2006.

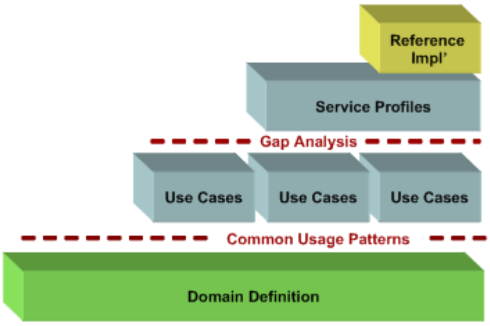


Figure K-0-4 The SORM methodology [26]

[24] Image reprint from http://klutzyuben.files.wordpress.com/2011/11/spiral1.gif

[25] Wills, G., D. Millard, S. Chennupati, E.R. Jam, I. Tulloch, L. Gilbert, and Y. Howard *FREMA: e-learning framework reference model for assessment*. FREMA Project Journal 2006; Available from: http://www.frema.ecs.soton.ac.uk/publications/index.htm .

[26] Image reprint from http://www.frema.ecs.soton.ac.uk/projectJournal/

Table K-0-2 SORM vs. SDLC

	SORM	SDLC
Comment	Both cover the stages of development life cycle	
Differences	More effect is put into the early stage of the life cycle to get the system requirements right	All stages are equal
Benefit	Focus on the early life cycle which suit the research nature of discovering the unknown issues of a new eCertificate system It was initially invented to develop the e-learning framework reference model. By using the same SOA approach, this will not only support the research for a suitable eCertificate framework, but also maximise the interoperability between the new system and the other systems across the e-Framework	Most well known, well tried and tested Development divided into distinct phases/stages which lead to easy management
Limitation	Still new, not been well tested	Inflexible, hard to cope with requirements changing Not easy to capture the true needs of users

There are in fact millions of software development methodologies, too many to summarise and compare here, but SDLC is the most well known.