# Healthcare Data Management Issues and the eCert Solution

Lisha Chen-Wilson, Xin Wang, Gary B Wills, David Argles
School of Electronic and Computer Science
University of Southampton
United Kingdom
{lcw07r, xw4g08, gbw, da}@ecs.soton.ac.uk

Charles Shoniregun
Infonomics Society
United Kingdom
cshoniregun@infonomics-society.org

***Abstract*—While our 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 our 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. What's more, information owners have increasing demands regarding their rights of ownership. Therefore, a secured user-centric healthcare information management system is not only required but also important. This paper presents a protocol for the management of healthcare information in the form of a securely distributed eHealthcare document, the eHealth-eCert. By analysis of the eHealthcare problem domain, a system has been derived with both eCert supported functions and eHealthcare unique features.**

***Keywords-security; eCertificate; eID; eHealthcare; user-centric; eCert protocol;***

## I. INTRODUCTION

Traditionally in the world of IT security, we tend to take what one might call a "Fortress Approach". We are systems orientated, and view our role as being one of protecting the system against misuse by both outside attackers and uninformed legitimate users. However, the world within which we operate is changing – we now need to deal with peer-to-peer networking, social networking and linked data. In this environment, there is increasing user concern about the security of their data.

Such concern is compounded by the knowledge that institutions that we ought to be able to depend upon are in fact unreliable. In the UK, the government has been responsible for the loss of 10 million personal records that included bank account details[1], and other examples exist of serious breaches of security protocol.

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 as noted above, 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 the confidential patient data won't be abused.

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.

Similar problem scenarios have been encountered in the realm of ePortfolios, where students maintain a record of their work and achievements. The intention is to make this record accessible to potential recruiters and employers, but they also may wish to protect against unauthorised collection of personal data by disreputable parties.

In order to address the ePortfolio problem, the eCert project has developed a user-centric eDocument transmission protocol, the eCert protocol, which enables users to share their data whilst still maintaining a measure of control over when and how it may be viewed. It has been demonstrated that this protocol has wider application than just the ePortfolio scenario, with an additional project, mobile eID, demonstrating how this same approach can provide a way for personal information, such as on a passport, to be made available for viewing by potentially untrustworthy parties, such as nightclub owners.

In this paper, we will explore the eCert approach as a mechanism for providing user-centric control over eHealth data, derive a design to achieve our goals, and then assess the issues that arise as a result.

## II. CURRENT HEALTHCARE INFORMATION SYSTEMS

Traditionally, healthcare data has been stored in filing cabinets. "Data transmission" has consisted of paper records being put into envelopes and sending them by post, leading to incidents of records being lost. In progressing to computerised systems, the filing cabinet metaphor has typically been applied to digital database design.

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

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

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 who have no right to know.

There are two competing aims we need to consider when designing a secure system for sharing of healthcare data. Firstly, "Can patient authorised data to be made available without reservation or delay in an emergency scenario?" Therefore, the patient does not want the doctor(s) to be hindered in treating them because their date cannot be accessed. However, to ensure that sensitive personal details are not visible to those that have no right to see them. These two aims are conflict paradox. The safest way to ensure best practice in an accident and emergency (A&E) is to be able to view patient data as when it is required. The question remains "Can my data be visible to those who are not obliged or authorised to do so.

A full healthcare information system includes the full data relating to a patient's care and includes information on support systems, for examples. In this paper, we wish to restrict our focus specifically to patient data. So we will focus on the security issues of patients' data management, known in this paper as the Patient Record System (PRS).

## III. HEALTHCARE SCENARIO

A number of healthcare scenarios have been selected and described below:

### A. Sharing Healthcare Records:

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

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

### B. 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 wrong diagnosis, while loss of records will waste inestimable amounts of valuable time.

Scenario 2: Patient A has history of heart problems and has been taken to a hospital for an 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.

## IV. UNDERLYING TECHNOLOGIES

### A. eCert as policy for the signing and key management

In order to provide a solution for our two healthcare scenarios, we wish to employ the eCert protocol as mentioned earlier. The eCert approach defines a secured and signed document that enables the user to determine what a reviewer is allowed to see and for how long. The file standard defines the content, format, and structure of what a eCert file is[2].

File structure: an eCert file will contain three sections: metadata, text content, and supported file outputs (can be in any format). Both the text content and the support files can be subdivided into two types: compulsory and optional. The text output will formed the main content, no matter compulsory or optional; the compulsory file outputs will be embedded within the main content, while the optional files will be attached.

Signing method: optional files will be signed individually using 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 enveloped signature, and encrypted before 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, depend on the applied situations. 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 link to the eCert central server. In addition, an online central service will provide the public access for the required service. In some cases, identity management system will be involved for access control.

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

A number of features of the eCert protocol may be noted.

#### 1) Secure:

The eCert approach is based on digital signing, but also addresses what is called the "eCertificate squared" problem. We not only need to ensure non-repudiation and the authenticity of the document, but we also need to detect current validity to cover the potential revocation of the data as well as the classical case of the revocation of the signing key. This means it is more secure than conventional digital signing.

#### 2) User-centric:

By taking this approach, we address the ownership right. 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 [3]".

*3) Lifetime Validation:*

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

*4) Verifiable distributed data:*

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

### *B. The eCertificate and mobile eID as applied examples*

The eCert protocol has been successfully applied to two eDocument transmitting use cases, the eCertificate for ePortfolio, and the eID in mobile environments.

*1) The eCertificate project*

The eCert project[4] is a UK government-sponsored project to implement an electronic version of a Qualification Certificates System. At the heart of this project is the initial eCert protocol which is being developed to address security issues which originally arose as a concern within the field of ePortfolios.

With the employed eCert protocol, it has proposed a user-centric eCertificate system, which enables the eCertificate owners to have usage control over their documents before distributing to the reviewers, prevent unauthorized modification and distribution.

The Delphi methodology[5] was employed for the evaluation of eCertificate system design through out its development stages alongside the SORM research methodology[6]. By following this method, a group of domain experts in the UK have been selected for the purpose of security system design, ePortfolio study, and represent of the stakeholders, this includes employment managers, IT security experts, exam board managers, and ePortfolio researchers. Two workshops have been run during two stages of the development to collect the professional opinions from these experts: one at the end of the system design stage, aim to evaluate and adjust the system from the strategic level; and the other one on demo completion stage, the system is brought back to the domain experts after the design adjustments and demonstrator production, aim to evaluate the system from the technical level.

The system has been further evaluated under a subproject named Integrating eCert in ePortfolios[7] to test the usage of the design principle. Through this project, the eCertificate system has been integrated and operative the UK ePortfolio system, the eFolio[8], and an Australian system, the Mahara[9]. Both systems can now be fully utilized. As a result, it has proved the usage of the system successfully as it can not only be used standalone but can also be plugged into other applications. The eCert protocol has also been improved through the process.

*2) The Mobile eID project*

As the case of eCertificate study represents the typical eDocument transmitting issues, it is believed that the concept of its solution could in turn solve the eDocument transmitting issues in other cases. Therefore, with the aim of proving this hypothesis, evaluate the applicability of the eCert protocol in a wider domain, the concept of the eCertificate solution is being tested under a project, Mobile eID, to explore the issues that arise in implementing the eCert protocol within a mobile platform to provide certified, certifiable, and protected identity information.

The eID system has been compared and analysis with the eCertificate system in terms of file structure, system structure, transferring paths, verifying processes, and their applied environments. it has been noted that even the idea of the eID and eCertificate is quite close, they are different in many ways. The eCert protocol that 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.[10]

As a result, the eCert protocol has been reviewed, and the successful eID project, which implemented a working demo system on Android platform, has proved that the eCert protocol can be applied in a wide eDocument transmitting domain.

## V. BENEFIS AND DRAWBACKS ON APPLYING ECERT TO EHEALTHCARE

The eCert protocol provides a unique, secure and trusted system for the management of data with a secure user-centric approach. This user-centric focus is key to the case of patient records management. Unlike the case of mobile eID, which has drawbacks of requiring reverse engineering process due to the immature of the eCert protocol, there is currently no known drawback for the eCert protocol to be employed in the case of eHealthcare - the updated version of eCert protocol has been designed to include the abstracted comment features in eDocument transmitting domain.

However, the eCert protocol is newly developed, even it has been successfully evaluated through two projects, it may still contain some unaddressed hidden issues.

## VI. THE PROPOSED EHEALTHCARE PROTOCOL

In applying the eCert protocol to the eHealthcare problem, our aim is to provide a mechanism for user-centric distribution of data. In this way, we seek to give patients control of their data in terms of who is allowed to see it. In order to achieve this aim, we require security controls for the issue and distribution of data, and a verification service for this distributed data.

### *A. Use case*

In developing the use cases for this problem, we note that there are three stakeholders: the issuer, the owner (i.e. patient), and the reviewer. We may consider a couple of PRS use case scenarios which have been developed to highlight the benefits and issues related to the data transferring in the healthcare sector. For example, one of the use cases, Record

healthcare history, is shown in Table1. These use cases are framed in terms of using a PRS.

Table1. Use case - Record healthcare history

| **eHealthcare use case – Record healthcare history** | |
|---|---|
| **Description** | A healthcare sector staff wishes to record a patient's healthcare information after providing the treatment |
| **Actors** | • Patient<br>• Healthcare sector staff |
| **Scenario** | 1. Patient requires treatment and provide related information<br>2. Healthcare sector staff retrieves the patient's healthcare history from PRS, and assess the patient<br>3. patient receives treatment<br>4. healthcare sector staff record the treatment process and result in PRS |
| **Variations** | If the patient has no record in the PRS yet, the healthcare sector staff can start from creating a new account |
| **Benefits** | • Patient: all treatment history is in record, no need to memorise them, specially the details in medical terms.<br>• 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.<br>• Incorrect record will lead to wrong treatments<br>• Lost of record or a whole database will affect the efficient of assessments<br>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. forward it to a private healthcare provider) |

*B. eHealthcare compared with eCertificate & eID*

By comparing the use cases of the three different systems, we may see that the implementation of the eCert protocol for eHealthcare is a mix version of the eCertificate and eID applications, but with some unique features:

*1) 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 to 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 diagrammatically in Figure 1.

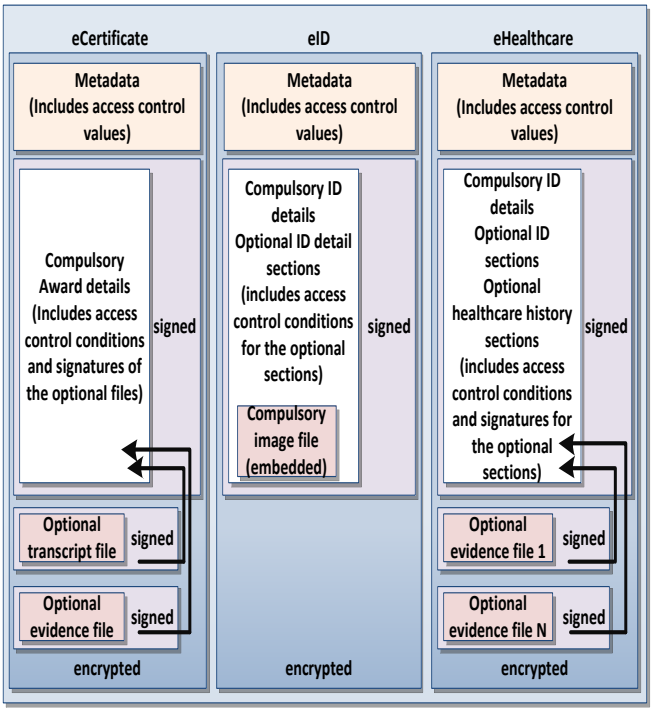


Figure 1. eCert file structures

*2) 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 of a certified healthcare sector, and they all have the needs and right to further transfer the document to its desired department. Therefore, not only the owner, but all stakeholders, should have the usage control of the document. But, to protect the 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 what they have on receipt (no hidden information should be made available on further transmission). This is shown diagrammatically in Figure 2.

*3) Technical skills:*

Unlike the case of eCertificate and eID, the information owners in the eHealthcare case are patients, which can be any age, may be new to computing technologies, or may have no capability of managing their own documents. We need to find a way so that they can have the required data in a simple but secured method.

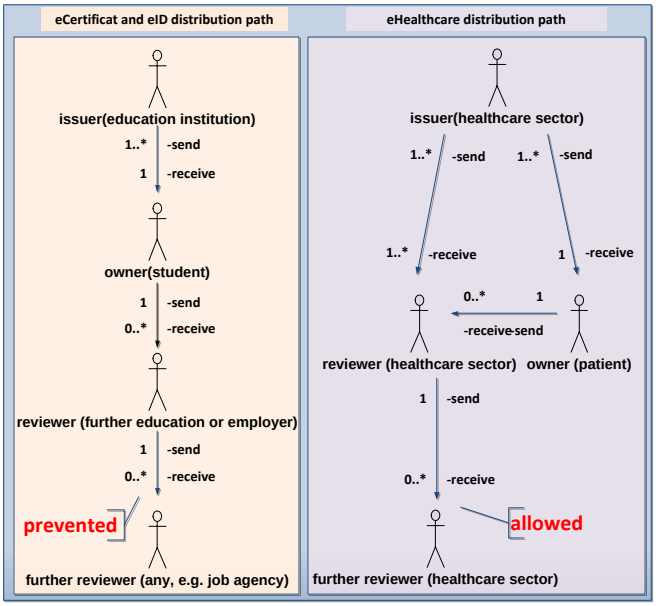


Figure 2. document transmission paths

*C. 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 link 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 display the enabled visible section(s). The user is allowed to set further access control to 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 secured to ensure confidentiality, integrity and availability during its issue, distribution, management, and verification processes. This is shown as use cases in figure 3.

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 available to which receiver and for how long. As all stakeholders can be both sender and receiver, they will all have the right the set access control values.

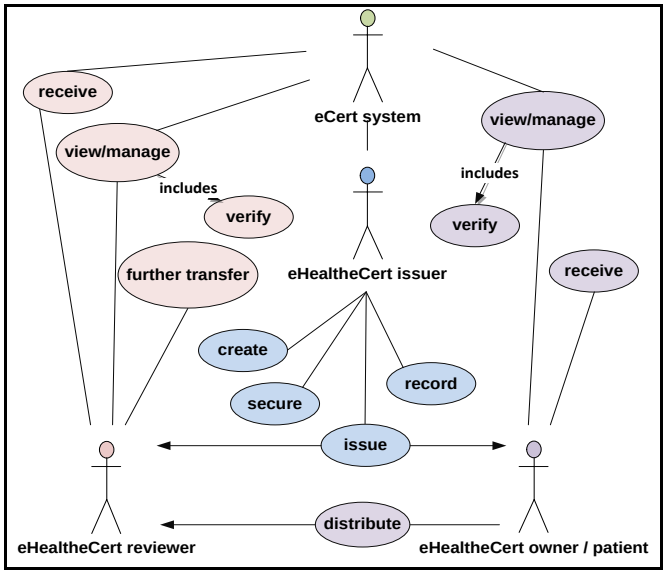


Figure 3. eHealthcare system use cases

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

Staff 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 it.

When issuing the initial eHealth-eCert document to the patient, the system default encryption key will be employed to enable all stakeholders can access it. This appears to mitigate against the 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. What is more, a list of encrypting options could be provided for advance users with specified privacy requirements. This use of keys is indicated in Table 2.

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. By applying the eCert technique, we employ the eCert signature method with the corresponding system structure design so that the document access key will be verified, together with its signing key status, content status, expiry time, and access time. These are all 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 records, but will also benefit some patients. This is especially so for those who

know they may require emergency treatments. 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, who, or 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"[11], as the eCert technique enables the document to be owner-controllable, verifiable, securely transferred, with lifetime validation, and easy backup.

Table2. 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 |

## VII. ISSUES

The balance for the data confidential and availability in security control in healthcare is extreme: on one hand, the patients' data is considered as highly sensitive, required high level of security; on the other hand, the information need 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 provide the functions for the patients to upgrade the security level if concerned. This is aim for the availability, especially if the document is the only available verifiable information that provided by an incapable patient in an emergency situation.

Whether this approach is suitable or not, could become the main security argument.

## VIII. CONCLUSION AND FUTURE WORK

In this paper we have identified the issues around eCertification in eHealth documents. This has led to the eHealth protocol and design of a system to address the issues identified.

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 system. It could be the answer to the current healthcare information system security problems. It also provides advantages over the exiting 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. In the next stage of the project we will investigate various methods and approaches to implement the design and evaluate such an approach.

## REFERENCE


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

[2] L. Chen-Wilson, A. Gravell, and D. Argles, "Giving You back Control of Your Data: Digital Signing Practical Issues and the eCert Solution.," in *IEEE World Congress on Internet Security (WorldCIS)*, London, UK, 2011, pp. 107-113.

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

[4] L. Chen-Wilson. (2010). *The eCert Project*. Available: http://ecert.ecs.soton.ac.uk/ (Access date: 9 November 2010).

[5] H. A. Linstone, and M. Turoff (2002). *The Delphi Method: Techniques and Applications*. Available: http://is.njit.edu/pubs/delphibook/(Access date: 03 June 2010).

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

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

[8] A. Furr. *eFolio: University of Southampton ePortfolio system*. Available: http://www.efolio.soton.ac.uk/. (Access date: 10 May 2010).

[9] K. Pacific. *Mahara: Open source eportfolios*. Available: http://mahara.org/. (Access date: 07 May 2010).

[10] M. Zenise, 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)*, London, UK, 2011, pp. 212-217.

[11] C. A. Shoniregun, "Security Comprehension of Healthcare Information Systems," presented at the IEEE World Congress on Internet Security (WorldCIS), London, UK, 2011.