

# BECTA Proposed e-Portfolio Security Model

14 March 2007

# BECTA Proposed e-Portfolio Security Model

Detailed assessment of security  
requirements and candidate solutions for  
e-Portfolio systems

14 March 2007

© PA Knowledge Limited 2007

Prepared for:	Stuart Jones - BECTA	PA Consulting Group 123 Buckingham Palace Road London SW1W 9SR Tel: +44 20 7730 9000
Prepared by:	Jamie Lasky and John Hughes	Fax: +44 20 7333 5050 <a href="http://www.paconsulting.com">www.paconsulting.com</a>

Version: 1.0

## ***EXECUTIVE SUMMARY***

---

This report provides a proposed security model and approach to securing e-Portfolios. It examines the requirements for security and describes some of the issues in deploying an e-Portfolio system securely. The report examines and describes a number of candidate security technologies as well as the potential use of existing or planned infrastructures.

The report describes a number of recommendations, including areas of further research and work.

# TABLE OF CONTENTS

## Executive Summary

- 1. Introduction**
  - 1.1 Background and Overview
  - 1.2 Description of e-Portfolios
  
- 2. E-Portfolio security models**
  - 2.1 Overview
  - 2.2 High Level Security Model
  - 2.3 Learner Perspective
  - 2.4 Remote User Perspective
  - 2.5 Source Perspective
  - 2.6 Target Perspective
  
- 3. Security Functions, Services & Mechanisms**
  - 3.1 System Security Model
  - 3.2 Security Functions and Services
  - 3.3 Infrastructure and Security Mechanisms
  - 3.4 Interoperability Security Requirements
  
- 4. Use Case Scenarios**
  - 4.1 Introduction
  
- 5. Other Recommendations**
  - 5.1 Security and Privacy
  - 5.2 Intellectual Property and Digital Rights
  - 5.3 Data Protection
  - 5.4 Use Case Scenarios

## Appendices

**Appendix A: Federation Techniques**

**Appendix B: Glossary and Terminology**

## 1. INTRODUCTION

---

### 1.1 BACKGROUND AND OVERVIEW

Portfolios have long been used in some disciplines to organise and present work; to provide a context for discussion, review and feedback from instructors, mentors, colleagues and friends and to demonstrate progress and accomplishments over time.

With work becoming increasingly digital, providing a common format for text, graphics, sound and video, the portfolio model can be extended to more disciplines and purposes. Network storage can remove the limitations of local disk space on file size. Network access can greatly expand opportunities for input and interaction beyond the physical limitations of traditional portfolios.

With the practical issues of storage, bandwidth, access and security being resolved, the essential elements of a traditional portfolio are being amplified through e-Portfolio projects.

E-Portfolios also change the resources available to the student, teacher and learning community, as well as change the information access and flow. Working in a common space where teachers, learning providers and students can selectively control who can view and comment makes learning a much more interactive process.

### 1.2 DESCRIPTION OF E-PORTFOLIOS

Within education, a **portfolio** refers to a personal collection of information describing and documenting an individual's progress, achievements and learning. Portfolios have been used for many years within learning programmes, particularly vocational and professional programmes. An e-Portfolio is an electronic version of a portfolio under the Learners' direct control. The list below defines the characteristics of an e-Portfolio:

- Supports lifelong learning;
- Provides a record of progress;
- Collates evidence for assessment of outcomes;
- Contains an overview of learners' progression and achievements to date;
- Enables a multiple of authorised readers to view progress, achievements and attainments, including institutions and potential employers;
- Encourages reflection on the process of learning and development.

An e-Portfolio is an *application*, the **engine** which enables the individual learner to join together what they have learned through different services so that they can demonstrate to another institution, an employer or a parent what they have done, how they are succeeding and who they are.

E-Portfolio is a means by which individuals can understand their skills, the skills they require and how they can achieve higher skills. In this way individuals can further themselves and their career.

E-Portfolio systems may offer any of these other services:

- A means of accessing personal information held in distributed databases;
- A means of selecting sets of items for a specific purpose and making connections and associations between them and with specified standards;
- A means of allowing other specific individuals to view any given selection, and controlling the time within which they are allowed to view;
- Guidance to support review and choice, reflection and action planning;
- A means of sharing and collaborating with individuals and communities.

### 1.2.1 E-Portfolio Modes of Usage and Types

It is useful to think of four main areas of use for e-Portfolios:

- Assessment;
- Transition;
- Presentation;
- Learning.

<h3>Assessment</h3> <p>For assessing or matching against specified criteria as in a qualification or job specification for example, evidence for a Key Skill or NVQ.</p>	<h3>Transition</h3> <p>For providing evidence and records at transition points for example, transfer of pupil information from primary to secondary school</p>
<h3>Presentation</h3> <p>For presenting information or achievements, often to particular audiences for example, selected design drawings to show to a client or prospective employer.</p>	<h3>Learning</h3> <p>For personal and group information, often related to learning, reflection and self-assessment for example, a record of learning goals, achievements towards them and teacher feedback.</p>

## **Assessment**

For assessing or matching against specified criteria as in a qualification or job specification, for example, evidence for a key skill or NVQ. Evidence gathering for formal qualification validation. Requires external authentication of held records and provides the link to assessment achievements.

## **Transition**

Enables capturing, accessing, editing and arranging of information. For providing evidence and records at transition points, for example, transfer of pupil information from primary to secondary school.

## **Presentation**

Enables the learner to collate, share and present the evidence of their capability and achievements. It will include examples of their work which may be in specific collections for differing purposes.

## **Learning**

For personal and group information, often related to learning, reflection and self-assessment, for example, a record of learning goals and outcomes, achievements towards them and teacher feedback.

*The aim is to satisfy all types of e-Portfolio recognising that not all e-Portfolio types will need to support all security functions.*

## **2. *E-PORTFOLIO SECURITY MODELS***

---

### **2.1 OVERVIEW**

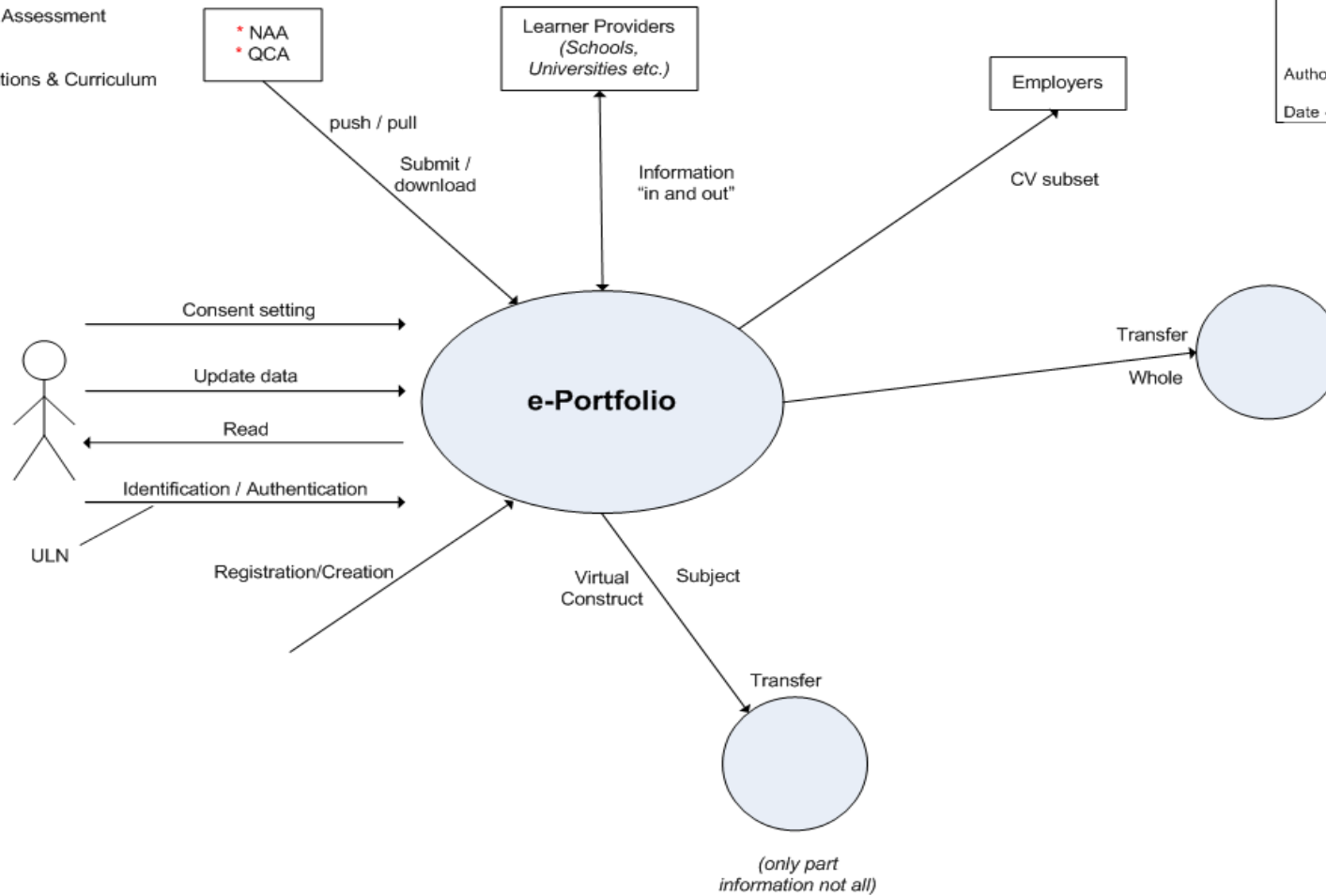
We have defined a security model with four perspectives around a high-level e-Portfolio security model. These are as follows:

- High Level Security Model
- Learner Perspective
- Remote User Perspective
- Source Perspective
- Target Perspective

The high-level security model and each of the perspectives are described in the following sections.

## 2.2 HIGH LEVEL SECURITY MODEL

- \* National Assessment Agency
- \* Qualifications & Curriculum Authority



### **2.2.1 High Level Security Model Description**

The e-Portfolio high-level security model is a learner centric model, whereby the learner feels in full control. Learning providers, attainment authorities and potential employers play a vital role in the exchange, interaction and transfer of information within the e-Portfolio.

Attainment authorities (NAA, QCA) are likely to have a 'push' and 'pull' effect on the e-Portfolio. Submitting attainment information (push) and downloading (pull) from the e-Portfolio will be commonplace.

There will be an interaction with the learning providers and the e-Portfolio with information going in and out on a regular basis.

CV's or subsets of the CV will be transferred and submitted to employers in a secure manner.

The learner can perform a number of functions incorporating certain security elements. These include:

- Registration;
- Logon Authentication;
- Consent Management;
- Content Management;
- Transfer Management;
- Transfer Security.

#### **Registration**

The learner will register for an e-Portfolio either directly or indirectly. Registration will require collection of core biographical details. When first being registered into the e-Portfolio, it will be usual to verify the claimed identity of the person being registered. This process is called either Identity Authentication or Identity Verification.

Biometric authentication may also be used to measure and analyse human and behavioural characteristics for later authentication purposes.

#### **Logon Authentication**

Access to the e-Portfolio either by the learner or by a remote user will require them to be authenticated during a "logon" process.

#### **Consent Management**

The e-Portfolio stores learner information in a secure manner. Access to the e-Portfolio can be limited to those people to whom the learner has given permission to view their e-Portfolio. The primary owner of the e-Portfolio is the learner who has the ability to

manage the appropriate access permissions. The e-Portfolio access and consent model will also need to support the following aspects:

- A defined set of roles will be required i.e. learner, assessor, teacher etc.
- A set of appropriate permissions will need to be defined i.e. read, write, import, export etc.
- Certain roles may be able to manipulate parts of the e-Portfolio. For instance a teacher inputting the results of an examination.

### **Content Management**

Ongoing maintenance of biographical details is required, for instance change of address. Adding new contents to the e-Portfolio would also be a requirement of the learner. Registering remote users in relation to assigning access permissions would also be relevant. These various users include teacher, lecturer, potential employers etc.

### **Transfer Management**

Transfer of information within an e-Portfolio can occur when transferring information to another system (this could be either the full e-Portfolio or just a subset).

### **Transfer Security**

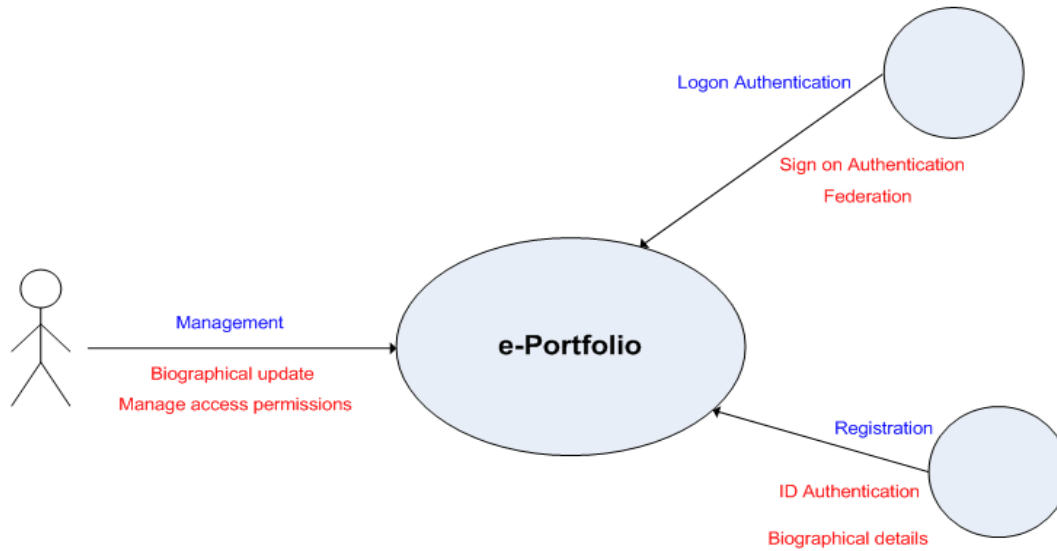
Security of transferring information within an e-Portfolio is of paramount importance. Secure transfer will need to enable confidentiality of data, validation of the integrity of the data, authenticity of the origination of the data and non-repudiation between two communicating parties.

### **Federation**

A *federation* is an association of organisations that come together to exchange information as appropriate about their users and resources in order to enable collaborations and transactions. *Federated identity* means the management of identity information between members of a federation.

Federated identity allows for information about users in one security domain to be provided to other organisations in a common federation. This allows for cross-domain single sign-on and removes the need for content providers to maintain usernames and passwords. Identity Providers supply user information, while Service Providers consume this information and gate access to secure content. This technique will be important within an e-Portfolio system enabling users on other systems to securely gain access to relevant e-Portfolio content.

## 2.3 LEARNER PERSPECTIVE



### **2.3.1 Learner Perspective Description**

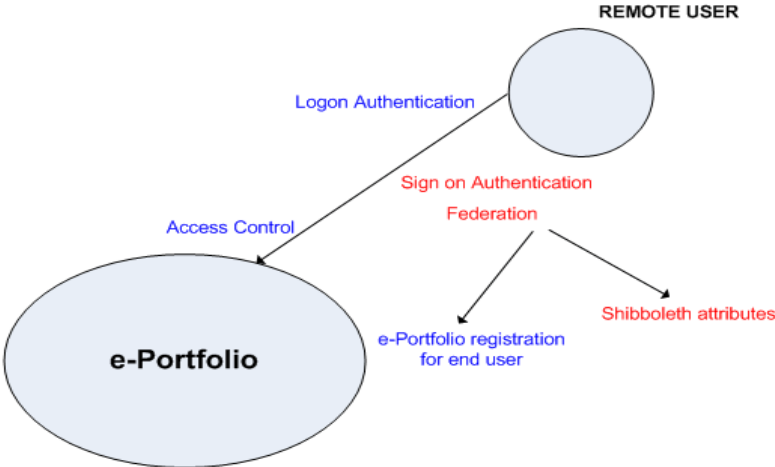
The learner will be provided with a number of functions to manage their e-Portfolio.

The learner is responsible for updating their core biographical details and managing appropriate access permissions to view their e-Portfolio.

The learner can register to the e-Portfolio by confirming their identity through standard 'logon' authentication and collection of core biographical details. Biometric authentication may also be used to measure and analyse human and behavioural characteristics for authentication purposes.

The learner may logon directly to the e-Portfolio or through a federated single sign-on authentication (SSO) that will enable the learner to be authenticated to another system but then be able to gain access to the e-Portfolio resources.

2.4 REMOTE USER PERSPECTIVE



### **2.4.1 Remote User Perspective Description**

A remote user is defined as anyone other than the learner i.e. teacher, lecturer, learning providers, potential employers and education/attainment authorities.

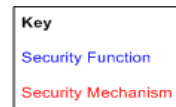
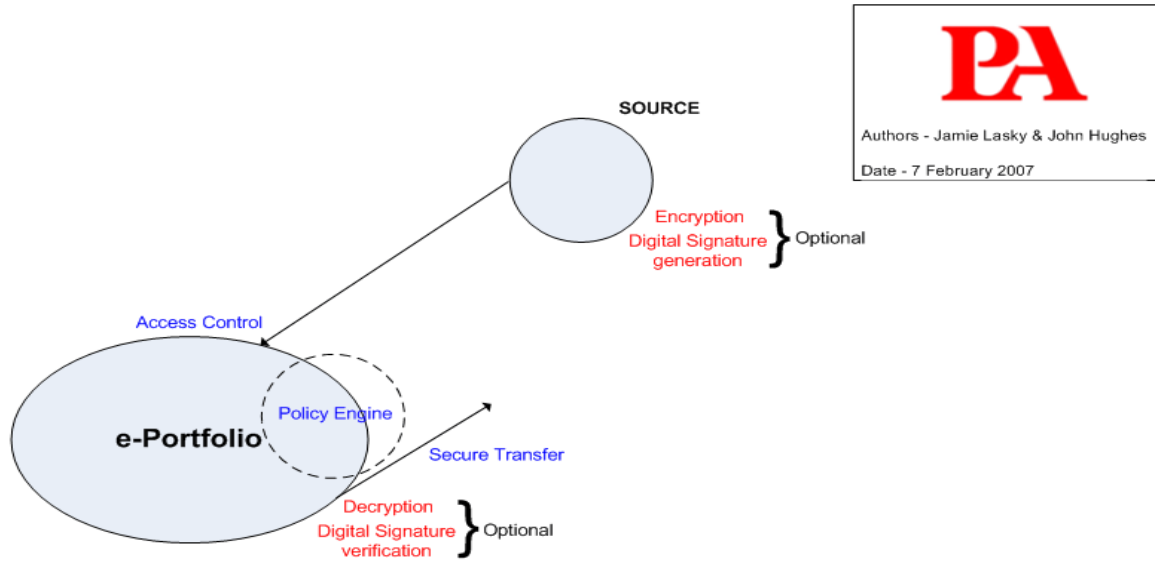
Standard logon authentication from the remote user will enable them to access certain areas of the learner's e-Portfolio, dependant on the access control model.

The remote user will not directly be able to manage the e-Portfolio. As described above, the e-Portfolio access and consent model will need to support the following aspects:

- A defined set of roles will be required i.e. learner, assessor, teacher etc.
- A set of appropriate permissions will need to be defined i.e. read, write, import, export etc.
- Certain roles may be able to manipulate parts of the e-Portfolio. For instance a teacher inputting the results of an examination.

The remote user may logon directly to the e-Portfolio or through a federated single sign-on (SSO) that will enable the remote user to be authenticated to another system but then be able to gain access to the e-Portfolio resources.

## 2.5 SOURCE PERSPECTIVE



### **2.5.1 Source Perspective Description**

Source data is defined as key information/data coming in to populate the e-Portfolio. Information/data coming in to the e-Portfolio needs to comply with the appropriate access control mechanisms.

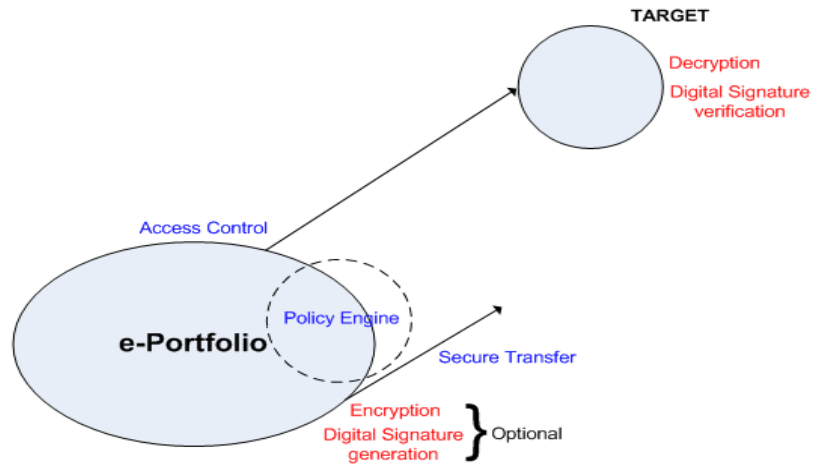
Optionally source data will need to be encrypted so that in certain use cases and environments the information cannot be easily understood by unauthorised users while either resident in the e-Portfolio or whilst in transit.

In certain situations the incoming data will need to be verified as to the integrity and authenticity of the information. Also digital signatures may need to be verified to provide necessary authentication of the data if non-repudiation is important.

An option within the source perspective model is to implement a sophisticated access control model, which allows a system to support a generic policy engine, one that supports much more than access control decisions. For instance additional policies could be enforced concerning import and export of data. The following policies could be enforced:

- All attainment certificates received from awarding bodies must have their digital signatures verified and the certificate must be from an approved awarding body;
- All extracts of a particular type sent to a given recipient must be encrypted (or digitally signed).

## 2.6 TARGET PERSPECTIVE



### **2.6.1 Target Perspective Description**

The target is defined as the external system or resource where e-Portfolio key information/data is transferred to. Information/data going out or transferring from the e-Portfolio needs to comply with the appropriate access control mechanisms.

Target data may need to be encrypted during the transfer. In situations where portions of the e-Portfolio are stored in an encrypted form then they may need to be decrypted so it is converted back into its original form prior to the transfer.

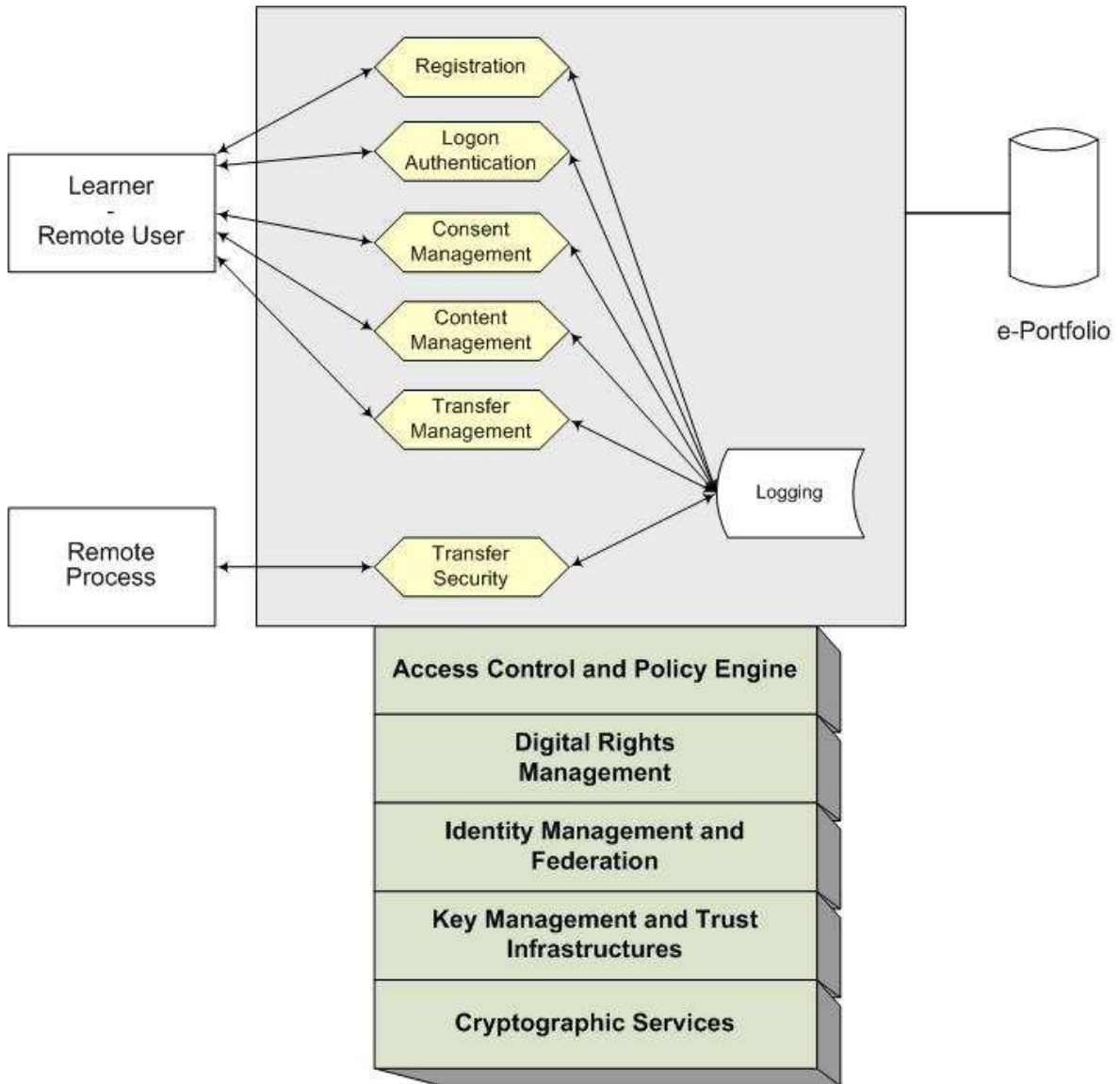
Digital signatures could be applied on the data being transferred so that the target can verify the information to ensure correct authentication and integrity of information/data.

As with the Source Perspective the system could support an access control model that implements a set of e-Portfolios policies on the import and export of data.

### 3. SECURITY FUNCTIONS, SERVICES & MECHANISMS

#### 3.1 SYSTEM SECURITY MODEL

In order to describe the security requirements and architectural components of an e-Portfolio system we have developed a System Security Model. This is shown in the diagram below.



On the left-hand side of the diagram are the external entities interacting with the e-Portfolio system, namely the learner, a remote user and an external process. The learner and the remote user directly interact with the system, whilst the remote process is representing process to process interactions (e.g. web services).

We have separated out security functions and services from security mechanisms and infrastructure components. In general the security functions represent those system elements that the external entities interact with (including the learner). The security mechanisms and infrastructure components support the security functions.

The following two sections describe each component. For each component we describe the candidate technologies and solutions as well providing relevant recommendations.

## **3.2 SECURITY FUNCTIONS AND SERVICES**

We have identified the following common security functions and services within the scope of e-Portfolio. They are as follows:

- Registration;
- Logon Authentication;
- Consent Management;
- Content Management;
- Transfer Management;
- Transfer Security;
- Logging.

Each of these services is now described in the following sections.

### **3.2.1 Registration**

In the DfES environment registration primarily concerns the recording of biographical details of an individual as well as appropriate verification that the person for whom claims to hold that identity actually does so. The DfES are working on an Identity Management strategy that requires the creation of a core biographical record, as well as a public facing identifier - the Unique Learner Number (ULN). The DfES Identity Management infrastructure is discussed more in the Identity Management and Federation section later in the report.

In the short and medium term it is likely that a learner being registered for an e-Portfolio will not be tied into any overall identity management infrastructure across the sector. A learner will be initially registered for an e-Portfolio on entering a learning provider. A system administrator in the learning provider will create an e-Portfolio with a minimal set of information, such as name, identifier and logon details. It is likely that the e-Portfolio would also be set up with other content, such as course schedules.

Longer term e-Portfolios could be set up for learners as soon as they enter the education system. Obviously very young children would not have the skills to manage their own e-Portfolio, in which case teachers may need to manage them on their behalf. At some point the learner will have sufficient skills and maturity to manage their e-Portfolio. Two models of use can be envisaged:

- Creation of an e-Portfolio account as soon as a learner is registered into the education system. Initially the account will be dormant until required;
- The e-Portfolio is not created until required and the learner has sufficient skills and is mature enough to use the e-Portfolio system.

## Candidate Technologies and Existing Infrastructure

The registration facility of e-Portfolios should be aligned with the emerging Identity Management infrastructure of DfES. It is likely that MIAP will play a major role in the infrastructure and hence the Learner Registration System (LRS) of MIAP, when deployed, could be a very good starting point for an e-Portfolio registration facility. MIAP will be available for post 14 learners.

If biometrics are considered a requirement for accessing e-Portfolio systems then during the registration process they must be captured. As currently it is not envisaged that the DfES Identity Management encompasses biometrics then e-Portfolio systems will need to accommodate this facility. Note that use of biometrics could depend on the role of the person. For instance only learners could be required to use biometrics.

When a registration occurs it is likely that this could trigger the creation of a number of accounts. In identity management parlance this is usually referred to as **provisioning**. To have a truly e-Portfolio meta-system requires that standard methods are defining for provisioning accounts.

One such standard is called Service Provisioning Markup Language (SPML). SPML has been defined by OASIS (the same standards organisation which has defined SAML, the basis for Shibboleth). Use of SPML should be considered further.

### Recommendations

**Recommendation (1):** The use of LRS of MIAP as the registration engine of e-Portfolios should be examined.

**Recommendation (2):** Research should be undertaken to determine appropriate skills and age required for a learner to take ownership of their own e-Portfolio.

**Recommendation (3):** Use of Service Provisioning Markup Language (SPML) should be considered further as a service provisioning standard. If SPML is of use to DfES then an education sector SPML profile will need to be produced.

### 3.2.2 Logon Authentication

Learners will be provided with logon credentials in order to access their e-Portfolio. This could be directly or via a federation connection using a technology such as Shibboleth. For more information about federation refer to the Identity Management and Federation section.

To ensure that the Logon Authentication is secure a minimum set of standards need to be applied to any e-Portfolio. The following areas need to be covered:

- Password complexity;
- Privacy of logon interaction (e.g. use of SSL);
- Use of two factor, or even three factor authentication. For instance use of hardware tokens and biometrics;
- Desktop security and use of Java, JavaScript etc.

The access control and policy engine mechanisms could be used to enforce authentication policies. For instance a policy could be defined that all learners accessing their accounts outside the perimeter of a learning provider need to use two factor authentication (or SSL).

Deployment of two factor authentication using hardware tokens can be expensive. An alternative method is to use the Short Message Service (SMS) provided by the mobile telephone operators. When a user wishes to access an e-Portfolio they will enter their logon identifier and optionally a local password, then a SMS message is sent to their mobile requesting they enter a password into their mobile. The authentication component will then authenticate the user supplied SMS password.

### **Candidate Technologies and Existing Infrastructure**

There are 4 technologies and infrastructure that exist, or should be rolled out in the next few years, that are of potential interest.

- Government Connect: This will permit citizens to access local and central government resources via an infrastructure provided by Local Authorities;
- Government Gateway: A registration and authentication infrastructure managed by the Cabinet Office. It supports a number of applications; including HMRC self assessment and DWP's pension forecast service;
- ID Cards: This will enable UK citizens that are over 16, and who are in possession of an ID card, to be authenticated to gain access to services;
- SMS from Mobile Operators.

The DfES Identity Management strategy and follow on work is examining the potential use of Government Connect, Government Gateway and ID Cards.

### **Recommendations**

**Recommendation (4):** A minimum set of security standards for authentication needs to be defined for the sector. These should be based on a combination of the Cabinet Offices Information Assurance framework and CESG standards.

**Recommendation (5):** Use of SMS as a two factor authentication mechanism should be considered further.

#### **3.2.3 Consent Management**

Consent Management allows data owners to control who can access and share what information within an e-Portfolio. It builds upon the access control mechanism to encompass controls on the access and sharing of data. Consent Management would hook into the policy engine as well as the access control engine. It would be able for a learner, and other data owners, to control:

- Who can access what information within the e-Portfolio, e.g. "pull" information;
- What information can be provided to what recipient, e.g. "pushed."

When an e-Portfolio account is created the various data owners will be defined. The primary data owner will be the learner. The data owner will be able to define the access permissions interims of both roles and individual identities.

### **Candidate Technologies and Existing Infrastructure**

There have been a number of pilot and prototype consent management “hubs” that have been deployed. However there are no standards in this area.

### **Recommendations**

**Recommendation (6):** Research should be undertaken to understand the requirements for consent within an e-Portfolio. In particular what content does each of the data owners “own” and what consent is required for different type of data. In effect a data model needs to be produced, one that is consistent with the access control and policy engine described later in the report.

#### **3.2.4 Content Management**

Content management covers the majority of an e-Portfolio set of functions and is the facility by which the learner and external users add and read content. What they can do in is controlled by the access control and policy engine mechanism.

The key requirement for this function is to interact seamlessly with the underlying access control and policy engine. As explained later in the report the requirements for the engine are unique to the education sector, hence it does seem sensible to build a reusable component that can be called from a number of environments.

Another requirement is the optional encryption/decryption of data stored within an e-Portfolio. Adding data into or extracting data out of encrypted portions of an e-Portfolio will require the content management component to be able encrypt/decrypt data on the fly.

### **Candidate Technologies and Existing Infrastructure**

The methods by which a “standard” access control and policy engine module may be invoked are as follows (note this list not exhaustive but does include those that are in wide spread use):

- Web Server plug-in: The primary web servers in the market place all have mechanisms by which authentication and authorisation modules can be invoked when accessing web resources. Of note all Apache modules for the Apache web Server; ISAPI for Microsoft IIS and NSAPI for the Sun/iPlanet web server;
- Java Authorisation Contract for Containers (JACC): A Java standard API that permits Java J2EE application servers and servlet containers to invoke authorisation services. All the main application servers and servlet containers in the market place support JACC. This would allow any Java application based on top of a J2EE application server to be governed by the access control and policy engine;
- The AzMan within Microsoft ASP.NET enables role based access control to be enforced within the ASP environment.

There are a number of encapsulation standards for encrypting data whilst stored on a disk. The chosen method will depend on how an e-Portfolio is stored, for example whether it is XML or a relational database.

If it is XML based then the xmlenc standard defined by W3C could be used (see later).

### **Recommendations**

**Recommendation (7):** In conjunction with the development of a DfES access control model it is recommended that research takes place to ensure that the primary API and plug-in technologies in the market place can be used to implement access to an access control and policy engine.

### **3.2.5 Transfer Management**

Transfer management allows the learner and a remote user to directly upload or download information and content.

Transferring of information may require the use of cryptography to ensure safe delivery of the content and ensure it's originated from a known source.

### **Candidate Technologies and Existing Infrastructure**

Please refer to transfer security.

### **Recommendations**

Please refer to transfer security.

### **3.2.6 Transfer Security**

This security function enables one or more of the following:

- The confidentiality of data to be maintained when being transferred or relayed between the originator and recipient;
- Validation of the integrity of the data, such that any modification of the data can be detected;
- Authenticity of the origination of the data, such that you can be confident as to the identity of the originator of the data;
- Non-repudiation between the two communicating parties. Non-repudiation can take many forms but in this context would normally mean the originator can not repudiate that they did not originate the message.

This security function will extensively call up the services of key management and trust infrastructure services as well as the cryptographic services.

Note that transfer security needs to be able to support multiple recipients, that is some content could be sent to a number of individuals and/or organisations.

As previously described, transfer security can also leverage the access control and policy engine to determine appropriate use of transfer security functions.

## Candidate Technologies and Existing Infrastructure

There are a large number of transfer security protocols that could be used, they fall broadly into three camps those that use traditional messaging service (such as S/mime), those that are XML based and finally those that are concerned with only connection security. Those that are widely used are described below:

- S/MIME: A secure messaging standard primarily used for electronic mail. Based on the Cryptographic Message Syntax (CMS). Secure email in products such as Microsoft's Outlook use S/MIME. It is also possible to use CMS as a general encapsulation protocol;
- Xmldsig and xmlenc: Two standards developed by W3C that enable the digital signing and optional encryption of an XML document;
- Web Services Security (WSS). An OASIS standard which builds upon W3C's xmldsig and xmlenc permitting secure web services. WSS also allows identity information to be transported in the form of tokens. Tokens supported include usernames/passwords, SAML assertions, Kerberos tickets as well as X.509 certificates;
- Transport Layer Security (TLS)/Secure Sockets Layer (SSL). Widely used by browser but can be used in other environments. Enable a secure pipe to be formed providing connection confidentiality and integrity. Also enables one-way or mutual authentication. Does not offer non-repudiation services and is more limited in functionality than the previously described protocols.

Whilst transfer security functionality could be embedded into e-Portfolio applications another approach is also viable, possibly as an intermediate step. This is to use an XML security gateway from a supplier such as Vordel or IBM/DataPower. XML security gateways add or (or strip) the XML security protocol from messages. They can also integrate with the secure infrastructure of the end systems.

## Recommendations

**Recommendation (8):** The techniques for uploading and downloading data securely into an e-Portfolio should be investigated. In particular once the techniques are agreed then standard profiles should be defined in order to maximise interoperability.

### 3.2.7 Logging

A generic logging service for the e-Portfolio system should be defined. The logging service should have the following characteristics:

- Ability to log all access of data and the changes of access permissions;
- A secure time stamping service so that accurate and secure time stamping of audit record can be achieved;
- Logging activity to support security, non-repudiation and Digital Rights Management functions;
- Ability to query and search through log files, including across organisational boundaries (potentially by using a consolidation service).

## **Candidate Technologies and Existing Infrastructure**

This area is not known for having standards. The only one of note is a technology called log4j. It is widely used in the Java environment and is now supported by the Apache Software Foundation. There is also log4c which is a port of log4j for a C environment.

## **Recommendations**

***Recommendation (9)***: A standard needs to be developed that defines minimum logging and audit standards. The standard needs to define those events that need to be recorded and the information collected.

### 3.3 INFRASTRUCTURE AND SECURITY MECHANISMS

We have identified the following infrastructure and security mechanisms within scope of e-Portfolios. They are:

- Access Control and Policy Engine;
- Digital Rights Management (DRM);
- Identity Management and Federation;
- Key Management and Trust Infrastructures;
- Cryptographic Services.

#### 3.3.1 Access Control and Policy Engine

There are a number of different forms of access control models in use across a wide range of applications, products and sectors. It is likely that none of them will exactly fit an e-Portfolio access control model. In summary the primary models that exist are described below, together with a description of their relevance to e-Portfolios.

##### ***Discretionary Access Control (DAC)***

Has the concept that every resource/file has an owner, and the owner can grant access permissions to the resource. A super user (administrator) can override the permissions if required. The owner grants permissions based on groups and the rest of the world. The permissions tend to be fixed, for instance “read”, “write” “execute” etc. The DAC model is implemented in many operating systems including UNIX/Linux and MS Windows. DAC allows the owner to be in control of who can access their resource; however it is rather rigid in its design and does not provide the richness of facilities that e-Portfolios require.

##### ***Access Control Lists (ACL)***

ACLs take DAC to the next level in sophistication with most current derivatives of UNIX supporting this facility. ACLs still have a concept of the owner managing access to objects they own. However in this model the owner can add additional users and groups, therefore forming a list of users/groups and their access permissions to a resource.

##### ***Mandatory Access Control (MAC)***

Has limited use in military circles and is designed to work in a multi level classification environment, e.g. RESTRICTED, SECRET. Users are highly constrained on what they can do. Administrators define maximum clearance levels of users. MAC is not appropriate for use on the e-Portfolio environment.

##### ***Role Based Access Control (RBAC)***

The “standard” model implemented by web access management products. The US standards organisation NIST published the RBAC model a few years ago. Although it has many advanced aspects, fundamentally it consists of the following:

- **Users:** A set of users: Users are assigned one or more roles;
- **Roles:** A set of roles: Typically a role is a job function that defines a user's responsibilities and authority within the organisation. A role is assigned a set of permissions;
- **Objects:** Objects are the resources, such as files, web pages or even transactions that are to be protected such that you require a particular permission to access it or perform a given operation;
- **Operations:** An operation is a function performed on an object. For file systems this could be "read" or "write", for transactional systems this could be "transfer file";
- **Permissions:** Permissions are an approval to perform a given operation on one or more RBAC-protected objects.

The NIST model permits advanced features including supporting hierarchical role structures and cardinality.

Whilst RBAC has many features that an e-Portfolio access control model requires, it does have one major weakness. Unfortunately all the management is performed by the administrators. They create the roles; assign roles to the users as well as the permissions allocated to the roles. In a learner centric e-Portfolio system the learner should be able to manage most of the access control system.

### ***Policy Based Access Control (PBAC)***

Policy Based Access Control (PBAC), or sometimes referred to as Rules Based Access Control, can be considered to be a super-set of RBAC. It supports a far richer set of access control operations. A typical PBAC implementation has the following characteristic:

- Rather than just roles, PBAC uses attributes. A role is just a special type of attribute. Attributes can be of various types:
  - User Attributes that are set upon a start of a session, for instance role, group membership;
  - Environment Attributes (for example, SSL connection strength);
  - Application "evidence" that can be used in the policies/rules, potentially of a dynamic nature.
- Operations are now defined as a combination of policy and rules. Both policies and rules are combinatorial and they can be dynamic and not just pertain to user attributes, such as roles. Combinatorial logic permit the use of Boolean algebra and hence a rule for exporting a resume could be defined as the following:

*isStudent AND isOwner AND isObjectResume*

This rule says that only a student who is the owner of the file, which has to be a resume, can be exported.

- Policy enforcement can be based on application attributes, potentially of a dynamic nature. For instance UCAS points, course results etc could be used as a basis of enforcing rules.

Implementing Policy Based access Control (PBAC) allows a system to support a generic policy engine, one that supports more than access control decisions. For instance additional policies could be enforced concerning import and export of data. As examples one could enforce the following policies:

- All attainment certificates received from awarding bodies must have their digital signatures verified AND the certificate must be from an approved awarding body;
- All extracts of a particular type send to a given recipient must be encrypted (or digitally signed).

None of the above models satisfy the requirements for a rich-portfolio access control model that can be used in multiple environments. However an e-Portfolio access model does need to support aspects of the above models. In particular note the following characteristics required of the e-Portfolio access control model:

- The primary owner of the e-Portfolio is the learner; the owner grants or rescinds permissions;
- Multiple owners of data must be supported;
- A defined set of roles are required, learner, assessor, teacher etc.
- A define set of permissions will need to be defined. These will be more than just read, write. To support a policy engine these permissions will need to include import, export and perhaps “sign” (see later);
- Certain roles may be able to manipulate parts of the e-Portfolio. For instance a teacher adding in the results of an examination;
- Different data sets within the e-Portfolio may need different access permissions. For instance, the learning provider may always be able to read and update the calendar.

### **Candidate Technologies and Existing Infrastructure**

None exist to support a rich and powerful education access control and policy engine. The closest set of products that support such a model are web access management products, such as CA's SiteMinder, RSA/EMC's ClearTrust, Sun's Access Manager and Oracle's NetPoint.

However there is one standard that may be appropriate, and that is the OASIS eXtensible Access Control Markup Language (XACML). XACML is a platform independent standard based access control policy specification language. It defines rules on how authorisation decisions from evaluating applicable access control policies are combined. A RBAC profile has been defined. Many of the web access management and application server vendors support XACML.

## Recommendations

**Recommendation (10):** It is recommended that a generic e-Portfolio access control model is developed and that all implementations conform to this model.

**Recommendation (11):** In addition it is recommended that a prototype of the model is developed and tested out in a pilot. This work should also examine whether the rules and policy engines of web access management products could be enhanced to accommodate the education sector requirements. As part of this work the potential use of XACML as an authorisation specification language for the access control model should be examined.

**Recommendation (12):** When developing an e-Portfolio access control model its use as a generic policy engine should also be examined. In particular the work should examine the use cases where policy could be applied, and the types of policy that could be enforced.

**Recommendation (13):** The attributes currently defined for Shibboleth (e.g. eduPersonScopedAffiliation, eduPersonPrincipalName etc.) should be examined to ensure they are sufficient to support the defined e-Portfolio access control model across the whole of the education sector covering both HE/FE and schools.

### 3.3.2 Digital Rights Management (DRM)

Digital Rights Management (generally abbreviated to DRM) is an umbrella term that refers to any of several technologies used by publishers or copyright owners to control access to and usage of digital data or hardware, and to restrictions associated with a specific instance of a digital work or device.

Enterprise Digital Rights Management (E-DRM or ERM) refers to the use of DRM technology to control access to corporate documents (Microsoft Word, PDF, TIFF, AutoCAD files, etc) rather than consumer playable media. The technology usually requires a Policy Server to authenticate users' rights to access certain documents but more recently software that does not require this has been created.

EDRM vendors include Microsoft, Adobe Systems, EMC Corporation and several smaller companies. There are open source implementations as well. EDRM is generally intended to apply to trade secrets, which are different from copyrighted material (though there is sometimes an overlap as some material is both copyrighted and a trade secret - e.g., the source code for some proprietary software) and for whom the primary issue is industrial or corporate espionage or inadvertent release.

DRM/E-DRM is relevant to e-Portfolios in two contexts:

- Allowing a learner to safely and responsibly upload into their e-Portfolio content that is either copy-righted and/or licensed;
- Developing new content within their e-Portfolio and to enable copyrighting and licensing to occur.

DRM and E-DRM usually use encryption technology to control access to the data. Ideally the key management services and policy engine used by other services should be used by DRM as well. It would be inefficient for the DRM service to use a completely separate key management and trust infrastructure.

## Candidate Technologies and Existing Infrastructure

There are a wide range of technologies used in DRM and E-DRM, some based on standards other are highly proprietary (e.g. Apple's FairPlay DRM system used in iTunes).

### Recommendations

**Recommendation (14):** A clear understanding of the role of DRM within the e-Portfolio environment must be established. The use of DRM will then drive the security services and mechanisms required and appropriate standards. This is a very large and complicated area and will take a great deal of research to determine both the requirements and a solution that can be applied sector wide.

### 3.3.3 Identity Management and Federation

Security and privacy of the contents of an e-Portfolio is of paramount importance as well as a third-party having trust in achievements and attainments recorded within it. All these are dependent on having a fit for purpose identity management infrastructure across the education sector. Many security services such as access control/authorisation, confidentiality, integrity and non-repudiation are dependent on having a trusted identity. Areas that are of importance for e-Portfolios are as follows:

- The strength of identity authentication when registering learners. Less important when they are young, but of increasing importance as financial considerations come into play;
- Having a unique and consistent identifier for each learner;
- Supporting single sign-on across a federation of organisations so that a learner (and remote users) can seamlessly and securely access a range of applications and resources, not just an e-Portfolio;
- Supporting identity federation in a web service environment, enabling identity information to be transported within services so access decision and logging can occur;
- Having a consistent set of standards in terms of login authentication and identity authentication.

## Candidate Technologies and Existing Infrastructure

MIAP has a registration facility which allocates unique identifiers (the ULN). ULNs are public facing and hence appropriate for use as an identifier in gaining access to an e-Portfolio. The DfES Identity Management strategy proposes wider use of MIAP and the ULN.

The use of Shibboleth as the e-Portfolio federation technology for HE/LE and schools seems a natural extension of its current use. Appendix A discusses the different federation models that are possible. Early deployments of Shibboleth only supported anonymous usage (using the transient pseudonym Identifier and attributes mode). For use in an e-Portfolio environment real identifiers and "account linking" will need to be supported.

## Recommendations

**Recommendation (15):** Future work on e-Portfolios and e-Portfolio security must be closely aligned with the DfES Identity management strategy and implementation.

### 3.3.4 Key Management and Trust Infrastructures

Key Management is a set of services that permit the lifecycle management of symmetric and asymmetric cryptographic keys. There are many forms of key management infrastructures; the most notable are Public Key Infrastructure (PKI) and Kerberos. Kerberos is used by Microsoft's Active Directory. Depending on the type of infrastructure key management supports the following services:

- Encryption/Decryption;
- Various forms of authentication (including logon authentication);
- Digital Signatures/Verification;
- Integrity Checking;
- Digital Rights Management;
- Inter-organisational trust infrastructures, such as used in SAML, Shibboleth and web services.

The first four of these services are described in the following cryptographic services section. Setting up a secure and scalable key management and trust infrastructure to support all the above services is a non-trivial matter. There are number of current and emerging technologies to choose from, each with their own set of challenges. For example Shibboleth supports a PKI trust infrastructure; however the granularity of trust is at the learning provider level. Enabling PKI at an individual level is several orders of magnitude more complicated.

### Candidate Technologies and Existing Infrastructure

Relevant Key Management technologies to examine include:

- Public Key Infrastructures using PKI;
- Kerberos;
- OASIS Enterprise Key Management Infrastructure (EKMI) currently being developed. A similar initiative is also being developed by IRTF called keyprov;
- XML Key management Specification (XKMS). Primarily supported by Verisign, it's a key management service designed to support XML based web service.

## Recommendations

**Recommendation (16):** A study needs to be sponsored to examine the key management requirements of e-Portfolios. This study should examine: scalability issues; the use of symmetric and asymmetric key technology and infrastructures; key/data recovery services; life-cycle management, distribution of root/trusted certificates and how key management supports other services such as DRM.

### 3.3.5 Cryptographic Services

Three type of cryptographic mechanism will be required, namely:

- Symmetric encryption/decryption: Used for encryption of data; generation of message authentication codes (MAC) and key distribution in the case of Kerberos;
- Asymmetric encryption/decryption: Used for key distribution and digital signatures;
- Hashing: Used for generating MACs and part of the process in generating digital signatures.

Digital Signature generation/verification relies on public key cryptography and hence a PKI trust infrastructure. Support will be required for two different types of digital signatures:

- Signing of discrete elements of data originated by a user (or a process on behalf of a user). The user being a learner, teacher, assessor etc;
- Signing of data by an organisation. For instance a recipient organisation verifying that a particular message was originated by another organisation.

Use of encryption will probably be an optional facility. Its use is many fold, and could include the following use cases:

- The more sensitive parts of the e-Portfolio could be encrypted, such that only the learner has the key to unlock that part of the e-Portfolio. The benefit of this approach is that if someone was to transfer the e-Portfolio to another system, only the learner could access it;
- If part of an e-Portfolio has potential for licensing then a Digital Rights Management (DRM) mechanism needs to be added in. DRM usually works by encrypting those portions of a file that requires access to be limited. (see the section on DRM);
- When transferring all or part of an e-Portfolio encryption could be applied to parts of it. Only the recipient, which could be the learner, will be able to open it.

Supporting encryption throughout a large distributed environment will be a challenge. Key management down to the granularity of a learner and teacher/assessor will require a large infrastructure. Learners losing their encryption/decryption keys should also be taken into account and hence key/data recovery mechanisms should be looked at.

## **Candidate Technologies and Existing Infrastructure**

There are many cryptographic standards to choose from, DfES need to define a consistent set across the sector.

### **Recommendations**

***Recommendation (17):*** To maximise interoperability DfES need to define a profile of cryptographic algorithms to be used across the sector. Algorithms need to be selected for public key cryptography, symmetric encryption/decryption, digital signing and hashing. Where relevant key lengths and modes of operation will need to be defined.

### **3.4 INTEROPERABILITY SECURITY REQUIREMENTS**

In order to meet user expectations, e-Portfolio management systems will need to interact with numerous diverse systems found at a typical institution of higher education. These may include course management systems, student information systems, authentication and authorisation systems and certification systems. e-Portfolio systems will need to exchange information about learners and other users, data the user has created, relationships between components of a portfolio, and information about the process of creating and using the portfolio.

Important interoperability considerations include:

- Access to information about users across systems;
- Access to data created by users across systems;
- Standardisation of data structures describing objects within a portfolio, the structure of e-Portfolio components, views of the portfolio, and the whole portfolio;
- Sharing common authentication and authorisation services with other systems;
- Mapping data between educational communities;
- Enforcing verifiability, non-revocability, and IP rights across systems;
- Managing workflow across systems.

#### **3.4.1 Access to information about users**

e-Portfolio systems will need access to learner's personal information (such as demographics, directory information and accessibility requirements), transcripts and other official records of educational progress. This information may be stored in student information systems, HR systems and other enterprise systems, some of which may be external to an institution.

#### **3.4.2 Access to data created by users**

e-Portfolio systems will need to be able to utilise content created within other learning systems, such as documents, reflections, links, feedback, views of a portfolio and complete portfolios. It is important that this information be passed in its entirety and that all significant internal structure is preserved.

#### **3.4.3 Standardisation of data structures**

In order for data to be meaningfully shared and represented across systems, the systems will need to support common data structures for each type of content. Elements of the structure of the portfolio itself need to be agreed upon and supported by interoperating systems to make full use of the data being shared.

#### **3.4.4 Common authentication and authorisation services**

There needs to be a consistent strategy for authenticating access to e-Portfolios and providing access control between different e-Portfolio systems. This enables the verification of a common identity across systems and maintains user defined access control to e-Portfolios and the content within them across systems.

#### **3.4.5 Mapping data between educational communities**

Different standards for representing learner information and portfolio content are accepted within different educational communities. It will be important to develop a standard way of mapping one standard to another in order to provide data integrity and usability.

#### **3.4.6 Verification and rights management**

In some cases, data within a portfolio may need to be verifiable with an external authority, such as a professional certification organisation. In addition, e-Portfolios may contain intellectual property, which belongs to the user, or one or more third parties, the rights to which need to be controlled. Information about these constraints and dependencies should be preserved as data is moved and systems should support the resolution of the constraints in a consistent way.

#### **3.4.7 Managing workflow**

The processes of creating, editing, sharing, evaluating and scoring portfolios may be performed using multiple applications and may be specified by someone other than the learner, such as in the context of a course. There should be a standard way to represent the workflow of these processes and mechanisms for applications to pass both the description of the process and messages about the status of individual portfolios within them.

## **4. USE CASE SCENARIOS**

---

### **4.1 INTRODUCTION**

A number of use cases have been developed defining different expressions of a service in order to define the over arching service definitions.

The following use case scenarios are intended to illustrate some of the many possible uses of e-Portfolios. These examples should contribute to an understanding of how e-Portfolios might be used and their potential benefit as well as appropriate security requirements taken into account.

Identified use case scenarios include:

- e-Portfolio creation;
- e-Portfolio management by the learner;
- Learner transfers to another learning provider (School, College, University etc);
- Learner applies to UCAS for university place;
- Learner applies to employer for job;
- University/learning provider views learners e-Portfolio;
- NAA/QCA/University uploads attainments to learners e-Portfolio (covers Learner Achievement Record from MIAP);
- Teacher/Lecturer views e-Portfolio;
- Learner changes modules/course within a learning provider;
- Learner applies to training provider.

#### **4.1.1 e-Portfolio creation**

This scenario covers the creation of a new e-Portfolio for a learner. The e-Portfolio management system offered by the learner's learning provider automatically and dynamically creates and maintains a personal portfolio site for each member of the institution based on the learner's user ID.

Public information, including e-mail address, and departmental links are available to the public in accordance with the Family Educational Rights and Privacy Act (FERPA).

The learner can quickly and easily create and update their personal portfolio site. They can add personal information such as contact numbers and home e-mail addresses and upload digital pictures. They can insert brief statements introducing themselves and describing their academic goals.

The learner's portfolio also includes sections for their CV and bookmarks, as well as a showcase to highlight accomplishments and a learning matrix that will be used to track and manage learning outcome requirements.

## Mapping to security functions and mechanisms

The table below clearly displays the mapping and usage between the specific use case scenario and the relevant security functions and services and infrastructure and security mechanisms.

Security Functions, Services & Mechanisms	Usage
<b>Security Functions &amp; Services</b>	
Registration	<ul style="list-style-type: none"><li>• Creation of e-Portfolio account</li><li>• Registering details</li></ul>
Logging	<ul style="list-style-type: none"><li>• Will log the registration</li><li>• Log that the user has logged in successfully</li><li>• Logged users permissions</li><li>• Will log unsuccessful attempts</li></ul>

### 4.1.2 e-Portfolio management by the learner

The scenario below explains how to increase personalisation of learning at age 14-19 through effective management of a learner's e-Portfolio.

The learning provider is given password access to the e-Portfolio. The learning provider selects appropriate teacher/mentor/advisors to register onto site.

Learner to register onto site, entering some personal details. Learner can also customise the way their part of site will be viewed. On registering, the learner creates a password protected space that others can only access with the learners permission. The learner can nominate certain parties to share selected information with e.g. tutor/mentor/advisor.

Once registered the learner begins the process of using the e-Portfolio where they record personal achievements, qualifications and work experience. The learner can choose to share selected work with their teacher. The teacher can then check student progress online and give feedback on the work they have done.

On completion of all of the steps, the information from the work summaries produced goes forward to produce an ILP (Individual Learning Plan) document. The ILP document can be shared and reviewed with the teacher at a later date and changes added to the original document, or a new document can be created.

All the information collected will be stored in a database ready to be amended the next time the learner uses the e-Portfolio.

## Mapping to security functions and mechanisms

The table below clearly displays the mapping and usage between the specific use case scenario and the relevant security functions and services and infrastructure and security mechanisms.

Security Functions, Services & Mechanisms	Usage
<b>Security Functions &amp; Services</b>	
Logon Authentication	<ul style="list-style-type: none"> <li>• Initialisation</li> </ul>
Consent Management	<ul style="list-style-type: none"> <li>• Defining appropriate access permissions for a set of users</li> </ul>
Content Management	<ul style="list-style-type: none"> <li>• Populating e-Portfolio with data</li> </ul>
Logging	<ul style="list-style-type: none"> <li>• Log that the user has logged in successfully</li> <li>• Logged users permissions</li> <li>• Will log unsuccessful attempts</li> </ul>
<b>Infrastructure &amp; Security Mechanisms</b>	
Access Control and Policy Engine	<ul style="list-style-type: none"> <li>• Checking the owner of the e-Portfolio</li> </ul>
Identity Management and Federation	<ul style="list-style-type: none"> <li>• Will the user be using a federated log-on identity?</li> </ul>
Key Management and Trust Infrastructures	<ul style="list-style-type: none"> <li>• Ensuring digital signatures generation/verification, integrity checking and PKI in use</li> </ul>

### 4.1.3 Learner transfers to another learning provider (School, College, University etc.)

As learners transfer from institution to institution during their educational careers, the ability to transport their e-Portfolios into new systems becomes increasingly important.

In this scenario, the learner transfers their course to another university. The learner transfers his/her courses to their chosen new university, which has a separate e-Portfolio system.

When the learner logs into the new e-Portfolio management system, they can import materials from a previous e-Portfolio, including profile information, coursework and personal files, CV, and Learning Matrix.

The learner is now ready to meet with his/her new academic advisor to review their academic program and determine which courses/modules he/she must pass to complete the requirements of the degree program at the new university.

## Mapping to security functions and mechanisms

The table below clearly displays the mapping and usage between the specific use case scenario and the relevant security functions and services and infrastructure and security mechanisms.

Security Functions, Services & Mechanisms	Usage
<b>Security Functions &amp; Services</b>	
Transfer Management	<ul style="list-style-type: none"> <li>Confidentiality of data to be maintained</li> <li>Ensuring integrity and authenticity of data</li> </ul>
Transfer Security	<ul style="list-style-type: none"> <li>Data needs to be transferred in a secure manner through the use of digital signatures and encryption</li> </ul>
Logging	<ul style="list-style-type: none"> <li>Logged users permissions and activities</li> <li>Data has been transferred and the target</li> </ul>
<b>Infrastructure &amp; Security Mechanisms</b>	
Access Control and Policy Engine	<ul style="list-style-type: none"> <li>Enforcing user has the appropriate rights to transfer data. Prompt that data can only be transferred if it is digitally signed and encrypted</li> </ul>
Key Management and Trust Infrastructures	<ul style="list-style-type: none"> <li>Ensuring digital signatures generation/verification, integrity checking and PKI in use</li> <li>To support cryptographic services</li> </ul>
Cryptographic Services	<ul style="list-style-type: none"> <li>Ensuring safe delivery of content and ensure it is originated from a known source</li> </ul>

### 4.1.4 Learner applies to UCAS for university place

UCAS is the central organisation that processes applications for full-time undergraduate courses at UK universities and colleges.

This scenario illustrates how the different materials for the different stages of the admissions service-flow link to one another. Some stages are well scoped and others are in development. There are also gaps that are being addressed.

As the learner enters college at 17, they have negotiated an Individual Learning Plan (ILP) with an advisor. The learner has used their e-Portfolio to help set themselves realistic but challenging goals, negotiate a plan and monitor progress. Application to Higher Education is an important theme throughout the plan.

Aged 18, the learner in their second term at college receives some results from a diagnostic assessment and prepares to meet and advisor to negotiate an extension to

their ILP. They review their performance using their learning e-Portfolio and provide the advisor with material for the meeting and negotiates the new ILP.

The learner will map themselves against the entry requirements of different courses by drafting some trial applications to Higher Education (UCAS). They then liaise with advisor on assessments of these applications.

The learner and referee are assisted by web services operating within an admissions service to complete a structured personal statement.

The following feedback of the use case scenario is relevant:

**Rejected application** - Failure to gain a place may well cause the learner to disengage. Formative feedback enables the applicant to learn from the experience and identify appropriate future opportunities.

**Accepted application** - The assessment of an application may reveal significant issues that the learner needs to address

**Feedback for institutions** - By aggregating the results of feedback to individuals, colleges may gain a better understanding of how their internal e-Portfolio-enabled processes may be enhanced.

**Mapping to security functions and mechanisms**

The table below clearly displays the mapping and usage between the specific use case scenario and the relevant security functions and services and infrastructure and security mechanisms.

Security Functions, Services & Mechanisms	Usage
<b>Security Functions &amp; Services</b>	
Content Management	<ul style="list-style-type: none"> <li>• Populating e-Portfolio with relevant data</li> </ul>
Transfer Management	<ul style="list-style-type: none"> <li>• Confidentiality of partial data to be maintained</li> <li>• Ensuring integrity and authenticity of partial data</li> </ul>
Transfer Security	<ul style="list-style-type: none"> <li>• Partial data needs to be transferred in a secure manner through the use of digital signatures and encryption</li> </ul>
Logging	<ul style="list-style-type: none"> <li>• Logged users permissions and activities</li> <li>• Logged UCAS application</li> </ul>
<b>Infrastructure &amp; Security Mechanisms</b>	
Access Control and Policy Engine	<ul style="list-style-type: none"> <li>• Enforcing user has the appropriate rights to transfer partial data. Prompt that partial data can only be transferred if it is digitally signed and encrypted</li> </ul>

Security Functions, Services & Mechanisms	Usage
Key Management and Trust Infrastructures	<ul style="list-style-type: none"> <li>• Ensuring digital signatures generation/verification, integrity checking and PKI in use</li> <li>• To support cryptographic services</li> </ul>
Cryptographic Services	<ul style="list-style-type: none"> <li>• Ensuring safe delivery of content and ensure it is originated from a known source</li> </ul>

#### 4.1.5 Learner applies to employer for job

The learner decides to apply for a job using the e-Portfolio system. The learner determines it is now time to create his/her CV and include links to relevant papers, projects and past work experiences.

The learner is able to build a CV to highlight personal information such as career objectives, education, work experience, and relevant references. This CV can then be made available to potential employers and other specific users.

The learner can use their e-Portfolio to create career portfolio profile packages, each optimised to offer supporting credentials corresponding to the requirements of a particular job.

The learner can then authorise potential employers to access restricted, employer specific material by entering a unique access code. Using that access code, the employer can review the various credentials and examples of work that the learner thought would strengthen their application for a particular position. The learner will then regularly check their site to review the access log to see if any potential employers have visited their career portfolio.

The learner may continuously update their CV and employment cover letters to suit various potential employers. A personal statement may also be written which is appropriate for an admissions committee.

## Mapping to security functions and mechanisms

The table below clearly displays the mapping and usage between the specific use case scenario and the relevant security functions and services and infrastructure and security mechanisms.

Security Functions, Services & Mechanisms	Usage
<b>Security Functions &amp; Services</b>	
Content Management	<ul style="list-style-type: none"> <li>• Populating e-Portfolio with relevant data</li> </ul>
Transfer Management	<ul style="list-style-type: none"> <li>• Confidentiality of data to be maintained</li> <li>• Ensuring integrity and authenticity of data</li> </ul>
Transfer Security	<ul style="list-style-type: none"> <li>• Data needs to be transferred in a secure manner through the use of digital signatures and encryption</li> </ul>
Logging	<ul style="list-style-type: none"> <li>• Logged users permissions and activities</li> <li>• Logged communication and transfer of data</li> </ul>
<b>Infrastructure &amp; Security Mechanisms</b>	
Access Control and Policy Engine	<ul style="list-style-type: none"> <li>• Enforcing user has the appropriate rights to add and edit content</li> </ul>
Digital Rights Management	<ul style="list-style-type: none"> <li>• Control access and usage of data</li> <li>• Allowing safe upload of e-Portfolio content that is either copyrighted and/or licensed</li> </ul>
Key Management and Trust Infrastructures	<ul style="list-style-type: none"> <li>• Ensuring digital signatures generation/verification, integrity checking and PKI in use</li> <li>• To support cryptographic services</li> </ul>
Cryptographic Services	<ul style="list-style-type: none"> <li>• Ensuring safe delivery of content and ensure it is originated from a known source</li> </ul>

#### 4.1.6 University/Learning Provider views learners e-Portfolio

This use case scenario is focused on how a lecturer/teacher can access and update the learner's e-Portfolio in order to provide feedback, add scores, marking and reviewing documents and calendar/schedule updates.

Benefits of this specific use case scenario include the following:

- Access to better advice;
- Enables an electronic dialogue with adviser;
- More ownership of the transition process;
- A smoother transition with greater continuity of learning;
- Allows learner to make sense of the range of disparate influences;
- Reduces the amount of time inputting information repeatedly;
- Ability to link back to adviser's;
- Advanced student data;
- Data should be more consistent.

#### Mapping to security functions and mechanisms

The table below clearly displays the mapping and usage between the specific use case scenario and the relevant security functions and services and infrastructure and security mechanisms.

Security Functions, Services & Mechanisms	Usage
<b>Security Functions &amp; Services</b>	
Logon Authentication	<ul style="list-style-type: none"> <li>• Initialisation for remote users</li> </ul>
Consent Management	<ul style="list-style-type: none"> <li>• Learner will want to explicitly allow teacher/lecturer to gain access to e-Portfolio and perform specific functions</li> <li>• Updating access permissions for a set of users</li> </ul>
Content Management	<ul style="list-style-type: none"> <li>• Responsibilities and permissions for teacher/lecturer assigned by learner</li> </ul>
Logging	<ul style="list-style-type: none"> <li>• Log that the user has logged in successfully</li> <li>• Logged users permissions</li> <li>• Will log unsuccessful attempts</li> </ul>

Security Functions, Services & Mechanisms	Usage
<b>Infrastructure &amp; Security Mechanisms</b>	
Identity Management and Federation	<ul style="list-style-type: none"> <li>Remote user can log in through a federated channel via federated logon</li> </ul>

#### 4.1.7 NAA/QCA/University uploads attainments to learners e-Portfolio (covers Learner Achievement Record from MIAP)

An e-Portfolio linked to external assessment systems would provide colleges with automatic verification. This would require the application including the learner's unique learner number (ULN).

Attainment authorities may upload/transfer files to a learner's e-Portfolio as evidence of learning achievement and competency.

Once submitted to a learner's e-Portfolio, this accreditation information is readily accessible as a means of providing documentary evidence to additional educational institutions and potential employers.

#### Mapping to security functions and mechanisms

The table below clearly displays the mapping and usage between the specific use case scenario and the relevant security functions and services and infrastructure and security mechanisms.

Security Functions, Services & Mechanisms	Usage
<b>Security Functions &amp; Services</b>	
Transfer Management	<ul style="list-style-type: none"> <li>Confidentiality of data to be maintained</li> <li>Ensuring integrity and authenticity of data</li> </ul>
Transfer Security	<ul style="list-style-type: none"> <li>Data needs to be transferred and uploaded in a secure manner through the use of digital signatures and encryption</li> <li>Data transferred inbound to the e-Portfolio</li> </ul>
Logging	<ul style="list-style-type: none"> <li>Logged users permissions and activities</li> <li>Log import of data and from which source</li> </ul>
<b>Infrastructure &amp; Security Mechanisms</b>	
Access Control and Policy Engine	<ul style="list-style-type: none"> <li>Enforcing user has the appropriate rights to transfer and upload data. Prompt that partial data can only be transferred if it is digitally signed and encrypted</li> </ul>

Security Functions, Services & Mechanisms	Usage
Key Management and Trust Infrastructures	<ul style="list-style-type: none"> <li>• Ensuring digital signatures generation/verification, integrity checking and PKI in use</li> <li>• To support cryptographic services</li> </ul>
Cryptographic Services	<ul style="list-style-type: none"> <li>• Ensuring safe delivery of content and ensure it is originated from a known source</li> </ul>

#### 4.1.8 Teacher/Lecturer views e-Portfolio

The teacher/lecturer has the ability to log into the learner's e-Portfolio management system once invited by the learner to conduct some example activities as described below:

- Authorise substitutions for required courses in learner's learning matrix;
- Review learner's learning outcomes to verify that his/her academic advancement is in accordance with institutional guidelines.

Additional tasks/activities that a teacher/lecturer may undertake include the following:

- Build on student interests and motivation;
- Increase the information retention of their students;
- Review coursework more efficiently;
- Provide developmental feedback and assessment to students;
- Offer better informed career advice to students.

A teacher/lecturer can support collation of school's progression data and allow schools to make iterative judgements on their procedures for supporting applications. The teacher, lecturer or tutor can then begin to populate curriculum systems for forthcoming academic years.

The teacher/lecturer can also use specific e-Portfolio tools to post messages and provide feedback on a learner's portfolio.

This scenario is similar to *4.1.6 - University/Learning Provider views learners' e-Portfolio*. The only differences being the use of access control as a security mechanism and assigning a different set of user permissions.

As an example, a department at a University would have access to update learners' calendars and schedules, although an individual (teacher/lecturer) would not have this access.

## Mapping to security functions and mechanisms

The table below clearly displays the mapping and usage between the specific use case scenario and the relevant security functions and services and infrastructure and security mechanisms.

Security Functions, Services & Mechanisms	Usage
<b>Security Functions &amp; Services</b>	
Logon Authentication	<ul style="list-style-type: none"> <li>• Initialisation for remote users</li> </ul>
Consent Management	<ul style="list-style-type: none"> <li>• Learner will want to explicitly allow teacher/lecturer to gain access to e-Portfolio and perform specific functions</li> <li>• Updating access permissions for individual users</li> </ul>
Content Management	<ul style="list-style-type: none"> <li>• Responsibilities and permissions for teacher/lecturer assigned by learner</li> </ul>
Logging	<ul style="list-style-type: none"> <li>• Log that the user has logged in successfully</li> <li>• Logged users permissions</li> <li>• Will log unsuccessful attempts</li> </ul>
<b>Infrastructure &amp; Security Mechanisms</b>	
Access Control and Policy Engine	<ul style="list-style-type: none"> <li>• Enforcing user has the appropriate rights to transfer and view data. Prompt that data can only be transferred if it is digitally signed and encrypted</li> </ul>
Identity Management and Federation	<ul style="list-style-type: none"> <li>• Remote user can log in through a federated channel via federated logon</li> </ul>

### 4.1.9 Learner changes modules/course within a learning provider

The learner arranges a meeting with the academic advisor/lecturer to review progress and work and ensure he/she is progressing effectively. During this consultation with the academic advisor/lecturer, they both agree that a new course selection could better meet the student's learning requirements and career objectives.

The academic advisor/lecturer will provide the necessary guidance and information on new module/course content whilst ensuring the Learner Achievement Record is updated.

## Mapping to security functions and mechanisms

The table below clearly displays the mapping and usage between the specific use case scenario and the relevant security functions and services and infrastructure and security mechanisms.

Security Functions, Services & Mechanisms	Usage
<b>Security Functions &amp; Services</b>	
Logon Authentication	<ul style="list-style-type: none"> <li>• Initialisation for remote users</li> </ul>
Consent Management	<ul style="list-style-type: none"> <li>• Learner will want to explicitly allow teacher/lecturer to gain access to e-Portfolio and perform specific functions</li> <li>• Updating access permissions for a set of users</li> </ul>
Content Management	<ul style="list-style-type: none"> <li>• Responsibilities and permissions for teacher/lecturer assigned by learner</li> </ul>
Logging	<ul style="list-style-type: none"> <li>• Log that the user has logged in successfully</li> <li>• Logged users permissions</li> <li>• Will log unsuccessful attempts</li> </ul>
<b>Infrastructure &amp; Security Mechanisms</b>	
Identity Management and Federation	<ul style="list-style-type: none"> <li>• Remote user can log in through a federated channel via federated logon</li> </ul>

### 4.1.10 Learner applies to training provider

The learner will be 'triggered' to apply to a training provider. The learner will share this decision with his/her adviser. The application will be completed with previous data being edited. The learner will send this onto a tutor or adviser who will add suggestions and then send it back to them.

The training provider will receive the application electronically. The training provider will acknowledge the application and ensure its progress can be monitored. The learner will be called to interview and present a range of 'softer data'.

The LA (Local Authority) training network will use some of the hard data to populate their administrative systems. The training provider will populate their own IM systems with all the received data and share some information with other relevant colleagues.

Learners will be able to forward further data to providers in preparation for induction. Training providers will verify learner's qualifications via UPN to the LA (Local Authority). Training providers will provide feedback data to schools on student's progression. Schools will use this data to inform their own processes and support their progression targets.

## Mapping to security functions and mechanisms

The table below clearly displays the mapping and usage between the specific use case scenario and the relevant security functions and services and infrastructure and security mechanisms.

Security Functions, Services & Mechanisms	Usage
<b>Security Functions &amp; Services</b>	
Content Management	<ul style="list-style-type: none"> <li>• Populating e-Portfolio with relevant partial data</li> </ul>
Transfer Management	<ul style="list-style-type: none"> <li>• Confidentiality of data to be maintained</li> <li>• Ensuring integrity and authenticity of partial data</li> </ul>
Transfer Security	<ul style="list-style-type: none"> <li>• Partial data needs to be transferred in a secure manner through the use of digital signatures and encryption</li> </ul>
Logging	<ul style="list-style-type: none"> <li>• Logged users permissions and activities</li> <li>• Logs application to training provider</li> </ul>
<b>Infrastructure &amp; Security Mechanisms</b>	
Access Control and Policy Engine	<ul style="list-style-type: none"> <li>• Enforcing user has the appropriate rights to transfer partial data. Prompt that partial data can only be transferred if it is digitally signed and encrypted</li> </ul>
Key Management and Trust Infrastructures	<ul style="list-style-type: none"> <li>• Ensuring digital signatures generation/verification, integrity checking and PKI in use</li> <li>• To support cryptographic services</li> </ul>
Cryptographic Services	<ul style="list-style-type: none"> <li>• Ensuring safe delivery of content and ensure it is originated from a known source</li> </ul>

## 5. OTHER RECOMMENDATIONS

---

### 5.1 SECURITY AND PRIVACY

The author of an e-Portfolio controls the content and access mechanisms. This brings about additional concerns issues regarding security and privacy.

**Recommendation (18):** BECTA needs to determine range of policies to be implemented for governing information access, security and privacy and how they will be determined and controlled.

**Recommendation (19):** BECTA to perform a study on how appropriate access permissions will be extended to include potential employers who are not known to specific learning providers.

### 5.2 INTELLECTUAL PROPERTY AND DIGITAL RIGHTS

Intellectual property management is becoming an increasing concern and e-Portfolios will bring new challenges to a number of learning providers. There is certainly a distinct lack of protection in the intellectual property rights of learners.

**Recommendation (20):** BECTA needs to determine who is the assigned owner of items uploaded into an e-Portfolio (learner, learning provider, or a combination) and examine the mechanisms in place for resolving ownership issues.

**Recommendation (21):** BECTA to kick off a study on how learning providers inform learners of the rights of authors and publishers to documents stored in e-Portfolios.

**Recommendation (22):** BECTA to examine how an e-Portfolio system can provide evidence and guarantees that the owner of the e-Portfolio created the work.

### 5.3 DATA PROTECTION

Data protection is an area that needs to be explored in further detail.

**Recommendation (23):** BECTA to issue guidance on agreement between learning providers as to what information should be transferred between e-Portfolios and systems. This includes checking data protection and data ownership regulations.

**Recommendation (24):** Infrastructure and security mechanisms need to acknowledge data quality, data assets, data ownership and data rights to access the e-Portfolio.

### 5.4 USE CASE SCENARIOS

**Recommendation (25):** BECTA to investigate inclusion of additional use case scenario around lifelong learning focusing on the full learning lifecycle. A lifelong learning e-Portfolio refers to an e-Portfolio that promises access and maintenance beyond graduation. Building a lifelong e-Portfolio promotes additional incentives for learners to create and maintain their e-Portfolios. Maintaining an e-Portfolio beyond the college and university years can have long-term personal and professional benefits, supporting both formal and informal lifelong learning.

**Recommendation (26):** Each use case scenario needs to be analysed in more detail to include the relevant security functions and services that would apply for each individual scenario.

## APPENDIX A: FEDERATION TECHNIQUES

---

There are many different ways one can build an Identity Management meta system. This appendix, in a technology neutral manner, illustrates the many different ways one can link up different systems. Before examining the different facets it is important to understand two key building blocks, they are:

- **Identity Provider (IdP)** The system, or administrative domain, that asserts information about a subject. For instance, the Identity Provider asserts that this user has been authenticated and has given associated attributes. For example: This user is John Doe, he has an email address of [jdoe@acompany.com](mailto:jdoe@acompany.com), and he was authenticated into this system using a password mechanism.
- **Service Provider (SP)** The system, or administrative domain, that relies on information supplied to it by the Identity Provider. It is up to the Service Provider as to whether it trusts the assertions provided to it. There are a number of mechanisms that enable the Service Provider to trust the assertions provided to it. It should be noted that although a Service Provider can trust the provided assertions, local access policy defines whether the subject may access local resources. Therefore, although the Service Provider trusts that I'm John Doe - it doesn't mean I'm given carte blanche access to all resources. Service Providers are also known as Relying Parties - due to the fact that they "rely" on information provided by an Identity Provider

Historically many systems provided **both** the IdP and SP functionality. With the introduction of Federation technologies some systems now only perform one of the roles.

The following sections examine:

- **Topology:** Whether there are multiple Identity Providers or a single Centralised IdP.
- **Account Linking:** How accounts (or identity data) can be linked. If the individual has an account on the Identity Provider how does that account get linked to an account on the Service Provider?

Many of the account linking methods can be used independently of the selected topology.

### A.1 TOPOLOGY

#### A.1.1 Centralised Federation

Centralised federation is an environment where there is a single Identity Provider surrounded by a number of Service Providers. The identity provider stores account information, as well as potentially master bio-graphical information. Users and accounts will be registered directly onto the Identity Provider. When a user wishes to access a resource or application on one of the service providers they will be directed to the central identity provider to prove their identity.

#### A.1.2 Distributed Federation

A distributed federation consists of a number of peer Identity Providers. Typically there is no one master system of accounts.

## **A.2 ACCOUNT LINKING**

There are three methods by which “accounts” can be linked, in summary they are:

- Out-of-Band Linkage;
- Persistent Pseudonym Identifiers;
- Transient Pseudonym Identifiers and Attributes.

The following sections describe each of these methods in turn.

### **A.2.1 Out-of-Band Linkage**

There are four different techniques by which accounts can be linked using out-of-band techniques. Out-of-band means that the federation protocol does not take part in the account linkage, and that other techniques are used. This usually means that any linking is achieved either by manual administrative steps or a separate system is used to lookup the mapping between accounts. The four techniques are described below:

#### *a. BOTH ACCOUNTS SHARE THE SAME IDENTIFIER*

Both the Identity Provider and the Service Provider share the same identifier to reference the account. For example both systems will know John Doe as jdoe. A number of methods can be used to achieve this including:

- When an account is created on the Identity Provider an account of the same name is created on the Service Provider using a separate communication channel;
- Regular updates of accounts on the Identity Provider are transferred to the Service Provider, perhaps commencing with an initial bulk upload of the existing accounts.

#### *b. LINKING AT THE IDENTITY PROVIDER*

In this situation the Identity Provider maps their account identifier to the identifier used by the target Source Provider, for example John Doe is known as jdoe on the Identity Provider but johnd on the Service Provider. In this case the Identity Provider looks up jdoe to establish he is known as johnd on the other system and sends the assertion to the Service Provider concerning johnd. The mapping can be performed directly on the Identity Provider or on a separate system. The separate system sometimes is called a lookup service or a matching service, and can be implemented using either directories or databases.

#### *c. LINKING AT THE SERVICE PROVIDER*

Mapping occurs at the Service Provider, rather than at the Identity Provider as in the previous case. As before the mapping information could be stored on the Service Provider or using a lookup/matching service.

d. *MAPPING TO A NETWORK IDENTIFIER*

In this final out-of-band technique, a network identifier is used to link between the two accounts. So for example the jdoe identifier on the Identity Provider is mapped to johndoe. The assertion concerning johndoe is sent to the Service Provider, where it maps it to johnd. The mapping could be achieved on the individual systems or using a lookup/matching service..

### **A.2.2 Persistent Pseudonym Identifier**

This is actually a special case of d) above. The "network identifier" is a persistent pseudonym that exists over a number of sessions, until the federation is explicitly terminated. Typically in this environment the user "opts in" (i.e. consents) to link their two separate accounts. The processing can take a number of forms, but frequently involves the following steps:

- a) The user wishes to gain access to a resource on the Service Provider
- b) As they have not been authenticated to the Service Provider then will be re-directed to the Identity Provider
- c) If they have not been already authenticated to the Identity Provider they will be asked to logon (as jdoe)
- d) The Identity Provider will create a new pseudonym (e.g. **1232354**) and assign it to jdoe.
- e) The Identity Provider sends to the Service Provider the pseudonym **1232354**
- f) The Service Provider prompts the user to authenticate to their johnd account and optionally ask whether the user would like to federate the two accounts
- g) If the authentication is successful then the pseudonym **1232354** is mapped to the johnd account on the Service Provider

Once the accounts are federated together the user is not required to authenticate themselves to the Service Provider.

### **A.2.3 Transient Pseudonym Identifier and Attributes**

The previous use cases showed the use of persistent identifiers, what if you do not want to establish a permanent federation. This is where the use of transient identifiers are useful. Transient identifiers allow you to:

- Avoid having to manage userids and passwords at the Service Provider. Therefore all authentication is performed at the Identity Provider;
- Have a scheme whereby the Service Provider does not have to manage specific user accounts, for instance it could be a site with a "group-like" access policy;
- Support a truly anonymous service.

In this case the transient pseudonym used only exists for that session. The target identifier represents a group of users, perhaps based on a role. Therefore a user jdoe on the Identity Provider would access a library system and the account they use is a generic "student" account. This is the primary model that Shibboleth uses in Higher Education. A wide range of attributes could be used to map to generic accounts on the Service Provider, including roles and membership levels.

## **APPENDIX B: GLOSSARY AND TERMINOLOGY**

---

<b>Abbreviation</b>	<b>Terminology</b>	<b>Description</b>
ACL	Access Control List	An explicit set of permissions pertaining to users (or groups of users) who can access objects.
	Algorithm	A mathematical function used in Encryption to increase the difficulty of retrieving the information if not authorised.
	Availability	Ensuring that information and vital services are available to users when required.
	Authentication	The action of verifying information such as identity, ownership or authorisation.
CETIS	Centre for Technical Interoperability Standards	Provides all UK higher and further education institutions with a means of expressing their requirements to the international consortia developing technical interoperability specifications, contributing to the production of UK and European Standards and of supporting their implementation.
	Confidentiality	Protecting sensitive information from unauthorised disclosure or intelligible interception.
	Cryptography	The study of message secrecy and protecting sensitive communications. Primary purpose is hiding the meaning of messages, but not usually their existence.
DAC	Discretionary Access Control	An access policy determined by the owner of an object. The owner decides who is allowed access to the object and what privileges they have.
	Decryption	The process of converting encrypted data back into its original form, so it can be understood.
	Digital Certificate	An electronic "credit card" that establishes credentials when doing business or other transactions on the Web. It is issued by a certification authority.

DRM	Digital Rights Management	Refers to any of several technologies used by publishers or copyright owners to control access to and usage of digital data or hardware and to restrictions associated with a specific instance of a digital work or device.
	Digital Signature	The process of adding an electronic marker to information to validate both the content and the originator of the data.
	Encryption	Scrambling information to prevent unauthorised disclosure or modification using mathematical techniques.
E-DRM	Enterprise Digital Rights Management	<p>Refers to the use of DRM technology to control access to corporate documents, rather than consumer playable media.</p> <p>The technology usually requires a Policy Server system to authenticate user's rights to access certain documents.</p>
IMS	Information Management System	
IMS LIP	Information Management System Learner Information Package	A specification that addresses the interoperability of internet based learner information systems with other systems that support the Internet learning environment. The intent of the specification is to define a set of packages that can be used to import data into and extract data from an IMS compliant learner information server.
	Integrity	Safeguarding the accuracy and completeness of information and computer software.
JISC	Joint Information Systems Committee	A UK body funded by government to support the needs of IT tertiary education and funds CETIS.
LA	Local Authority	
LAR	Learner Achievement Record	A single electronic record that lists an individual's credit, unit and qualification achievements.

MAC	Mandatory Access Control	<p>An access policy determined by the system, not the owner. MAC is used in multi-level systems that process highly sensitive data.</p> <p>A multilevel system is a single computer system that handles multiple classification levels between subjects and objects.</p>
MIAP	Managing Information Across Partners	Streamlining how information on learning and achievement is collected, handled and shared across the education sector ensuring services are made available to individuals, employers and communities.
	Minerva	<p>The Minerva Programme is a working partnership of awarding bodies and regulation and delivery bodies across England, Wales and Northern Ireland, led by the National Assessment Agency.</p> <p>The Programme supports the modernisation of the exams administration system and enables the introduction of the specialised Diploma qualification.</p>
MIS	Management Information Systems	
NAA	National Assessment Agency	Develops and delivers high quality national curriculum tests and supervises the delivery and modernization of GCSE and A level examinations.
PBAC	Policy Based Access Control	Rather than roles, PBAC uses attributes. A role is just a special type of attribute. Attributes can be of various types including user attributes, environment attributes and application evidence.
PDP	Personal Development Planning	A structured and supported process undertaken by an individual to reflect upon their own learning, performance and/or achievement and to plan for their personal, educational and career development.

PKI	Public Key Infrastructure	<p>An arrangement that provides for trusted third party vetting of, and vouching for, user identities. It also allows binding of public keys to users. The public keys are typically in certificates.</p> <p>The term is used to mean both the certificate authority and related arrangements as well as the use of public key algorithms in electronic communications.</p>
QCA	Qualifications & Curriculum Authority	Maintains, regulates and develops the national curriculum and associated assessments, test and examinations, and accredits and monitors qualifications in colleges and at work.
RBAC	Role Based Access Control	<p>An approach to restricting system access to authorised users.</p> <p>The permissions to perform certain operations are assigned to specific roles. Users are assigned particular roles and through those role assignments acquire the permissions to perform particular system functions.</p>
SAML	Security Assertion Markup Language	An OASIS standard that enables authentication and authorisation information to be securely transferred between organisations. One of its uses is to support Federated Single Sign-On (SSO).
Shibboleth		Shibboleth is an Internet2 Middleware Initiative project that has created an architecture and open-source implementation for federated identity-based authentication and authorisation infrastructure based on SAML.
S/MIME	Secure Multipurpose Internet Mail Extensions	A standard for public key encryption and signing of e-mail encapsulated in MIME. Provides cryptographic security services for electronic messaging applications.

SSO	Single Sign On Authentication	<p>An authentication process that permits a user to enter one name and password in order to access multiple applications.</p> <p>The process authenticates the user for all the applications they have been given rights to and eliminates further prompts when they switch applications.</p>
UK LIP	UK Learner Information Profile	<p>Covers the learner profiles in use in tertiary education within the UK. Acts as the normative basis for standards learner information profiling and is designed to meet the needs of the further and higher education community.</p>
ULN	Unique Learner Number	<p>This is unique to an individual and is used to link all Qualifications and Credit Framework achievements to the individual's Learner Achievement Record.</p> <p>MIAP programme is developing the ULN for post 14 learners (including Further Education and Higher Education).</p>
UPN	Unique Pupil Number	<p>Associated with the National Pupil Database (NPD) for learners from 3 years old until they finish Key Stage 3 or 4.</p>
VLE	Virtual Learning Environment	<p>A software system designed to facilitate teachers in the management of educational courses for their students, especially by helping teachers and learners with course administration.</p> <p>The system can often track the learner's progress. While often thought of as primarily tools for distance education, they are most often used to supplement the face-to-face classroom.</p>