Australian *Flexible* Learning Framework

Supporting Flexible Learning Opportunities

Legal Issues in Electronic Authentication for Flexible Learning

– A Research and Advisory Paper –

Prepared by

Galexia Consulting Pty Ltd

Level 1, 3 Montague St, Balmain (Sydney), NSW, 2041, Australia

www: consult.galexia.com

An initiative within the Australian Flexible Learning Framework for the National Vocational Education and Training System 2000 – 2004.

Managed by the Flexible Learning Advisory Group on behalf of the Commonwealth, and all States and Territories, in conjunction with ANTA.

© 2003 Australian National Training Authority

This work has been produced with the assistance of funding provided by the Commonwealth Government through the Australian National Training Authority. Copyright for this document vests in ANTA. ANTA will allow free use of the material so long as ANTA's interest is acknowledged and the use is not for profit.

Contents

Executive Summary

Overview

Authentication is the process of establishing whether someone or something is who or what its identifier states it is. The key benefit of electronic authentication is that it enables electronic transactions to take place in an environment of trust and confidence.

There are numerous electronic authentication tools available, including: user name and password; digital signature certificates (with or without Public Key Infrastructure (PKI)); and biometrics. In the Australian regulatory and business environment there is no legal requirement to choose a particular electronic authentication tool.

Benefits of electronic authentication

There are benefits for the VET sector in migrating to a strong, centrally managed, coordinated electronic authentication model. These include:

- **Reduction in cheating**
  Electronic authentication may provide a deterrent to cheating through strong registration processes (which help to reduce opportunities for identity fraud) and improvements in message integrity during interactions between learners and VET providers.

- **Improved user convenience**
  There is potential for significant enhancement to user convenience, simplicity, customisation and service if a sector-wide electronic authentication solution is developed. For example, a system which provided ‘single sign on’ for all VET providers could reduce the number of login names and passwords which participants have to remember, and the development of a skills passport could provide a convenient, portable mechanism for carrying strong evidence of qualifications. These improvements in user convenience are probably of greater benefit than the potential impact on cheating.

- **Improved system integrity, operability and flexibility**
  There is potential for a sector wide electronic authentication solution to provide significant advantages over the current system of *ad hoc* electronic authentication initiatives. These benefits include greater trust and confidence in the integrity of the system, greater interoperability between applications across the sector, and greater flexibility for participants as they move between VET providers.

- **Improved cross recognition of assessment and qualifications**
  Electronic authentication may enhance trust and confidence in the cross recognition of assessment and qualification – a major objective in flexible learning.

Main legal issues

During the research for this paper, Galexia Consulting has confirmed that there are a number of legal and regulatory obstacles to the successful development and implementation of electronic authentication for flexible learning in the VET sector.

The importance of particular legal issues depends on the electronic authentication model adopted in the VET sector. This paper identifies five potential models for electronic authentication in the flexible learning environment.

The main legal obstacles to electronic authentication are:

- Legal uncertainty caused by the continuing absence of a general regulatory framework for electronic authentication (a situation which we expect to continue in the medium term); and
- Where a Public Key Infrastructure is the chosen method of electronic authentication, legal uncertainty regarding the allocation of liability between participants in authenticated transactions as part of a Public Key Infrastructure.

A number of other legal issues have been resolved in Australia, including those surrounding electronic payments and the difficult issue of forming contracts via purely electronic means (i.e. without paper copies or handwritten signatures). This paper also identifies the importance of privacy issues in electronic authentication and discusses strategies to ensure that privacy is protected in the majority of transactions and electronic authentication scenarios.

National and international practice of electronic authentication

The Australian VET sector has not yet advanced beyond ad hoc arrangements in its an approach to electronic authentication. Different forms of electronic authentication are used in individual applications. The choice of electronic authentication tool may be based on availability, the level of understanding of participants, or in some cases on a risk and cost/benefit analysis.

The Australian non-VET sector (e.g. higher education) is slightly more advanced and is presently positioned between:

- a model where a centralised body provides to a tool-box of electronic authentication solutions which are considered suitable for use in the sector and limited additional functions such as additional layer of technical support, education, and professional development; and
- a model in which the central body has a stronger role in driving inter-operability of electronic authentication within the sector, by adding standards to the tool-box and other functions, ensuring that the majority of authentication solutions are suitable for the sector and will work together.

Other jurisdictions are more advanced, especially the United Kingdom where they are close to successfully a model that involves a central body making decisions about the adoption of electronic authentication across the whole VET sector, determining appropriate electronic authentication solutions, and liaising and coordinating with other sectors (such as higher education).

Recommendations for the way forward

It is our primary conclusion that electronic authentication (and hence flexible learning) is unlikely to advance further in the VET sector without implementation of a model that involves a central body making decisions about the adoption of electronic authentication across the whole VET sector, determining appropriate electronic authentication solutions, and liaising and coordinating with other sectors (such as higher education).

A strong national electronic authentication solution across the entire VET sector will not be achieved quickly. Our recommendations contemplate a staged migration path.

This paper sets out recommendations to FLAG to enable them to assist ANTA CEOs and their Ministers for Education to develop a planned and scaleable way forward.

Document outline

Chapter 1 Introduction sets out the background and scope of this paper.

Chapter 2 What is electronic authentication? explains the general concepts of electronic authentication and examines the range of electronic authentication tools that are now available.

The key benefit of electronic authentication is that it enables electronic transactions to take place in an environment of trust and confidence. Four particular issues need to be addressed before participants will have trust and confidence in an electronic environment: identity; privacy; security; and authentication.

There are numerous electronic authentication tools available, and more are developed every year. In choosing which authentication technology to use, considerations will include: the value and risk of the transaction; the cost of implementing the authentication technology; and the ease of use for clients/consumers. Chapter 2 includes a summary of the main characteristics of various electronic authentication tools currently available, and explains in further detail one such tool, Public Key Infrastructure (PKI) - currently a popular strong authentication tool favoured in advanced electronic authentication environments.

Chapter 3 Flexible Learning Initiatives provides an overview of flexible learning and summarises research into its take-up in Australia.

In practice, most flexible learning has the important characteristic of being learner centred, but its delivery is ‘blended’, rather than purely online.

Chapter 3 also includes 4 detailed case studies of electronic delivery of education services drawn from Australia and overseas.

Chapter 4 Flexible learning and electronic authentication examines the motivations for using electronic authentication in a flexible learning environment and sets out a number of relationship and application scenarios in which electronic authentication might be used in the VET sector.

Chapter 5 The current legal and regulatory framework for electronic authentication in Australia examines the existing legal and regulatory framework in which flexible learning operates in Australia. Relevant legislation, codes and common law are identified and summarised.

Chapter 6 General legal and regulatory issues discusses some broad legal and regulatory issues that apply across the entire VET sector. There is a lack of a legal and regulatory framework within Australia for electronic authentication, and while there are proposals to develop such a framework, progress is slow. Legal and regulatory issues identified and discussed include: privacy; legal liability; and electronic formation of contracts.

The impact of legal and regulatory issues on the VET sector will depend on the electronic authentication tool used and the characteristics of the transaction or relationship in question.

Chapter 7 Specific legal and regulatory issues examines the legal and regulatory issues identified in Chapter 6 from a different perspective: by identifying a sample of transactions or relationships which might arise in the flexible learning environment, and considering the legal and regulatory issues which might arise in that particular context.

Until an authentication model is chosen there are too many potential legal scenarios to provide a detailed response on each issue. Accordingly, Chapter 7 identifies the key issues and then provides pointers to sources of further legal guidance.

Scenarios considered include: access to content and learning materials; verifying the qualifications of education providers; the identification of learners, their attributes and qualifications; administrative transactions with learners (eg subscription, payment, enrolment); online assessment of learners; and the reliance by third parties (eg employers, licensing authorities or other education providers) on the VET sector electronic authentication system. Where appropriate, Chapter 7 also notes any different issues raised by the type of electronic authentication tool selected in the context of each sample transaction or relationship.

By examining typical transactions and relationships, the benefits that electronic authentication would bring in those scenarios, and the legal issues raised by the use of electronic authentication in such scenarios, this paper identifies a requirement for the VET sector to develop appropriate and effective electronic authentication arrangements.

Chapter 8 Models for electronic authentication in VET describes 5 potential models for the development and implementation of electronic authentication in the VET sector. These models range over a continuum: from the current ad hoc arrangements for electronic authentication in the VET sector, to an ambitious model which involves centralising decision-making about the adoption of and solutions for electronic authentication across the whole VET sector.

Chapter 9 Findings and Recommendations sets out the primary conclusions to be drawn from this paper and makes recommendations to FLAG to enable it to assist ANTA CEOs and their Ministers for Education to develop a planned and scaleable migration path forward. Underpinning these recommendations is the conclusion that the costs of allowing existing ad hoc arrangements to continue and spread may be high in the long term. Untangling existing arrangements at a later stage and attempting to replace them with an inter-operable solution will be costly.

As well as ANTA co-ordinating the provision to the VET sector of education and assistance in managing legal issues in current *ad hoc* arrangements for electronic authentication, it is recommended that the VET sector coordinate a program to raise the general awareness and professional development of key participants in the sector in relation to the role and importance of electronic authentication. In addition, the VET sector should maintain a watching brief and actively participate in the law reform process surrounding outstanding legal issues in electronic authentication.

The recommendations also envisage ANTA being given a central role in developing, adopting and pursuing an electronic authentication strategy for the VET sector as a whole, and taking a leading role to drive a national framework for electronic authentication in the VET sector. The VET sector should foster coordination of electronic authentication activities with other education sectors, perhaps through joint projects or research. A commercial foundation for the work required in relation to electronic authentication in the VET sector needs to be established, and some options are suggested for further exploration.

It is also recommended that the VET sector consider further research on a range of strategic issues in electronic authentication for the sector, including research relating to: matching specific legal issues against the chosen authentication model, once broad strategic decisions have been made about the likely electronic authentication solution; the development of common contractual clauses across the VET sector to allocate legal liability in electronic authentication; the cross recognition of qualifications; and jurisdiction issues for cross recognition and cross border transactions.

Additional materials included in the paper

- a list of the sources of law and regulation, and references to primary materials available online;
- a glossary;
- a list of recommended reading; and
- a list of institutions consulted in the course of preparing this paper.

Chapter 1. Introduction

1.1. Introduction to this paper

The Flexible Learning Advisory Group (FLAG) have commissioned this research paper to map Commonwealth and State/Territory legislation and regulation in relation to electronic authentication and the needs of flexible learning, particularly in an online environment.

In addition this paper identifies a number of electronic authentication models for vocational education and training (VET) given current regulatory structures and practices.

This paper also makes recommendations for regulatory changes in order to enable wider use of electronic authentication in VET.

1.2. Background

In August 1999, the Australian National Training Authority Chief Executive Officers (ANTA CEOs) endorsed the *Australian Flexible Learning Framework for VET 2000 – 2004.*[1] The Framework is the five-year strategic plan for national collaboration for flexible learning in Australia's VET system. It is designed to support both accelerated take-up of flexible learning modes and to position Australia as a world leader in applying new technologies to vocational education products and services.

The term 'flexible learning' incorporates the wide range of learning options available in the Australian VET sector. It has been defined as follows:

> 'An approach to vocational education and training which allows for the adoption of a range of learning strategies in a variety of learning environments to cater for differences in learning styles, learning interests and needs, and variations in learning opportunities (including on-line).'[2]

FLAG is a strategically-focused group of senior VET personnel advising ANTA CEOs, the ANTA Board, the Department of Education Science and Training (DEST), and the Australian Information and Communication Technology Education Committee (AICTEC), on national issues relating to the directions and priorities for flexible learning in VET, with particular reference to online technologies.

The Australian Flexible Learning Framework (the Framework) is built on five goals:

1. Creative, capable people;
2. Supportive technological infrastructure;
3. World-class online content;
4. Enabling policies; and
5. Problem-solving regulation

---

[1] Australian National Training Authority (EdNA VET Advisory Group), Flexible Learning for the Information Economy: Australian Flexible Learning Framework for the Vocational Education and Training System 2000 – 2004 (2000) <http://flexiblelearning.net.au/aboutus/aflframework2000.pdf>.

[2] EdNA VET Advisory Group (2001). see http://flexiblelearning.net.au/policies/year2001/finchap 1.pdf.

The Expert Advisory Group has been established to address issues that relate to *Goal 5 (Problem Solving Regulation)* of the *Australian Flexible Learning Framework*. Its purpose is to assist FLAG (and through FLAG, the wider VET sector) to advocate that the legal and regulatory framework in Australia provides adequate protection for learners; removes legal and regulatory barriers to the effective use of information technology in VET; and fosters open trade in Australian VET products and services. This Expert Advisory Group had direct oversight over this current project and the production of this research paper.

Electronic authentication issues are relevant to several other Australian National Training Authority (ANTA) projects which are currently in progress:

- **Skills Passport**
  ANTA is examining the development of a 'Skills Passport'. This is broadly defined as a portable record of competencies possessed by an individual. Its aim is to facilitate improved recognition of what an individual can do, both in terms of formal qualifications held and individual, or groups of, competencies. A skills passport could either include electronic authentication tools or complement them.

- **Unique Client Identifier**
  ANTA has a national project examining the development and implementation of a unique education and training client identifier.

- **Qualification Authorities**
  Individual states are developing Qualification Authorities[3] which will initially serve as accreditation providers for participants in the VET sector. In the future they may act as a repository for qualifications (and assessment) and may be closely linked to the skills passport and the underlying electronic authentication infrastructure.

- **Digital Rights Management Systems**
  ANTA is exploring the opportunities and obstacles regarding the deployment of Digital Rights Management Systems (DRMS) in the VET sector. Electronic authentication may act as an enabler for DRMS.

- **E-business Program**
  This proposed project will help coordinate a range of recent e-business activities in the VET sector and provide a coherent foundational infrastructure for e-business in VET. A sub-project includes the development of a VET portal. Electronic authentication may play a role in achieving inter-operability across the various e-business applications.

[3] Victoria has established a Qualification Authority (QA) and Tasmania has a current project examining the establishment of a QA. QAs have been developed in other jurisdictions – e.g. New Zealand, Scotland and Ireland.

1.3. Initial questions for this research paper

The key objective of ANTA is to provide world-class flexible learning models for VET. To achieve this it will be necessary to develop a seamless system for delivery, from a provider and a learner perspective. Authentication is a vital component of the provision of flexible learning. An authentication system must be able to provide:

- Authenticity;
- Integrity and confidentiality; and
- Certainty.

As a starting point, this paper was asked to consider the following questions:

- What approaches to electronic authentication will be accepted as providing authenticity, integrity and confidentiality, and certainty in terms of flexible learning in Vocational Education and Training?
- Are there any good practice models of electronic authentication in an online environment in Australia?
    - If yes, what are they?
    - If no, are there any overseas that may be of use to Vocational Education and Training in Australia?
- Are there any privacy issues that need to be considered in the use of electronic authentication?
- Is online assessment proving successful? Is it accepted by auditors?
- What are the risks of providers accepting online enrolments?
- What are the legal ramifications of online transactions in a Vocational Education and Training environment?
- What level of authentication will a provider need to ensure certainty of pedagogical and administrative relationships?
- What initiatives are underway on this issue in the higher education and schools sectors and what opportunities are there to work with the higher education and schools sectors in pursuing a collective education industry viewpoint on this issue?

1.4. Production of this paper

In September 2002, Galexia Consulting[4] was commissioned to produce this paper. The Galexia Consulting project team included Chris Connolly, Jack Goodman and Peter van Dijk.[5]

Galexia Consulting conducted a series of consultations with key stakeholders in Australia and the United States, and undertook extensive research on national and international initiatives in VET and electronic authentication.

The project was managed for FLAG by Jennifer Dunbabin of the Office of Post Compulsory Education and Training, Tasmania.

The final draft of this paper was provided to FLAG in February 2003.

1.5. All references and URLS are correct as at 25 February 2003.

[4] <http://consult.galexia.com.au>.

[5] With assistance from Nawaz Isaji, Fiona O'Loughlin, Prashanti Ravindra, Francis Vierboom and Richard Weatherley.

Chapter 2. What is electronic authentication?

This chapter explains the general concepts of electronic authentication and examines the range of electronic authentication tools which are now available.

A technical definition of authentication is the process of establishing whether someone or something is who or what its identifier states it is. An authentication process may be enabled by:

- Something you know, like a PIN or password;
- Something you have, as with smartcards, challenge-response mechanisms, or public-key certificates; or
- Something you are, as with positive photo identification, fingerprints, and biometrics.

The key benefit of electronic authentication is that it enables electronic transactions to take place in an environment of trust and confidence. The Internet, for example, is an open network where the community has a low level of trust. However, authentication tools can provide greater confidence in the identity, validity and authenticity of participants, sites and objects.

Some means of electronic authentication are weak and may be easily stolen, accidentally revealed or forgotten.

> 'Failure to properly authenticate a transacting party may lead to situations such as the illegal transfer of funds, unauthorised ordering of goods or the mischievous alteration of data. Authentication therefore underpins confidence in electronic transactions and is a vital component of e-commerce, which depends upon transactions being accepted as valid and binding.'[6]

Authentication also needs to be distinguished from identification. Authentication can assist a relying party to decide whether the presenting party has the required attributes to participate in a transaction. Although one of these attributes may be identification, many transactions can proceed without identification. For example, in an online publishing context, the relying party only needs to check whether the presenting party is a paying subscriber, they may have no motive for knowing the actual identity of that particular subscriber.

[6] National Office for the Information Economy, *Online Authentication – A Guide for Government Managers* (July 2002) <http://www.noie.gov.au/publications/NOIE/online_authentication/OnlineGuideFinal.pdf> at page 3.

In the electronic learning sector, some commentators are hoping that electronic authentication will solve some or all of the sector's current security problems:

> 'There are promising technologies that offer solutions to the problem of security on open networks: cryptography, digital certificates, biometrics for example. These solutions are however expensive, and digital certificates for example are not a mature technology. There is also a danger that implementations will ignore realities of how users and administrators behave. However secure the technology is, if the users and administrators do not fully understand or are motivated to get round the system, they probably will find ways to do so.'[7]

2.1. Trust

A starting point for a discussion of electronic authentication is to consider the concept of trust. The Internet and other electronic environments in which flexible learning may take place are mediums for exchanging the information necessary for individuals and organisations to engage with each other. However, this environment raises issues of trust, privacy and security.

Four particular issues need to be addressed before participants will have trust and confidence in these electronic environments:

- **1. Identity**
  How do consumers establish unique identities conclusively for the purposes of participating without laying themselves open to the threat of having that identity misappropriated, copied, or abused in some other manner?
- **2. Privacy**
  How do individuals have confidence that the personal information which they must often supply to public and private sector providers of goods and services will not be made available to third parties for other purposes including marketing services to them which they did not seek?
- **3. Security**
  How can individuals be confident that the communications systems which they use are fully secure from interception and have adequate security management systems in place to cope with major threats?
- **4. Authentication**
  How can the parties to an electronic transaction have confidence that each is who they claim to be, and that they have? For example, the appropriate attributes which give them the legitimate capacity to enter into particular transactions which cannot then be repudiated once entered into.[8]

[7] Joint Information Systems Committee (JISC) Committee for Awareness, Liaison and Training Programme (JCALT), Identification of Human and Organisation Issues Concerning Network Security (March 2001) <http://www.jisc.ac.uk/uploaded_documents/ns.rtf>. For the final report refer to http://www.litc.sbu.ac.uk/jcalt/report.pdf.

[8] National Office for the Information Economy, *Towards a National Authentication Technology Framework* (May 2002) <http://www.noie.gov.au/publications/NOIE/Authentication/NATF_Discussion_paper_July2002.pdf>.

All four of these issues are inter-connected. However, it is important to understand that authentication is not the same thing as personal identity. Frequently all that an individual has to do for the purposes of authentication is to establish that they are a member of an organisation and are authorised within that organisation to conduct a given transaction.

A range of scenarios for the use of electronic authentication in the VET sector are described in *Chapter 4. Flexible learning and electronic authentication*. These scenarios help illustrate the importance of trust. One particularly useful example is the level of trust which is required before an employer, licensing authority or education institution would recognise a learner's qualifications. They will have to trust that the learner is correctly identified, that the qualifications meet the appropriate standards and that the qualifications have in fact been obtained. Electronic authentication tools can help with each of these requirements.

2.2. Electronic authentication tools

There are numerous electronic authentication tools available, and more are developed every year. Some categories are:

- User name and password or PIN;
- SSL (secure sockets layer);
- Two factor;
- Digital signature certificates (without Public Key Infrastructure (PKI));
- Digital signature certificates (with PKI); and
- Biometrics.

In the Australian regulatory and business environment there is no legal requirement to choose a particular electronic authentication tool. The decision is up to the electronic service provider, and will usually be made by balancing the risks of fraud, impersonation and identity theft against issues of cost and convenience.

In *Trusting the Internet – A small business guide to E-security*[9] the National Office for the Information Economy (NOIE) recommends that the choice of which authentication technology to use should be based on the following factors:

- Value of the transaction (financial and content) and corresponding risks;
- Cost of implementing and then maintaining the authentication technology in use against future benefits; and
- Ease of use for clients/consumers.

[9] National Office for the Information Economy, *Trusting the Internet – A small business guide to E-security* (July 2002) <http://www.noie.gov.au/publications/NOIE/trust/>; National Office for the Information Economy, *Online Authentication – A Guide for Government Managers* (July 2002) <http://www.noie.gov.au/publications/NOIE/online_authentication/OnlineGuideFinal.pdf>.

The following table summarises the main characteristics of each technology.

Technology	Example	How it works	Pros	Cons
Password or PIN	Online subscription to the Australian Financial Review – http://afr.com	Matches user name and password to restrict access and authenticate identity	• Inexpensive • Well understood by users	• Can be compromised by users • Does not authenticate data • Often transmitted insecurely
Two Factor	Clough Hall Technology School (UK) student and staff use SecurID tokens for authentication, confidentiality, integrity and 'single sign on' (SSO)[10] – http://www.rsasecurity.com	Uses username, password and token, plus time/event synchronous or challenge-response authentication method	• Mature • Understood by users (card plus PIN)	• Does not provide encryption • Does not support digital certificates • Can be costly
SSL (Secure Sockets Layer)	Membership of Hotmail for personal email services – http://www.hotmail.com	Creates a secure connection between Internet application and user	• Widely supported in Web browsers • Offers protection for all data transmitted between servers	• Customers cannot choose when it is used • Can rely on passwords for initial access
Digital Signature Certificate (without PKI)	Pretty Good Privacy (PGP) used for email authentication – http://www.pgp.com	Uses public key cryptography; keys can be generated and authenticated by individual users	• Keys provide higher levels of authentication • Supported by many software packages	• Private keys can be compromised • Public keys required to send information
Digital Signature Certificate with PKI	Health Electronic Signature Authority issues digital certificates for medical organisations and individuals – http://www.hesa.com.au	Uses public key cryptography; keys are generated by Certificate Authorities	• Keys provide higher levels of authentication • Used by governments and major companies • May be used with biometrics to access private keys	• Issuing digital certificates can be costly • Businesses may require multiple digital certificates • Private keys can be compromised • Public keys required to send information
Biometrics	Smartgate – a trial of photo matching technology for air-crew at Sydney Airport – http://www.customs.gov.au/	Uses unique biometric information about the user to match against a file held centrally or distributed on a token (such as a smart card).	• Makes identity fraud difficult • May not require users to remember PINs etc.	• Can be costly to implement • Not a mature technology – still largely in pilot phase.

[10] Clough Hall Technology School, *RSA Security helps raise student achievement* (2000) <http://www.rsasecurity.com/products/securid/success/CLOU_CP_0700.pdf>.

Many common business applications also use a variety of authentication technologies. Two or three factor security is becoming more common for high value transactions. For example, a system may require a PIN and Password to log in, and may also use SSL technology to encrypt the contents of the transaction. Nearly all biometric applications will take place within multi-factor security environments.

One electronic authentication tool which requires further detailed discussion in this report is Public Key Infrastructure (PKI).

2.3. Public Key Infrastructure (PKI)

A Public Key Infrastructure (PKI) can be used to help deliver trust and confidence in electronic transactions and communications. As the name suggests, a Public Key Infrastructure is the broad system of technology, processes and policies which allows electronic authentication to be implemented using public key encryption.

Encryption is the science of secret writing. It allows two parties to communicate in such a way that a third party is unable to determine the content of the message (confidentiality) or alter the message without detection (integrity). Encryption can also provide authentication and non-repudiation because the two communicating parties alone know how to encrypt and decrypt each other's messages.

In a PKI a user has two keys (a key pair): a public key, and a private key. (The term 'key' is used to describe a mathematical value, derived from a prime number that can be used in conjunction with an algorithm to encrypt or decrypt a message.) Users may publish their public key freely so that others can use it to communicate with them.

The system then allows users to create digital signatures which can be attached to electronic transactions to assist validate the identity of the person who sent the communication, and to provide the recipient with the ability to ensure that the communication has not been altered. Digital signature certificates contain information about users which verify their identity and attributes.

A digital signature has four distinct features:

- **Authentication** – A digital signature verifies who sent the message/object;
- **Integrity** – A digital signature verifies the message/object content has not been altered in any way between being sent and received;
- **Non-repudiation** – A digital signature can limit opportunities to dispute content and authorship of a message/object; and
- **Confidentiality (optional) –** An optional feature is that a digital signature can be used to ensure that only the person to whom the message/object is directed can read it.

Digital signatures can function with electronic messages, documents or communications in the same way as physical signatures do on paper. Digital signatures can be applied to email, Internet transactions, Web pages, online transactions and more.

To enable all the features offered by PKI (i.e. authentication, integrity, non-repudiation and confidentiality), two key pairs are used: a signing key pair and an encryption (or confidentiality) key pair. The user's signing key pair can authenticate, verify the integrity of and prevent repudiation of a message sent by the user. Use of the encryption key pair of the recipient can preserve the confidentiality of a message sent to the recipient.

Digital signature certificates can be used to make a public key freely available. They associate (or 'bind') a particular public key with either:

- An identified particular person (an identity certificate);
- A person who is not specifically identified in the digital certificate with certain attributes (an attribute certificate); or
- An identified person who has certain attributes (e.g. a role within an organisation, qualifications, eligibility or entitlements).

Digital signature certificates are analogous to physical or paper certificates, such as a driver licence, passport, or membership card. Physical certificates can identify an individual for a certain purpose - e.g. a driver's licence identifies someone who can legally drive in a particular country. Likewise, a digital certificate can be presented electronically to establish identity or enable access to information or services on the Internet.

To trust the assertion in a digital certificate, that the public key in the digital certificate is associated with the person identified (or who has the attributes listed in the digital certificate), digital certificates are endorsed by a trusted third party known as a Certification Authority (CA). The CA is responsible for validating all applications for digital certificates. If the CA is satisfied that the association made between the public key and the person/attributes is valid, it attests to this validity by 'stamping' its digital signature on the digital certificates it issues.

For public key cryptography to be widely accepted it needs to be supported by an administrative framework with standards and rules that are well known and transparent. This administrative framework – a Public Key Infrastructure (PKI) – can support authentication of an individual (or role), the integrity of messages and the confidential transfer of messages.

The main components of a PKI are:

- **Certification Authorities (CAs)** – issue and revoke digital certificates;
- **Registration Authorities (RAs)** – conduct the initial verification of a potential subscriber's identity and/or attributes;
- **Subscribers** – digital certificate holders;
- **Relying parties** – rely on the contents of a digital certificate in communicating with subscribers; and
- **Directories** – may store public keys, digital certificates or Certificate Revocation Lists (CRLs).

The main operations and processes of a PKI are:

- **Registration** – the process whereby a potential subscriber makes themselves and/or their relevant attributes known to the CA directly (or through an RA);
- **Key generation –** the generation of one or more key pairs by the CA or by the subscriber;
- **Certification –** the issue by a CA of a digital certificate to a subscriber;
- **Certificate expiry** – the allocation of a period for which a digital certificate will remain valid;
- **Certificate revocation** – the revocation of a digital certificate prior to its expiry (e.g. where the private key has been compromised); and
- **Certificate Revocation Lists** (CRLs) – directories of revoked digital certificates.

In Australia, Gatekeeper is the Commonwealth Government's strategy for the use of PKI. Gatekeeper includes accreditation of CAs and RAs to ensure that their technologies and practices comply with Government policies. The accreditation process aims to provide certainty and trust for all parties involved in the use of Gatekeeper digital certificates. Gatekeeper standards are mandated in contracts and policy statements between the National Office for the Information Economy (NOIE) and CAs and RAs, and between the CAs and RAs and their subscribers and relying parties in various contracts.

The private sector has been slow to roll out substantial PKI applications for individuals. Currently, there is no mass market private sector PKI application in place in Australia at this time, although there are plans for widespread use of PKI in financial services. However, there are numerous PKI applications in the government and private sectors for business-to-business and professional services.

In the VET sector (and elsewhere in the education sector) there are numerous opportunities for the use of PKI:

- Business to client – e.g. Registered Training Authority (RTO) to student;
- Business to business – e.g. RTO to trainer, RTO to administrator, RTO to RTO, RTO to education content providers.

These opportunities in the VET sector are discussed in greater detail in *Chapter 4. Flexible learning and electronic authentication*.

Chapter 3. Flexible Learning Initiatives

3.1. Overview of flexible learning

Flexible learning is a term to describe a range of learning environments that collectively provide a convenient and collaborative learning experience for students. The National Centre for Vocational and Education Research (NCVER) stated:

> 'There is a range of definitions of what online learning is and little consistency in information about its full scope. Online is seen as a convenient and flexible way to provide learning which is student-centred and collaborative and can be outside, or within, a physical classroom, or involve other approaches to delivery.'[11]

The EdNA (Education Network Australia) VET Advisory Group has defined flexible learning as:

> 'An approach to vocational education and training which allows for the adoption of a range of learning strategies in a variety of learning environments to cater for differences in learning styles, learning interests and needs, and variations in learning opportunities (including on-line).'[12]

In practice, most flexible learning has the important characteristic of being learner centred, but its delivery is 'blended', rather than purely online.

3.2. Flexible learning – take up in Australia

Under the auspices of the Australian Flexible Learning Framework[13] NCVER (on behalf of ANTA-FLAG) has conducted substantial research and analysis regarding the take-up of flexible learning in Australia. The following general conclusions have been drawn from the research to date:[14]

- There appears to be relatively little pure online delivery of VET. Online approaches are being used in combination with other delivery methodologies;
- Most students who experience online learning do so as part of a program delivered by mixed mode, using face-to-face and other strategies as well as an online approach;
- It is difficult to determine the exact amount of online learning taking place, because it is often combined with other learning approaches;

---

[11] National Centre for Vocational and Educational Research, *At a Glance: Flexibility through online learning* (2002) <http://www.ncver.edu.au/research/proj/nr1F12/nr1F12.pdf>.

[12] EdNA VET Advisory Group(2001) see <http://flexiblelearning.net.au/policies/year2001/finchap1.pdf>.

[13] Australian National Training Authority (EdNA VET Advisory Group), *Flexible Learning for the Information Economy: Australian Flexible Learning* Framework *for the Vocational Education and Training System 2000 – 2004* (2000) <http://flexiblelearning.net.au/aboutus/aflframework2000.pdf>.

[14] National Centre for Vocational and Educational Research, *At a Glance:* Flexibility *through online learning* (2002) <http://www.ncver.edu.au/research/proj/nr1F12/nr1F12.pdf>.

- The cost-effectiveness of online delivery is difficult to determine accurately. However, it seems that online delivery is likely to be more expensive than conventional approaches, but is also likely to deliver better learning outcomes and levels of learner satisfaction;
- What learners value particularly about online delivery is its flexibility - the convenience and freedom it offers; that is, learning that is ‘just in time, just enough and just for me’;
- Other qualities of the learning experience which are highly valued by learners include opportunities to communicate and interact with teachers and other students, responsive teaching staff who give frequent, thoughtful and informed feedback, well-planned and organised programs of learning, and well-designed, interactive, up-to-date and accessible learning resources and assessment materials;
- Teachers as well as students are positive and enthusiastic about online learning and its quality features, but both recognise the need for support to ensure more effective online learning;
- The changing role of teachers and the way they are working to provide flexible training needs to be acknowledged and supported; and
- A range of strategies has been identified to overcome key barriers to the successful adoption of online delivery, the most important being induction programs, cost reduction strategies for delivery, use of e-business approaches, teachers’ professional development and improved recognition of their work roles and the funding models being used.

There have also been two Australian statistical reviews of the take up of flexible learning in Australia:

3.2.1. TAFE Frontiers (2001) – The Current Status of Online Learning in Australia

The TAFE Frontiers report[15] found that in 2000 approximately 30 percent of organisations were using intranets and 14 percent using the Internet to deliver learning. According to the report, this low level was in part due to the number of decisions required to implement online learning systems within organisations.

While take-up may be slow, organisations surveyed planned to increase the use of online training over the next three years.

Key findings in relation to the planned use of online learning included:

- The number of organisations planning to use the Internet or intranets to deliver learning is set to more than double (use of intranets will grow from 29% to 65.7% of the survey respondents; and use of the Internet will grow from 14.6% to 54.5%);
- The planned rise is steepest in certain sectors, such as health and community services, construction and wholesale trade;
- Local government outstrips the public and private sectors in their intention to use the Internet or intranets to deliver learning;
- All Federal government respondents either currently or in the next two years will use the Internet to deliver training;
- Multimedia, teleconferencing and online learning are the preferred information technology systems to deliver learning; and
- The amount of training time delivered by online methods is expected to almost double in the next three years.

Of those organisations not using or planning to use online learning, the reasons given were:

Factors limiting online learning implementations	
Not a business priority at this stage	20.2%
Budgetary considerations	14.6%
Lack of knowledge about online learning	10.3%
IT limitations	10.3%
Not appropriate for the organisation	9.4%

[15] TAFE Frontiers, *The Current Status of Online Learning in Australia* (2001) <http://www.tafefrontiers.com.au>. In June 2001, TAFE Frontiers and Online Learning Australia produced a draft report that analysed the current status of online learning in Australia. The report surveyed 1,200 of Australia's largest employing businesses in both the public and private sectors and, amongst other things, analysed the current and planned use of information technology systems to deliver or provide access to learning.

For organisations that were planning to adopt online learning strategies, there were a number of trends identified in the report that highlight how these organisations may use and develop online learning strategies:

- There is a general trend towards greater use of customised training rather than generic online learning products;
- More organisations are likely to look to external rather than internal training providers for the delivery of online learning;
- An overall increase is expected to be seen in the use of online learning supported by other processes such as classroom training and mentoring;
- Many organisations do not know where they would go to obtain assistance in developing online learning services or packages;
- Those who identified their source of assistance were far less likely to nominate TAFE or other educational providers as sources of assistance. Budget/resource constraints are the most commonly cited obstacle in developing online learning within an organisation; and
- Organisational culture and lack of knowledge are also seen as major barriers.

For organisations that were surveyed as part of the analysis of online learning in Australia, there were a number of strategic issues that effected decisions to develop online learning within organisations, namely:

- Business priorities and budgetary factors were most commonly cited as factors behind the non-use of online learning;
- Accessibility was given as the main attraction of online learning, ahead of other factors such as cost, consistency and improved learning outcomes; and
- The majority of organisations are developing an online learning strategy as a whole of business approach.

3.2.2. NCVER Research on online usage in the VET sector

National Centre for Vocational and Education Research (NCVER) research[16] suggests that there is extensive and rapidly growing take-up and use of online learning, although there appears to be variation across industry categories. Categories with relatively low levels of online provision are wholesale trade; electrical gas and water; plus manufacture and mining. Higher levels are in agriculture, forestry and fishing; accommodation, cafes and restaurants; communication services; property and business; education and health plus community services.

The NCVER report found there were 68 providers delivering more than 700 online VET modules. The number of students studying online was very low. The types of online communication used by those who were surveyed is indicated in the table below:

Communications channel	Take-up
Email	96.4%
Newsgroups and bulletin boards	86.9%
Online portfolio and assignment submission	78.1%
Chatrooms	68.8%

[16] National Centre for Vocational and Educational Research, *At a Glance: Flexibility through online learning* (2002) <http://www.ncver.edu.au/research/proj/nr1F12/nr1F12.pdf>. The study used a mixture of quantitative and qualitative approaches, including a literature review: surveys of VET public and private providers, interviews with practitioners (147 respondents) and four case studies.

3.3. Case Studies of national and overseas implementations

During the project the research team interviewed several education institutions and service providers in Australia and the United States. These interviews assisted our general consideration of the issues (a complete list of consultations is appended to this paper). There were four stand out case studies which require more detailed consideration, and provide a useful insight into the use of electronic authentication in practice.

3.3.1. WebCT / Blackboard

Organisation	WebCT
Type/Mission	For-profit learning management system provider
Location	Lynnfield, Massachusetts, USA
Year Founded	1995
Financing	$125-million (USD)
Annual Sales	N/A (private company)
Products	Campus Edition v. 3.8, WebCT Vista
Est. # of customers	2,600
Contact	David Rosenbaum, Director of Marketing
URL	http://www.webct.com

Organisation	Blackboard
Type/Mission	For-profit learning management system provider
Location	Washington, DC USA
Year Founded	1997
Financing	Over $100-million (USD)
Annual Sales	$16-million (USD) – 2nd quarter, 2002 (Private co.)
Products	Bb Learning System 5.51, plus multi-language version.
Est. # of customers	2,400
Contact	Chris Etesse, Senior Director of Technology
URL	http://www.blackboard.com

Overview

WebCT and Blackboard compete directly as the two dominant, for-profit providers of Learning Management Systems (LMS) software for universities and other educational institutions. Between WebCT and Blackboard, more than 5,000 institutions around the world run their software. In Australia approximately 65 institutions run WebCT and 40 run Blackboard.

LMS software has evolved over the past several years primarily to enable instructors to publish and manage online components to existing courses. The vast majority of WebCT and Blackboard customers utilise their LMS software in this way to supplement face-to-face learning environments and not to offer pure distance learning courses. As a result, WebCT and Blackboard offer only limited tools and solutions for managing the authentication of learners and ensuring the security and integrity of distance-learning environments. Online authentication, according to WebCT and Blackboard, consists primarily of maintaining open infrastructures to their LMS offerings which can interface with universities' existing Student Information Systems (SIS) which track registrations, enrolments, and other sensitive learner data.

WebCT

WebCT's Campus Edition v.3.8 and Vista enterprise LMS software are capable of integrating with institutions' existing authentication databases, including LDAP and Kerberos. The majority of client institutions have not enabled data-passing to their WebCT environment, instead choosing to import student enrolment data via paper printouts from SIS systems or comma-delimited files. One consequence of this lack of integration is that students can end up with multiple passwords and user IDs for each system on campus.

WebCT offers an online registration tool, however few clients use it as it can be used to register in specific classes but not to enrol at an institution for a degree. Moreover, WebCT's LMS cannot track credits of a degree program and cannot collect money and manage learner finances.

The WebCT LMS offers a range of distance learning tools to learners and instructors, including online quizzing, chatrooms, email communication and a digital drop-box for assignment submissions. These tools are all accessed through a standard user ID and password, though SSL can be implemented for the email client and grade book access. The testing environment allows instructors to create seven question types, randomise questions and answer orders and insert random variables into word problems. It is generally used for interim assessments and self-tests as WebCT believes it is impossible to adequately authenticate learners for high-stakes exams without using human supervisors.

WebCT's email application enables learners to send mail in two ways. Internal messages can be sent to all learners in a course and are neither encrypted nor digitally signed. Learners can also forward mail outside of the WebCT environment. WebCT captures a log of all activity within the LMS and archives every course, including emails, message boards, and chat logs for security purposes (logs can be checked at a later day to assist in the investigation of cheating and identity fraud). The digital drop-box, which delivers a time-stamp but no receipt for each submission, does not re-authenticate users to ensure the integrity of attached assignments. The LMS does track and archive all drop-box related events for security purposes. Results can be delivered through WebCT via an SSL interface with an automatic sign-off feature to protect learner data when accessed at computer labs, libraries, and other public venues.

WebCT has established its current authentication policies based on 'following the desires of its customers.' It sees three levels of fraud risk: learners who cheat in the learning process (i.e. impersonation), hacking into the LMS software, and the physical security of the servers. Online authentication is designed to counter the first risk, but WebCT views this as a near-impossible task. Instead, it believes instructional design that features a 'nuisance factor' is the greatest deterrent to fraud. If an online course has a single final assessment, then it is relatively simple to cheat. However, if the course has a range of requirements that take place on a weekly basis, 'you are not going to find someone to be you for a term.'

WebCT's five-year vision for online authentication includes maintaining its current policies and incorporating developments of the National Science Foundation Internet2[17]project, as well as additional use of SSL.

Blackboard

Blackboard Learning System 5.51 (soon moving to version 6) contains many of the same features and functionality as WebCT's offerings. It uses a Java authentication tool to communicate with institutions' authentication servers (e.g. LDAP), but only about 20 percent of Blackboard customers currently engage in any level of data integration with their SIS servers.

For the 80 percent of institutions that use Blackboard as a stand alone LMS, the software uses a standard user name and password with MD5 HASH encryption. The email client uses a Web front end that allows the learner to edit only the 'subject' and 'message' fields, making it difficult if not impossible to insert a false email address. Assignments are submitted to a digital drop box that generates a Web-based receipt page.

Blackboard's assessment tool is substantially similar to WebCT's. According to Chris Etesse, it's a 'middle of the road' testing tool that meets the needs of its users and can communicate with external assessment engines, but it is not designed to counter dishonesty. Blackboard believes the only way to ensure against cheating on assessments is via supervisors. The grade book feature allows an administrator to enable SSL as an option.

Like WebCT, Blackboard's LMS is generally installed on a dedicated server and managed by the customer's IT staff . As a result, the ultimate security and integrity of the system is dependent on the measures taken by each institution.

It is noteworthy that Blackboard has recently acquired the capability of managing campus-based financial transactions, student identification, dining services, building access, etc. via identification cards it creates as part of its Blackboard Transaction System. Blackboard offers a combined LMS and transaction system called the Community Portal System, which could have greater potential to incorporate stronger authentication systems for distance learning applications.

Five years into the future Etesse envisions a modified/new architecture that will include more APIs, enabling the platform to extend its flexibility to incorporate more sophisticated authentication systems. Among the initiatives he sees Blackboard developing compatibility with are Web ISO[18] and Shibboleth[19].

[17] See *Internet2* in the *Glossary* section of this paper.

[18] See *Web Initial Sign-on (WebISO)* in the *Glossary* section of this paper.

[19] See *Shibboleth Project* in the *Glossary* section of this paper.

3.3.2. University of Phoenix Online (UOPO)

Organisation	University of Phoenix Online
Type/Mission	For-profit online learning division Of University of Phoenix
Location	Phoenix, Arizona, USA
Year Founded	1989
Financing	N/A (public company – NASD: UOPX)
Annual Sales	$400-million (USD)
Degrees	11 accredited degree programs
Est. # of students	49,000
Contact	Russ Paden, Vice President, Academic Services
URL	http://www.phoenix.edu/

Overview

The University of Phoenix Online (UOPO) is the online division of the University of Phoenix, the largest and oldest (founded 1976) for-profit university in the United States. The University of Phoenix enrols more than 133,000 students, approximately 63 percent of whom attend classes at its 116 locations in North America. About 49,000 (37 percent) attend UOPO, completing courses and degrees entirely via the Internet. Degrees offered include bachelors, masters, and doctorates in the fields of business, technology, management, education, nursing, counselling, and criminal justice. The average UOPO student is 34 years old and is studying part-time.

UOPO is among the few accredited institutions that are successfully implementing a pure online-learning experience, delivering courses and degree programs for a rapidly growing student enrolment. Its approach is decidedly 'low-tech' by online education standards, utilising an asynchronous, email and Web-based interface. 'Authentication' is accomplished not through a technology solution but through required, regular communications between students and instructors and through instructional design of courses. Based on its enrolment figures and growth, it appears learners find UOPO's online approach more than satisfactory in delivering flexible learning.

UOPO Authentication Strategies

Learners register for UOPO via telephone at which time they receive an Individual Record Number than enables them to establish their own user ID and password on the UOPO website. During the registration process, the customer service representative plots out a calendar and schedule of courses so there is no need to call at the start of each course.

The UOPO learning approach is designed to replicate in an online environment, the practitioner model the company uses in its campus locations. Briefly, the faculty staff who work in their fields of expertise, teach online in the evenings. Students take five-week, sequential courses, that are highly participative, requiring communication five out of seven days each week. Typically instructors post lectures at the start of each week and students are required to comment and respond through the rest of the week.

Practically, UOPO's technology solution consists of Microsoft Exchange server software with Microsoft Outlook Express as the learner interface. Upon registering, learners receive a CD-ROM from UOPO that is pre-configured for installation on a personal computer. Prior to the start of the learner's first class, UOPO technical support calls to confirm correct installation of the software.

Each class functions like a small Usenet news group where up to 13 learners and one instructor engage in what amounts to a moderated discussion board. Learners can access the online message boards either via the Microsoft Outlook client installed on a local computer or via the Outlook Web client, which is accessible from any computer with a 28.8kbps connection to the Internet.

Learners are authenticated into the MS-Outlook environment with their self-set user name and password or online using SSL. All email postings are publicly viewable and learners are expected to engage in 'conversation' with their classmates. Assignments are posted as attachments to special folders in Outlook. No receipt is generated; instructors are trained to give quick feedback, including manual confirmation of receipt. Results are sent via private email to each learner, as are final grades. Learners can also print out grade cards online, which are not official transcripts but are generally adequate for obtaining corporate reimbursement of tuition costs.

UOPO does make use of the World Wide Web to deliver some additional materials to learners. It is moving away from physical textbooks and toward e-texts in PDF formats. It is also using a Web based Resource Center to deliver syllabi, self-test quizzes, links to relevant sites, and some supplemental multimedia materials.

The UOPO experience offers no anonymity for learners and no online testing. The five-week long, participatory course structure is intended to enable the instructor to 'hear' and identify each learner's written 'voice' from his submissions. Assessments are in the form of weekly, written team projects with final individual and team projects. Most projects are 'case-study' based.

According to Russ Paden, Vice President of Academic Services, the UOPO approach makes identifying cheating and plagiarism much easier than in a face-to-face setting. 'I see writing samples five to seven times per week. Unless they pay someone to be them for the entire course, they ca not cheat.' Paden estimates that he catches approximately 10 percent of his students plagiarising and assumes a similar rate amongst UOPO's other 6,600 faculty. While he notes plagiarism is rampant online, he says it is 'much easier to catch' than in a face-to-face setting. UOPO does not use plagiarism detection software but it does train its instructors to identify it and it requires its learners to agree to a 'Student Code of Responsibility.' All UOPO courses are archived for five years to facilitate investigations into fraud and cheating.

Overall, Paden is 'confident' that UOPO's authentication system is adequate based on the 'high levels of interaction' required between instructor and learner. The greatest risks of dishonesty are in submission of assignments, where he assumes some plagiarism sneaks past instructors, and the potential for 'malicious hacker types' to breach UOPO's servers. Five years into the future, he envisions UOPO may offer additional technology features, including synchronous tools. However, the core asynchronous, discussion based email groups that are time-zone insensitive will remain.

3.3.3. WestOne

Organisation	WestOne Services
Type/Mission	Division of the Department of Training and Employment WA
Location	Perth, WA, Australia
Year Founded	1998
Financing	N/A
Budget	$8-9 million
Online student enrolments	35-40,000 (est.)
Contact	Stuart Young, Director of WestOne Services
URL	http://www.westone.wa.gov.au/

Overview

WestOne Services was established in 1998 by the Department of Employment and Training in Western Australia to unite the Training Publications, TAFE Television and WestOne Online units. It reports directly to the director general and is a relatively autonomous organisation.

WestOne Online

The online component of WestOne Services serves as a clearinghouse for TAFE and RTO delivered courses, both online and face-to-face. In this regard WestOne acts in two capacities: it develops content – in the form of video, multimedia, and print – and technologies to enable and facilitate the delivery of VET materials to learners.

The current website is relatively old and not reflective of the depth of work WestOne has delivered to TAFEs and RTOs, according to Stuart Young, Director of WestOne services. Beyond the directories of available courses, WestOne has developed a set of technologies to facilitate the enrolment of VET learners in courses and improve the interface with institutions' existing technology infrastructures.

Enrolment

WestOne has built an online enrolment tool that enables learners to enrol in either short courses or award courses. To date, approximately eight TAFEs have implemented the short course online enrolment tool while two TAFEs are using the longer, award course version. WestOne has taken the important and necessary step of developing an interface to pass data between its enrolment tool and the College Management Information System (CMIS) used by all public/TAFE providers in Western Australia. Moreover, the tool is capable of processing payments by credit card, improving fee collection times. As a result, usage of the service has been substantial with 35-40,000 enrolments processed in the last 12 months. As an example, Challenger TAFE in Fremantle is processing 100 percent of its enrolments using the WestOne online registration tool, whether the learner is registering remotely or in person.

Online Course Authentication

When a learner enrols using the WestOne enrolment tool, a flag is raised if the course chosen utilises online materials. At that point, a user ID and password are automatically generated and emailed to the learner. The user ID is a variation of the learner's surname and the password is the learner's numerical birth date. Upon logging into the Learning Management System (LMS), learners are able to change their password.

The LMS licensed by WestOne for WA TAFEs is WebCT[20] To improve authentication into WebCT, WestOne has built an Identity Management System which extracts data from the TAFE's CMIS to Novell Direct XML. Using this technology makes it possible to automatically authenticate the learner into online resources, databases, and services on the TAFE network, effectively implementing 'single sign on' (SSO).

In WA VET, most courses are 'blended learning' meaning they combine online and face-to-face components. WestOne has not seen a need for, and is not currently pursuing, strategies for implementing complete online learning courses. Online assessment available through the WebCT LMS is only for self-testing, not for graded assessment. WestOne develops no assessment materials, relying on instructors to add assessment, which is normally done via a supervised exam, a written paper, competency based assessment or a combination of these tools.

The Future

Young envisions further development of the Identity Management System in the coming years. He expects the registration process to include a series of tick boxes for every type of electronically enabled service available at the institution, bringing the benefits of SSO to both learners and instructors.

WestOne is also looking into various types of storage cards that may be used for authentication and identification purposes and also to function as a 'passport' detailing competencies learned. Young envisions this happening most easily through a partnership with a sponsoring company.

A future challenge is the potential for the real authentication of human beings, which Young believes will incorporate some usage of biometrics. However, he believes such tools are too expensive right now and outside the practical framework of delivering solutions for 'blended learning.'

[20] See *3.3.1. WebCT / Blackboard* case study in this paper.

3.3.4. TAFE Tasmania

Organisation	TAFE Tasmania
Type/Mission	State-run technical and further education provider
Location	Hobart, Tasmania, Australia (HQ)
Year Founded	1998 - *TAFE Tasmania Act 1997* (Tas)
Financing	N/A
Budget	$80-million ($65-million 'government revenue')
Courses Offered	Over 500
Students	23,000 (13,000 Full Time Equivalents)
Contact	Peter Higgs, Manager, Learning & Business Tech. Andrew Meers, Educational Systems Officer
URL	http://www.tafe.tas.edu.au

Overview

TAFE Tasmania is the State of Tasmania's vocational, technical and further education provider. With seven campuses across the island, as well as on-site and customised curriculum delivery to workplaces and homes, and increasingly utilising the Internet, 'flexible delivery is the key to the Institute's operations.'

Learning and Business Technologies

TAFE Tasmania's Learning and Business Technologies group is responsible for developing online teaching and learning curricula as well as TAFE's delivery platform or Learning Management System (LMS). The LMS TAFE Tasmania currently employs is WebCT.[21]

Online Registration and Authentication

TAFE Tasmania's website currently offers links to three types of courses – the full TAFE course guide of award courses, short courses for specific skills, and online courses. The latter consist of 25 study units covering basic skills in general education, hospitality, and other areas. Approximately 300 additional study units are available online, mostly as part of the TAFE's award courses.

While the website contains information about all three types of courses, learners who want to enrol in an award course or a short course are only able to 'express interest' by clicking a link which sends a non-secure (unencrypted) inquiry to the relevant faculty. They are then contacted via telephone to begin the enrolment process for these face-to-face courses.

[21] See *3.3.1. WebCT / Blackboard* case study in this paper.

By contrast, learners can enrol in any of the 25 online study units by submitting an online application. A simple Web interface collects relevant personal information, which is passed to the online learning management staff for processing. The enrolment form is not a 'live' application as it cannot process credit card payments (and thus uses no encryption or other form of security) and is only used to deliver data to the TAFE, where it is then input into the student information system (SIS) (i.e. there is no database integration or data passing between the LMS and the SIS). By clicking the 'submit' button learners 'agree' to the following declaration:

> 'I accept that no results will be awarded in any course if my enrolment fees are not paid and that by clicking on the submit button I am certifying that all the details provided in this form are correct.'

The TAFE contacts the learner to complete the enrolment process, obtain payment details and generate an account with user name and password for the WebCT LMS. A handful of such enrolments are processed each week.

Over 300 students are currently enrolled in study units that are delivered completely online. Most of these form parts of award courses (i.e. are not part of the 25 online study units listed on the TAFE's site). An additional 700 or so are taking courses that incorporate 'blended learning' – that is, a combination of face-to-face instruction with some Web based curriculum delivery.

Assessment

Learners who are accessing TAFE Tasmania's online study units complete the entire unit online, including self-assessments that are delivered via the WebCT testing tool (see the WebCT case study). For those enrolled in 'blended learning' award or short courses, the online component delivers formative assessment but not summative assessment.

TAFE Tasmania is not 'overly concerned' with online cheating or fraud during formative assessment but takes summative assessment much more seriously, particularly for award courses. Its current solution for distance education students requires supervised assessment at a location of the learner's choice. The supervisor signs a statutory declaration that the learner is who they say they are and has received no assistance on the exam.

The Future

TAFE Tasmania's manager of Learning and Business Technologies, Peter Higgs believes that the greatest inhibitor to the uptake of flexible learning lies with instructors who are uncomfortable with the approach and concerned about authentication issues. He explains that while TAFE Tasmania's current system is functional, it uses a simple authentication system based on a pre-Internet, correspondence-course approach to distance learning, which can be easily abused.

Higgs points out that distance learning requires a higher level of maturity on the part of the learner to 'stick with a course and pursue the gain of knowledge honestly', but 'that does not mean flexible learners are less dishonest' than traditional TAFE students. He is hopeful that within five years, TAFE Tasmania will use biometric identification tools, but he believes that an intermediate step will probably include the issuance of some sort of identity card to learners.

Chapter 4. Flexible learning and electronic authentication

4.1. Motivation for electronic authentication in flexible learning

It is relevant to look at the motivation behind the adoption of electronic authentication in flexible learning environments. Although the momentum behind electronic authentication in flexible learning in Australia is recent, other jurisdictions, particularly the United Kingdom, have been considering the question of electronic authentication in this context for some time.

For example, a Joint Information Systems Committee (JISC) report[22] summarised the motivation behind the push for electronic authentication amongst academics involved in online learning initiatives. The report found that in the long term, there is a widespread view that greater security and authentication would be required. In particular, the following reasons for using security were noted :

- Academics wanting to 'practice what we teach';
- Allowing access from alternative locations (e.g. from home);
- Authentication for the purpose of making copyrighted material available to a target community;
- Authentication for administrative purposes (e.g. for people updating databases, directories or mailing lists);
- Authentication for controlling access to restricted resources, while other resources remain open to the public;
- Authentication in order to charge for document supply;
- Authentication to manage closed mailing lists;
- Cryptographic checksums of served data to prevent tampering and help detect illegal copying of resources;
- Encryption of electronic mailing lists;
- Prevent random passers-by from seeing unfinished work and gaining the wrong impression of a service;
- Restrict access to course material;
- Security against hacking attacks from the Internet; and
- Uniform access control and authentication mechanisms across information service providers.

[22] Joint Information Systems Committee (JISC), *Access Management Service for UK Higher and Further Education (Information Memorandum)* (2002) <http://www.jisc.ac.uk/index.cfm?name=funding_4_02>.

There has been no similar survey of the motives and expectations of Australian RTOs or other education institutions in relation to authentication. However, it can be expected that the experience in Australia will be similar to that in the United Kingdom. From the case studies and other research conducted during this paper, it appears that Australia institutions in the VET sector are interested in the use of authentication to enable remote access to courses and materials, and to assist in the prevention of cheating. The other potential uses of authentication are secondary.

4.2. Electronic authentication scenarios in flexible learning

It is beyond the scope of this paper to anticipate all of the likely uses of electronic authentication in the flexible learning environment. However, a number of major categories (and typical scenarios) can be identified.

4.2.1. Scenario 1 – Managing relationships between RTOs and service providers

In this scenario, electronic authentication could be used to assist in the relationship between an RTO (or multiple RTOs) and their various service providers (lecturers, tutors, assessors, content providers, supervisors etc.)

A similar system for electronic authentication (within a Public Key Infrastructure) has been developed for the Australian health sector – the Health eSignature Authority (HeSA).[23]

HeSA acts as a Registration Authority (RA) for the provision of digital keys and digital certificates across the entire health sector. (HeSA is a Gatekeeper accredited wholly owned subsidiary of the Health Insurance Commission).

Since February 2001, HeSA has supplied digital keys and digital certificates to a variety of professions and organisations in the health sector. PKI has subsequently been used to transfer information between GPs and specialists, practitioners and hospitals, GPs and Divisions of General Practice. The Health Insurance Commission uses PKI for all its new Electronic Data Interchange (EDI) and e-business solutions.

It is important to note that this system does not include the electronic authentication of patients – merely the electronic authentication of all other health sector participants (hospitals, health professionals, laboratories, insurers, Divisions of General Practice etc.). This is analogous to the use of electronic authentication in the VET sector for TAFEs, RTOs, teachers, tutors, service providers, funders etc., but not for individual learners.

4.2.2. Scenario 2 – Mix of student administration and learning

In this scenario, electronic authentication could be used for a mix of both student administration applications and learning applications. The number of applications which utilise electronic authentication could be large, and it is likely the authentication infrastructure would include a multi-function smart card or token.

[23] <http://www.hesa.com.au>.

A useful case study of this approach is the *University of California – Common Authentication Project*. Although this is a research project rather than a practical implementation (the practical implementation is currently stalled), the overall vision and concept provides useful guidance.

The University of California (UC) considered a university wide PKI system to allow UC to 'speak with one voice when developing agreements for use of its digital credentials'[24]. The University saw PKI as fulfilling the following roles:

- **Access to licensed or otherwise restricted content**
  Areas where both authentication and authorisation will be important include access to university enterprise directories, data warehouses and records.

- **Student and Employee "Self Service" applications**
  Increasingly institutions turn to individuals to retrieve their personal information themselves and/or maintain such information through web interfaces rather than paper forms. Access to personal information must be managed so that only the individual subject or qualified university staff can view and/or modify such data. In some cases audit logs must be maintained that reliably indicate the individual who performed a retrieval or modification. In highly sensitive cases it may be necessary to require a digital signature in order to conclude a transaction.

- **Electronic commercial transactions with external partners**
  Commercial transactions over the network may occur with a large variety of partners and may cover a wide range of financial values. Strong digital credentials that result in appropriate validation of responsibility are essential to make this activity scalable as well as auditable. The university's digital credentials must be recognised by external partners.

- **Data security**
  It is critical that sensitive information be protected against inappropriate interception while in transit across networks and/or retrieval when in storage. Asymmetric encryption ensures that only the intended recipient can decrypt and view the data. Exchange of student records is one area where this protection is required. Other areas include employee data and evaluations, research data, and university strategic plans.

- **Exchange of student or other sensitive records among institutions**
  The University both accepts student transcripts from other schools and provides transcripts to other schools. Such documents must be signed by an authorised official and protected in transit from inappropriate interception. PKI technology can accomplish both.

- **Student loan application and management**
  The application for and management of student loans requires authentication of the student to the university and the lender(s).

[24] University of California Office of the President, *Why UC Must Invest in a Public Key Infrastructure (PKI): The Case for Digital Certificates* (May 2000) <http://www.ucop.edu/irc/auth/whypki.pdf>.

— **Integrity of on-line content, systems and web pages**
A large amount of information is available over the network but there is essentially no assurance that the information a reader sees is what was originally made available. Digitally signing on-line documents can allow readers to validate the integrity of those documents.

— **Access to IT-based services**
Access to administrative information processing systems and services must be managed appropriately. Today this is done most commonly with individual IDs and passwords. A PKI-based credential system could enable a 'single sign on' method for all campus systems.

— **Digital records: notary, retention and archive**
The university must keep certain records for defined periods of time, or sometimes indefinitely. Today many original records are in digital form, for example electronic memos, documents, or transaction records. There must be an appropriate way to archive and retrieve such records without resorting to printing them and filing the paper copy. The use of PKI digital signatures can enable a robust digital archiving system.

These applications could be implemented in the VET sector to assist in the development of flexible learning. Students could receive their digital certificates from one of the institutions with which they were studying, or from a central agency.

4.2.3. Scenario 3 – Cross recognition of qualifications

In this scenario, electronic authentication could be used as a tool to assist in the cross recognition of qualifications and part-qualifications.

Institutions are often required by State/Territory VET legislation[25] to provide cross recognition of qualifications which form part of the national curriculum. In order to do this, institutions need to have trust and confidence in the identity of the student, the authentication of the qualifications, and the currency of those qualifications.

In practice, authentication of qualifications could be achieved in several of the Authentication Models discussed in *Chapter 8. Models for electronic authentication in VET*. Electronic authentication could improve trust in cross recognition. It is important to note that the improved trust will only relate to the evidence of the qualification – it may not improve trust in the qualification itself.

[25] See *5.1.9.* in this paper.

4.2.4. Scenario 4 – Skills passport

In this scenario, a skills passport could involve the development of a system or device which combines all of the elements of the previous three scenarios into a national, student centred scheme which includes an electronic authentication layer.

As discussed in *Chapter 1. Introduction* ANTA is investigating the development of a skills passport, and has been considering the role of a skills passport within wider strategic discussions. The following quote from *Shaping Our Future – National Strategy Discussion Starter*[26] outlines the current strategic thinking on this issue:

> 'The national system encourages and enables continuous learning and assessment of competence, leading us to reflect on the traditional nature of qualifications (issued at the end of a complete study program or, in the case of Training Packages, a group of competency standards comprising a qualification). While the system does award a statement recognising attained competencies that don't add up to a full qualification, research indicates that people want a quality and user-friendly statement (recording their competencies and learning through life) that they can show to potential employers. This statement could take the form of a 'skills passport' or an electronic smart-card. This would be particularly useful for the increasing number of people who don't want full qualifications but small numbers of competencies related to current work challenges, as well as people whose circumstances lead them to drop in and out of structured learning. Many people choose a smorgasbord approach to learning (through self-assembly of smaller, shorter, targeted chunks). The frameworks now need to recognise this. Also, while assessment in a competency-based system, logically, results in a learner being declared 'competent' or 'not yet competent', market research indicates that learners want richer recognition of their performance; and that employers want that, too. Successful learners want to stand out from the crowd. Is it time that we had a 'skills passport' type statement of competence and a way of reporting achievement that allows for recognition of excellence?'[27]

Similar discussions are occurring in other jurisdictions. For example, the *IMS Global Learning Consortium Project*[28] envisages the development of a skills passport. The *IMS Project* defines and delivers interoperable specifications for exchanging learning content and information about learners among learning system components. IMS members (including several education institutions in Australia) adopt these specifications to make learning easier to deliver anywhere and anytime. IMS specifications may become the de facto global standards for delivering flexible learning products and services, especially electronic authentication.

---

[26] Australian National Training Authority, *A discussion starter for the next national strategy for vocational education and training 2004-2010 (January 2003)* <http://www.anta.gov.au/images/publications/National_strategy-discussion_starter.pdf>.

[27] Ibid, page 16.

[28] <http://www.imsproject.org>.

The IMS protocols support the following categories of learner information:

- **Education record**
  The record of educational achievement from school through to college/university. The different education systems throughout the world need to be supported.
- **Training log**
  The record of training activities undertaken - e.g. courses carrying formal certification.
- **Professional development record**
  The record of professional development activities undertaken including membership in the appropriate professional bodies.
- **Resume/CV**
  A record of personal achievement that includes relevant work experience, qualifications and education history. Different types of resumes need to be supported - e.g. business, academic, medical, etc.
- **Life-long learning record**
  A cradle-to-grave record of the learning activities and achievements of an individual. The time-related nature of the record is reflected by the sequential nature of the information and the tagging of the specific record by its date of entry.
- **Community service record**
  A record of the community-oriented activities of an individual and the corresponding work and training experience.

A national skills passport containing all of these fields could provide learners with a convenient method of carrying their qualifications using the same system/token[29] they use for accessing flexible learning.

[29] Such as a smart card.

Chapter 5. The current legal and regulatory framework for electronic authentication in Australia

This chapter examines the existing legal and regulatory framework in three categories:

- Legislation;
- Guidelines and codes; and
- Common law.

5.1. Relevant legislation

5.1.1. Electronic Transactions Act 1999 (Cth)

The *Electronic Transactions Act 1999 (Cth)*[30] (ETA) provides businesses and individuals with the option of using electronic communications when dealing with government agencies. See *6.4. Electronic formation of contracts* in this paper for further discussions of the ETA.

This law states that transactions taking place under a law of the Commonwealth will not be invalid just because they are completed electronically. The ETA applies to all laws of the Commonwealth unless specifically excluded by the *Electronic Transactions Regulations 2000 (Cth)*[31] (most education applications are unlikely to be excluded).

The ETA is based on two principles:

- **1. Functional equivalence**
  Paper documents and electronic transactions are treated equally by the law.
- **2.Technology neutrality**
  The law does not discriminate between different forms of technology.

The ETA allows businesses to fulfil, in electronic form, any of the following legal requirements:

- **Giving information in writing**
  For example, a student's written application for special consideration following illness.
- **Providing a handwritten signature**
  For example, signing a student loan application.
- **Producing a document in material form**
  For example, providing a hard copy transcript of qualifications obtained.
- **Recording or retaining information**
  For example, retaining copies of submitted assessment.

---

[30] <http://scaleplus.law.gov.au/html/pasteact/3/3328/top.htm>.

[31] <http://scaleplus.law.gov.au/html/pastereg/3/1579/top.htm>.

The ETA stipulates a uniform method for attributing the time and place of dispatch and receipt of electronic communications. This can be important in many transactions and may be of significance in the submission of assessments in an education environment – particularly where late penalties apply.

Generally, a contract is taken to have been formed at the place where acceptance of the offer to transact is received. The ETA provides that receipt of an electronic communication occurs at the *place of business* of the addressee or, if the addressee does not have a physical place of business, at the addressee's ordinary place of residence. The time of receipt is the time when the electronic communication *enters an information system* designated by the addressee. If no such system has been designated, then an electronic communication is received when it comes to the attention of the addressee.

Under the Act, a range of electronic 'time-stamping' methods could be used by RTOs to determine the exact time and date of submission of assessment. However, some guidance or standards (or indeed the electronic time-stamping tools themselves) could be provided by ANTA or a similar body.

In order to achieve national uniformity all States and Territories have passed Electronic Transactions Acts that complement the Commonwealth's ETA. This layer of state legislation therefore covers private sector transactions.

- Australian Capital Territory – *Electronic Transactions Act 2001 (ACT)*[32]
- New South Wales – *Electronic Transactions Act 2000 (NSW) No 8* [33]
- Northern Territory – *Electronic Transactions Act 2001 (NT)*
- Queensland – *Electronic Transactions Act 2001 (Qld)*[34]
- South Australia – *Electronic Transactions Act 2000 (SA)*[35]
- Tasmania – *Electronic Transactions Act 2000 (Tas)*[36]
- Victoria – *Electronic Transactions Act 2000 (Vic)*[37]
- Western Australia – *Electronic Transactions Bill 2001(WA) No 38* not yet enacted[38]

[32] <http://www.legislation.act.gov.au/a/2001-10/default.asp>.

[33] <http://www.legislation.nsw.gov.au/fullhtml/inforce/act+8+2000+FR+0+N>.

[34] <http://www.legislation.qld.gov.au/LEGISLTN/ACTS/2001/01AC042.pdf>.

[35] <http://www.parliament.sa.gov.au/dbsearch/acts-list.htm>.

[36] <http://www.thelaw.tas.gov.au/view/75++2000+AT@EN+2002112600>.

[37] <http://www.dms.dpc.vic.gov.au/l2d/E/ACT02321/>.

[38] As at 11 February 2003 the *Electronic Transactions Bill 2001(WA)* is not yet enacted. See <http://www.parliament.wa.gov.au/parliament/bills.nsf/2eb57164d5f552f448256adc00255c5f?OpenView&Start=30> for more information

5.1.2. Privacy Act 1998 (Cth) – Commonwealth Public Sector requirements

The *Privacy Act 1988 (Cth)*[39] was introduced shortly after a high profile national debate on a proposal to introduce a national identification card – the Australia Card. The Australia Card proposal was abandoned in 1987. A lengthy public debate raised awareness of privacy issues, and assisted in the development of Australian privacy legislation, which was initially quite limited in its scope.

Section 14 of the Act contains a set of Information Privacy Principles (IPPs) which apply to the handling of personal information by Commonwealth Government agencies.

The Commonwealth IPPs are:

- **Principle 1** – Manner and purpose of collection of personal information
- **Principle 2** – Solicitation of personal information from individual concerned
- **Principle 3** – Solicitation of personal information generally
- **Principle 4** – Storage and security of personal information
- **Principle 5** – Information relating to records kept by record-keeper
- **Principle 6** – Access to records containing personal information
- **Principle 7** – Alteration of records containing personal information
- **Principle 8** – Record-keeper to check accuracy etc. of personal information before use
- **Principle 9** – Personal information to be used only for relevant purposes
- **Principle 10** – Limits on use of personal information
- **Principle 11** – Limits on disclosure of personal information

[39] <http://scaleplus.law.gov.au/html/pasteact/0/157/top.htm>.

5.1.3. Privacy Act 1988 (Cth) – Private sector requirements

In December 2000, the *Privacy Amendment (Private Sector) Act 2000 (Cth)*[40] was passed through Federal Parliament. This amended the *Privacy Act 1988 (Cth)*, which applied primarily to public sector agencies. As a result of the amendments, which came into force on 21 December 2001, the National Privacy Principles (NPPs) contained in *Schedule 3*[41] of the *Privacy Act 1998 (Cth)* apply to the private sector.

However, the National Privacy Principles do not apply to businesses with an annual turnover of $3 million or less, unless those businesses:

- Choose to 'opt-in' voluntarily;
- Trade in personal information;
- Provide a health service and hold health information; or
- Provide contractual services to the Commonwealth.

Some RTOs will be small enough to qualify for the small business exemption[42]. However, many of these will be required to comply with privacy laws as part of their funding contracts. It is considered best practice to comply with the National Privacy Principles.

The National Privacy Principles (NPPs) are:

- **Principle 1** – Collection
- **Principle 2** – Use and disclosure
- **Principle 3** – Data quality
- **Principle 4** – Data security
- **Principle 5** – Openness
- **Principle 6** – Access and correction
- **Principle 7** – Identifiers
- **Principle 8** – Anonymity
- **Principle 9** – Transborder data flows
- **Principle 10** – Sensitive information

[40] <http://scaleplus.law.gov.au/html/comact/10/6269/top.htm>.

[41] <http://scaleplus.law.gov.au/html/pasteact/0/157/0/PA002310.htm>.

[42] Department of Employment, Workplace Relations and Small Business, *Is your small business exempt?* (June 2001) <http://www.industry.gov.au/library/content_library/Privacy_brochure.pdf>. A useful guide to whether or not the exemption applies to a small business.

The NPPs differ slightly from the IPPs. In particular, they include two new principles which may be relevant to flexible learning and electronic authentication:

- **NPP 7 – Identifiers**
  An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by a government agency. In practice this would exclude using a tax file number, driver licence, passport number, Medicare number or any similar government identifier, as the RTO's student identification number.

- **NPP 8 – Anonymity**
  Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation. In practice, this means that identification should not be a requirement of every online transaction. Some basic inquiries and downloads should be available on an anonymous basis. However, in the education sector it will be 'reasonable' to require identification in most transactions and interactions.

5.1.4. State privacy legislation – Privacy and Personal Information Protection Act 1998 (NSW)

Since 1998, a set of Information Privacy Principles (IPPs) contained in *Part 2 Division 1* of the *Privacy and Personal Information Protection Act 1998 (NSW)*[43] have applied to the handling of personal information by NSW Government agencies.

The NSW Information Privacy Principles (IPPs) are:

- **Principle 1** – Collection of personal information for lawful purposes
- **Principle 2** – Collection of personal information directly from individual
- **Principle 3** – Requirements when collecting personal information
- **Principle 4** – Other requirements relating to collection of personal information
- **Principle 5** – Retention and security of personal information
- **Principle 6** – Information about personal information held by agencies
- **Principle 7** – Access to personal information held by agencies
- **Principle 8** – Alteration of personal information
- **Principle 9** – Agency must check accuracy of personal information before use
- **Principle 10** – Limits on use of personal information
- **Principle 11** – Limits on disclosure of personal information

[43] <http://www.legislation.nsw.gov.au/fullhtml/inforce/act+116+2002+FIRST+0+N>.

5.1.5. State privacy legislation – Information Privacy Act 2000 (Vic)

Victorian public sector organisations (including government organisations, statutory bodies and local councils) are subject to the *Information Privacy Act 2000 (Vic)*[44] which came into full effect on 1 September 2002. Organisations performing work for Victorian government may also be subject to the Act, depending on the particular contract.

The Act requires public sector organisations (with some limited exceptions) to comply with ten Information Privacy Principles (IPPs) or have an approved code of practice. Health information is not governed by the Act and is the subject of separate legislation. Privacy Victoria[45] is the Office of the Victorian Privacy Commissioner, an independent statutory office established pursuant to the Act, which has authority to administer and enforce the Act and to investigate and conciliate complaints. Disputes which cannot be resolved may be referred to the Victorian Civil and Administrative Appeals Tribunal (VCAT) which can offer a number of remedies, including requiring the organisation to make an apology, correct or delete personal information or pay compensation.

5.1.6. State privacy legislation – Queensland

It is expected that Queensland will introduce state privacy legislation within the next five years.

Currently, Queensland has an administrative privacy regime based on *Queensland Information Standard 42 – Privacy*[46]. This standard applies to all Queensland Government agencies and while it does not have the full force of law it seems to have achieved widespread compliance. The core of IS42 is a set of Information Privacy Principles which mirror the Commonwealth IPPs.

5.1.7. State privacy legislation – Other

Gradually, most states will introduce privacy legislation and consensus may develop about which set of 'principles' should be included in each state's legislation. However, the situation may remain fractured for many years.

5.1.8. Cybercrime Act 2001 (Cth)

Agreement has been reached between the Commonwealth and the States and Territories to implement new laws to address shortcomings in existing computer offences. The *Cybercrime Act 2001 (Cth)*[47] outlaws activities such as the unauthorised access of commercial or confidential information, spreading computer viruses and trading in technology that is designed to either hack into or damage another person's computer.

This legislation will be relevant for some forms of cheating in the online learning environment – especially where hacking or theft of documents (e.g. exams) from online sources is involved.

The *Cybercrime Act 2001 (Cth)* and the mirror State legislation criminalise harmful technology assisted activities, such as producing a destructive virus, hacking and cracking. It also imposes heavy penalties on offenders and increases police powers of investigation.

---

[44] <http://www.dms.dpc.vic.gov.au/l2d/l/ACT01911>.

[45] <http://www.privacy.vic.gov.au>.

[46] <http://www.iie.qld.gov.au/comminfo/guidelines.asp>.

[47] <http://scaleplus.law.gov.au/html/pasteact/3/3486/top.htm>.

In NSW the *Crimes Amendment (Computer Offences) Act 2001 (NSW)*[48] was enacted which replicated the provisions of the Commonwealth legislation. Certain sections also have extra-territorial application, recognising the fact that the effect of many computer crimes are not felt in the same state or even country from which they originate (*s 308C(3)* and *s 308F(2)(b)*).

5.1.9. VET legislation

The VET sector works within a complex framework of Commonwealth and State/Territory legislation dealing with the recognition of qualifications, training requirements, funding arrangements and administration. The relevance of VET legislation for electronic authentication issues is limited, although the legislation does provide a useful framework and context for developments in the sector.

Recently, legislation has been enacted (or is being considered) regarding the establishment of Qualification Authorities, which could play an important role in any future electronic authentication implementations (e.g. as repositories for records of qualifications).

The following table lists the main Commonwealth and State/Territory VET legislative instruments.

[48] <http://www.legislation.nsw.gov.au/fullhtml/inforce/act+20+2001+FIRST+0+N>.

Jurisdiction	Acts relating to vocational education	Acts relating to qualification authority	Name Of Act(s)
Commonwealth	yes	no	*Vocational Education and Training Funding Act 1992 (Cth)*[49]
ACT	yes	no	*Vocational Education and Training Act 1995 (ACT)*[50] *Vocational Education and Training Regulations 1998 (ACT)*[51]
New South Wales	yes	no	*Vocational Education and Training Accreditation Act 1990 (NSW)*[52]
Northern Territory	no	no	
Queensland	yes	no	*Vocational Education and Training (Industry Placement) Act 1992 (Qld)*[53] *Vocational Education, Training and Employment Act 1991 (Qld)*[54]
South Australia	yes	no	*Vocational Education, Employment and Training Act 1994 (SA)*[55]
Tasmania	yes	no	*Vocational Education and Training Act 1994 (Tas)*[56]
Victoria	yes	yes	*Vocational Education and Training Act 1990 (Vic)*[57] *Victorian Qualifications Authority Act 2000 (Vic)*[58]
Western Australia	yes	no	*Vocational Education and Training Act 1996 (WA)*[59]

[49] <http://scaleplus.law.gov.au/html/pasteact/0/421/top.htm>.

[50] <http://www.legislation.act.gov.au/a/1995-37/current/pdf/1995-37.pdf>.

[51] <http://www.legislation.act.gov.au/sl/1998-26/current/pdf/1998-26.pdf>.

[52] <http://www.legislation.nsw.gov.au/fullhtml/inforce/act+120+1990+FIRST+0+N>.

[53] <http://www.austlii.edu.au/au/legis/qld/consol_act/veatpa1992508>.

[54] <http://www.austlii.edu.au/au/legis/qld/consol_act/vetaea1991434>.

[55] <http://www.austlii.edu.au/au/legis/sa/consol_act/veeata1994434>.

[56] <http://www.thelaw.tas.gov.au/view/88++1994+GS1@EN+2003021000>.

[57] <http://www.dms.dpc.vic.gov.au/l2d/V/ACT01268>.

[58] <http://www.dms.dpc.vic.gov.au/l2d/V/ACT01971>.

[59] <http://www.austlii.edu.au/au/legis/wa/consol_act/veata1996306>.

5.2. Relevant guidelines and codes

5.2.1. Office of the Federal Privacy Commissioner (OFPC) Guidelines – PKI and Privacy

The *Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to communicate or transact with individuals*[60] were published by the Office of the Federal Privacy Commissioner (OFPC) in December 2001 with the purpose of 'identifying privacy risks associated with PKI and to set out guidance for Commonwealth and ACT agencies where they provide services to individuals using PKI'.[61] The Guidelines aim to protect the privacy of users by providing PKI facilities that allow secure and confidential transmissions. The guidelines emphasise the need to carefully research the appropriateness of using PKI, including careful consideration of the issues and risks involved. PKI is only intended to be used after such research and when the user is able to make an informed decision.

The guidelines are:

- **Guideline 1** – Agency Client Choice on the Use of PKI Applications
- **Guideline 2** – Awareness and Education
- **Guideline 3** – Privacy Impact Assessments (PIAs)
- **Guideline 4** – Evidence of Identity
- **Guideline 5** – Aggregation of Personal Information
- **Guideline 6** – Single or Multiple Digital Certificates
- **Guideline 7** – Subscriber Generation of Keys
- **Guideline 8** – Public Key Directories
- **Guideline 9** – Pseudonymity and Anonymity

These requirements are discussed in more detail in *5.3. Electronic authentication and privacy requirements.*

[60] Office of the Federal Privacy Commissioner, *Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to communicate or transact with individuals* (December 2001) <http://www.privacy.gov.au/publications/pki.rtf>.

[61] Ibid., page *5.*

5.2.2. Office of the Federal Privacy Commissioner (OFPC) Guidelines – National Privacy Principles (NPPs)

The OFPC's *Guidelines to the National Privacy Principles*[62] were released in September 2001 and are designed to assist businesses comply with the NPPs. It is a thorough document which details the context in which the NPPs are designed to operate, and explains the key underlying concepts of the NPPs. As the NPPs do not universally apply to all businesses, the guidelines also list the criteria involved in determining whether a businesses needs to comply with the NPPs. The most important feature of the OFPC's *Guidelines to the NPPs* is that they outline the obligations that arise under each NPP as well as tips for compliance, and methods of avoiding interfering with an individual's privacy.

In addition to the guidelines, the OFPC has also published numerous *Information Sheets*[63], some on the IPPs in general and some on specific NPPs. Titles include:

- Overview of the Private Sector Provisions;
- Openness;
- Access and Correction;
- Access and the Use of Intermediaries;
- Security and Personal Information;
- Unlawful Activity and Law Enforcement; and
- Coverage of and Exemptions from the Private Sector Provisions.

5.2.3. Gatekeeper requirements – General

The Government's Gatekeeper strategy deals with the accreditation of parties in a Public Key Infrastructure. Different participants in the Gatekeeper strategy (e.g. CAs and RAs) have different standards and criteria for registration.[64]

The requirements are too lengthy, technical and detailed to describe in this paper. The following list of key documents is provided for general guidance:

General

- Evaluation Criteria and Contacts
- Gatekeeper Accreditation Dependencies Chart
- Gatekeeper Accreditation Dependencies Table
- Gatekeeper X.509 Digital Certificate and Certificate Revocation List (CRL) Profiles
- Gatekeeper Processing Implementation Conformance Statement (PICS) Proforma

---

[62] Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (September 2001) <http://www.privacy.gov.au/publications/nppgl_01.html>.

[63] <http://privacy.gov.au/publications/>.

[64] National Office for the Information Economy, *Gatekeeper Accreditation Information* <http://www.noie.gov.au/projects/confidence/Securing/GatekeeperAccreditation.htm>.

Certification Authorities

- Concept of Operations – Evaluation Criteria
- Criteria for Accreditation of Certification Authorities
- CA/RA Operations Manual Evaluation Criteria

Registration Authorities

- Concept of Operations – Evaluation Criteria
- CA/RA Operations Manual Evaluation Criteria

Legal

- Model Certificate Policy
- Glossary to the Model Certificate Policy
- Gatekeeper Certification Authority Head Agreement

5.2.4. Gatekeeper requirements – Privacy

In May 2000 the privacy recommendations[65] made by the Government Public Key Authority to the CEO, Office for Government Online were included in the Gatekeeper accreditation requirements. The recommendations relate specifically to situations where a client of a Commonwealth agency is using a digital signature certificate in an online transaction with the agency.

The recommendations cover:

- Multiple use of key-pairs or digital certificates;
- Key-pair generation;
- Personal choice as to issuers of digital certificates and tokens;
- Personal possession and control of tokens;
- Pseudonymity;
- Key revocation;
- Non-intrusive identification processes;
- Centralised storage of identification details; and
- Freedom from appropriation and cancellation of identity.

These requirements are discussed in more detail in *5.3 Electronic authentication and privacy requirements.*

[65] <http://www.noie.gov.au/projects/confidence/Securing/Gatekeeper_privacy_recommendations_May2000.htm>.

5.2.5. Smart Card Code of Conduct

The *Asia Pacific Smart Card Forum Code of Conduct*[66] was first envisaged in 1995 and published in 1997. It remains the world's only comprehensive smart card code of conduct, and about 70 organisations have signed.

The Code serves three functions. The first is to provide a Code for members of the Smart Card Forum where no industry specific code is developed. The second is to provide minimum standards which must be observed in industry specific codes. The third is to provide the basis upon which Code Subscribers can use a 'compliance logo.'

The Code is voluntary and is administered by a small code advisory committee and a sanctions committee. It contains:

- Privacy provisions;
- Security provisions;
- Access and correction rights;
- Special requirements for terms and conditions;
- Provisions for loss and misuse of cards;
- Provisions regarding advertising; and
- Complaints procedures.

The role of the Smart Card Code in electronic payment systems will be greatly reduced following the introduction of the revised EFT Code (see *5.2.6.*), which contains a specific section (Part B) covering stored value products, including stored value smart cards. However, the Smart Card Code may have ongoing relevance for other smart card applications in the VET sector (e.g. the use of smart cards to carry digital signature certificates and the use of smart cards as student cards).

5.2.6. Electronic Funds transfer (EFT) Code of Conduct

The *Electronic Funds Transfer Code of Conduct*[67] is the main regulatory instrument in Australia for providing consumer protection in electronic payment systems. The *EFT Code* was the subject of a lengthy review, chaired by the Australian Securities and Investments Commission (ASIC). The *EFT Code* review working group issued two discussion papers[68] and a final version of the revised *EFT Code* was published in April 2001.

The revised *EFT Code* covers any business to consumer electronic transfer of value. Business to business electronic transfers of value will be excluded where the product being used was intended primarily for business use.

---

[66] <http://www.smartcardforum.asn.au/code.htm>.

[67] <http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/eft_code.pdf/$file/eft_code.pdf>.

[68] Australian Securities and Investments Commission, *Second Draft Expanded EFT Code of Practice and Commentary* (January 2000) <http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/eftcode_draft2.pdf/$file/eftcode_draft2.pdf> and *July 1999 Discussion Paper* <http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/fineft.pdf/$file/fineft.pdf>.

An 'electronic transfer of value' includes coverage of credit cards in some circumstances, but not where a handwritten signature is obtained. It includes EFTPOS, ATM transactions, most Internet and telephone banking transactions, direct debits and direct transfers.

Stored value products, such as electronic purses and stored value smart cards, are now included in a new section of the *EFT Code – Part B*.

Specific requirements of the *EFT Code* stipulate that:

- Terms and conditions must be provided to consumers;
- Records of transactions must be available to consumers;
- Audit trails must be kept;
- Privacy provisions mirroring the new federal privacy legislation for the private sector must be complied with, plus some specific EFT industry privacy guidelines; and
- Complaint investigation and resolution procedures must be in place.

Of course, the most important section of the previous *EFT Code* was the section apportioning liability for unauthorised transactions. This section has been completely updated and revised, and includes coverage of:

- Access methods;
- Security and disguise of codes;
- Contribution to loss;
- Fraud and negligence;
- Lost and stolen cards or devices; and
- System or equipment malfunction.

While the *EFT Code* is voluntary, the vast majority of payment system providers in Australia are members. Any electronic payment systems used in the VET sector (for payment of staff, procurement of content, collection of student fees etc.) are therefore likely to be covered by the *EFT Code*.

5.2.7. Biometrics Code of Conduct

There is no specific regulation of biometrics in Australia. The Biometrics Institute[69] has indicated a desire to prepare a Code (mainly to cover privacy issues) in the near future. However, at the time of writing, there is no timetable for the development of this code.

[69] <http://www.biometricsinstitute.org/>.

5.3. Electronic authentication and privacy requirements – Summary table

This table sets out each step in a typical electronic authentication process in the left hand column. The other columns represent the current legal requirements for protecting privacy at each step. For most organisations in the VET sector it will be necessary to comply with one or more of the columns, so it is useful to present the requirements in this format to avoid gaps and overlaps in compliance.

In this example the RTO authenticates the learner for a variety of purposes (administration, payment, student identification, access to materials etc.) and the learner may choose to select additional useful applications (library access, student club membership etc.).

Authentication Example (User Steps)	Information Privacy Principles (Cth Agencies and outsourced contracts)[70]	National Privacy Principles (Private Sector)[71]	Gatekeeper Related Requirements[72]	OFPC PKI Guidelines[73]
Choice of authentication If PKI, the user can also choose an issuer of a digital certificate (or issuers of digital certificates)			GK 10 – Multiple digital certificates GK Supplementary C – Personal Choice as to Issuers of Digital Certificates and Tokens	Guideline 1 – Agency Client Choice on the Use of PKI Applications
Accept Terms and Conditions The learner will consider and agree to the terms and conditions of use.			GK Supplementary I – Freedom from Appropriation and Cancellation of Identity	Guideline 2 – Awareness and Education
Present Identification The learner will present proof of identification documents (where appropriate).	IPP 1 – Manner and purpose of collection of personal information	NPP 1 – Collection	GK Supplementary H – Centralised Storage of Identification Details	Guideline 4 – Evidence of Identity .
Generate Key Pair (PKI only) The learner will generate a key pair.			GK Supplementary B – Key-Pair Generation	Guideline 7 – Subscriber Generation of Keys

[70] Office of the Federal Privacy Commissioner, *Guidelines to* Information *Privacy Principles* (October 1994) <http://www.privacy.gov.au/government/guidelines>.

[71] Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy* Principles (September 2001) <http://www.privacy.gov.au/publications/nppgl_01.html>.

[72] National Office for the Information Economy, *Gatekeeper Accreditation Information* <http://www.noie.gov.au/projects/confidence/Securing/GatekeeperAccreditation.htm>.

[73] Office of the Federal Privacy Commissioner, *Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to communicate or transact with individuals* (December 2001) <http://www.privacy.gov.au/publications/pki.rtf>.

Authentication Example (User Steps)	Information Privacy Principles (Cth Agencies and outsourced contracts)[70]	National Privacy Principles (Private Sector)[71]	Gatekeeper Related Requirements[72]	OFPC PKI Guidelines[73]
Note 1 None of the above process should result in the same unique identifier being used as one already allocated by a Cth Agency.		NPP 7 – Identifiers		
Choose Digital Certificate (PKI only) The learner will then consider an application and choose an appropriate digital certificate.			GK Supplementary A – Multiple Use of Key-Pairs or Digital Certificates	Guideline 6 – Single or Multiple Digital Certificates.
Provide Information The learner will provide information to the RTO (or other relying party).	IPP 1 – Manner and purpose of collection of personal information IPP 2 – Solicitation of personal information from individual concerned IPP 3 – Solicitation of personal information generally	NPP 1 – Collection	GK 01 – Manner and extent of collection of personal information GK Supplementary G – Non-Intrusive Identification Processes	
Note 2 At or before this stage, where appropriate, anonymous or pseudonymous options for learners should be made available.		NPP 8 – Anonymity	GK 12 – Support of anonymous or pseudonymous digital certificates GK Supplementary E – Pseudonymity	Guideline 9 – Pseudonymity and Anonymity
Directory Check (PKI only) A directory check may now take place to obtain the public key, or to confirm the authentication, or to confirm some particular attribute.			GK 09 – Privacy protection is provided for personal information published in publicly accessible lists / registers	Guideline 8 – Public Key Directories .
CRL Check (PKI only) A check may now be made against a Certificate Revocation List (CRL)			GK 09 – Privacy protection is provided for personal information published in publicly accessible lists / registers	

Authentication Example (User Steps)	Information Privacy Principles (Cth Agencies and outsourced contracts)[70]	National Privacy Principles (Private Sector)[71]	Gatekeeper Related Requirements[72]	OFPC PKI Guidelines[73]
Application to Proceed The application will now proceed. Depending on the application some personal information may now be used or disclosed.	IPP 9 – Personal information to be used only for relevant purposes IPP 10 – Limits on use of personal information IPP 11 – Limits on disclosure of personal information	NPP 2 – Use and disclosure	GK 06 – Personal information is used only for relevant purposes GK 07 – Limits placed on the use of personal information GK 08 – Limits placed on disclosure of personal information	
Record keeping In some applications the RTO or relying party will now have a record of personal information, leading to some additional requirements regarding quality and storage.	IPP 8 – Record-keeper to check accuracy etc. of personal information before use	NPP 3 – Data quality	GK 05 – Accuracy of personal information	Guideline 5 – Aggregation of Personal Information .
Information to be Secured Any personal information now held by the Agency or relying party will be held securely.	IPP 4 – Storage and security of personal information	NPP 4 – Data security	GK 02 – Security safeguards in relation to personal information	
Awareness of Information held The learner may wish to ascertain what sort of information is held by the RTO or relying party, and how they deal with this information.	IPP 5 – Information relating to records kept by record-keeper	NPP 5 – Openness	GK 03 – Openness about the types of personal information held and information handling policies	
Access The learner may at some stage want to gain access to personal information held by the RTO or relying party, and correct such information.	IPP 6 – Access to records containing personal information IPP 7 – Alteration of records containing personal information	NPP 6 – Access and correction	GK 04 – Availability of procedures to allow subjects of personal information to access and correct the information	

Chapter 6. General legal and regulatory issues

The impact of legal and regulatory issues in the VET sector will depend on two factors:

- The electronic authentication tool (or combination of tools) used; and
- The characteristics of the transaction or relationship in question.

This chapter discusses some broad legal and regulatory issues which apply across the entire VET sector. *Chapter 7. Specific legal and regulatory issues* lists the legal and regulatory issues under the second factor (transactions and relationships), and notes any differences based on the first factor (the electronic authentication tool selected) where appropriate.

6.1. Electronic authentication regulatory framework

6.1.1. Current regulatory framework for electronic authentication in Australia

The degree of legal and regulatory intervention in the different electronic authentication tools varies significantly. The National Office for the Information Economy (NOIE) has determined that it is unlikely any further regulatory or accreditation requirements are necessary to promote the take-up and use of 'simple' forms of authentication technology (such as passwords, tokens, or Secure Socket Layer (SSL) technology). These 'simple' authentication technologies are not heavily regulated and their use only has to comply with general industry standards.[74] They are widely used across the Australian economy. However, there seems to be some agreement that more 'complex' technologies such as PKI and biometrics require accreditation and regulatory frameworks to facilitate their more widespread use.[75]

It is clear that some of the more advanced forms of electronic authentication are likely to be subject to a greater degree of regulatory intervention. In the case of Public Key Infrastructure this is already the case. In the case of biometrics, additional regulation may be some time away.

A starting point for the consideration of general legal issues facing electronic authentication is the lack of a legal and regulatory framework within Australia for electronic authentication. The absence of this structure has not gone unnoticed, and in 2002 the National Office for the Information Economy (NOIE) published a major discussion paper[76] on proposals for a National Electronic Authentication Framework, and engaged in a series of public consultations on the scope and nature of an appropriate regulatory framework.

[74] Standards developed by industry working groups or issued by Standards Australia. For a list of preferred standards in the VET sector see <http://flexiblelearning.net.au/standards/navigation/home.shtml>.

[75] National Office for the Information Economy, *Towards a National Authentication Technology Framework* (May 2002) <http://www.noie.gov.au/publications/NOIE/Authentication/NATF_Discussion_paper_July2002.pdf>.

[76] Ibid.

The proposal (replacing the current system of ad-hoc committees, policies and guidelines) would see the establishment of a National Electronic Authentication Authority with power to set standards, accredit service providers (e.g. Certificate Authorities (CAs) in a Public Key Infrastructure (PKI)), monitor industry developments and promote appropriate policies and law reform. The structure of the new body is a major discussion point in the review and there does not appear to be consensus on the outcome of this proposal at the time of this research paper. Indeed, progress on the proposal has been slow and there may not be any new developments or final recommendations until well into 2003.[77]

One submission to the National Authentication Technology Framework review captured the opinions of many participants. Stephen Wilson, from SecureNet[78] stated:

> 'To this day, NOIE's advice to PKI users is that the legal relationships between Subscriber and Relying Party, and between Relying Party and the CA, are 'unclear in Australian Law.' We suspect that this frank uncertainty alone deters many from adopting PKI. Yet it should be possible to preserve legal relationships between parties who choose to use digital certificates to assert their existing credentials online.'[79]

6.1.2. Managing regulatory framework issues

In *Recommendations 1.* and *7.* of *Chapter 9.* Galexia Consulting recommends a watching brief be maintained on the regulatory debate surrounding electronic authentication, and for the VET sector to be represented in consultations on the potential legal and regulatory framework.

6.2. Privacy

If PKI is the selected electronic authentication tool then identifying privacy risks and current privacy compliance requirements (such as the *OFPC PKI and Privacy Guidelines* and the *Gatekeeper Privacy requirements*) will be a key factor in nearly all aspects of electronic authentication in the online learning environment.

Privacy is discussed throughout the electronic authentication and flexible learning literature as a significant issue.

For example, the IMS Global Learning Consortium Project[80] dedicates a considerable proportion of its documentation to privacy issues. The IMS Project defines and delivers interoperable specifications for exchanging learning content and information about learners among learning system components. IMS members (including several education institutions in Australia) adopt these specifications to make learning easier to deliver anywhere and anytime. IMS specifications are becoming the defacto global standards for delivering flexible learning products and services, especially electronic authentication.

---

[77] Confirmed in discussions between Galexia Consulting and NOIE in November 2002 and February 2003.

[78] <http://www.securenet.com.au>.

[79] <http://www.noie.gov.au/projects/confidence/Improving/Securenet.pdf>.

[80] <http://www.imsproject.org>.

The IMS *Learner Information Package Specification*[81] states:

> 'The IMS project recognises the need to:
>
> 1. Maintain the privacy of learner information;
> 2. Protect information from inappropriate access;
> 3. Ensure the integrity of information;
> 4. Accommodate the regulatory policies and requirements of different jurisdictions.'

In addition, the IMS *Learner Information Package Specification* claims that it can assist in the protection of privacy by 'allowing for the inclusion of mechanisms for maintaining privacy and protecting the integrity of data with all data that comprises learner information.' However, IMS notes that 'the specification cannot, however, specify the form, format, or type of these mechanisms or policies for their use. These must be determined by specific implementations in accordance with their requirements.'

Following from the earlier discussion of privacy requirements in Commonwealth and State legislation (see *5.1. Relevant legislation*), these statements apply directly to the Australian environment – where privacy compliance requirements must be assessed on a case by case basis.

The IMS *Learner Information Package Specification* also notes:

> 'We would have been remiss if we had not focused much of our attention on the issue of maintaining control of the privacy of the data. Our focus was to provide structure down to the element level to allow implementers of this specification to describe and control the privacy of the data. At the same time we have left the decisions on coding and the means for controlling the privacy of the data to those packaging the data.'[82]

While the general literature acknowledges the importance of privacy as an issue, it does not set out specific privacy risks beyond legal compliance.

The full set of relevant privacy risks for electronic authentication in flexible learning are as follows:

6.2.1. General failure to comply with Commonwealth or State/Territory privacy legislation (where applicable)

RTOs, service providers and other organisations involved in online learning will sometimes be subject to Commonwealth or State/Territory privacy legislation. Occasionally they will be subject to both (e.g. where a commercial organisation is providing outsourced services to a Government agency). The requirements to comply with either the IPPs or the NPPs are relatively straight-forward, and usually require only a common sense approach to handling the personal information of students.

---

[81] IMS Global Learning Consortium Inc, *IMS Learner Information Package Specification* [version 1.0] (March 2001) <http://www.imsproject.org/profiles/>.

[82] See <http://www.imsproject.org/profiles/primer1.html>.

However, complying with some specific principles (such as IPP 8, NPP 2 and NPP 7[83]) can be tricky, and overall compliance can be difficult if a privacy culture is not already in existence within the organisation.

Generally, compliance with the legislation will require the development of a detailed privacy policy (made available to students at enrolment and on the web site), an update of documentation and some staff training.

Each privacy policy must reflect the particular nature of data collection by that education provider, but some standard headings and clauses are beginning to develop in the Australian context.

An example of a privacy policy covering electronic authentication issues in the education sector can be found on the 'MyFuture'[84] web site. Their privacy policy provides a useful insight into the privacy compliance issues faced in the online learning environment.

The consequences of not complying with Commonwealth or State/Territory privacy legislation can be serious. Complaints can be lodged with the relevant Privacy Commissioner and can result in fines, compensation and a range of other specific sanctions and remedies. The damage to an organisation's reputation which can be caused by a breach of privacy legislation should not be underestimated.

6.2.2. Intruding to an unnecessary degree into the personal affairs of students

In order to improve authentication of students, organisations may be tempted to adopt privacy intrusive practices. This may involve the collection of excessive personal information at enrolment, or perhaps during investigations of suspected cheating or impersonation. Technologies chosen to implement electronic authentication solutions may also be overly intrusive, such as cookies, web bugs, 'single sign on' logs, etc which may track all Internet use by students.

The consequences of such intrusion may include a significant backlash from students, staff, other stakeholders (including funders) and the media. Some forms of intrusion may also breach privacy legislation.

6.2.3. Function creep

In implementing a new technology such as electronic authentication it is important to guard against future expansion of the purposes for which personal information collected in the electronic authentication process is used. This potential to expand future uses is commonly referred to as 'function creep' and is a recognised privacy risk.

A common problem with new technologies which improve authentication is that they may improve identification, and even have the potential to create a national identifier – a scenario opposed (and feared) by a majority of Australians.

---

[83] See also *5.1.2. Privacy Act 1998 (Cth) – Commonwealth Public Sector requirements* and *5.1.3. Privacy Act 1988 (Cth) – Private sector requirements* in this research paper for more details.

[84] <http://www.myfuture.edu.au>.

Function creep can be difficult to manage, but three key tools are available which help limit the potential for function creep:

- **Clear and specific primary purpose**
  If the primary purpose of the collection, use or disclosure of personal information is clearly defined (often in legislation) this can have a limiting effect on future use of the information. An example would be where an electronic authentication program implemented by an RTO restricted the primary purpose to 'education.' In the Australian VET sector, some control can be maintained over the collection of data through the application of the Australian Vocational Education and Training Management Information Statistical Standard (AVETMISS) which mandates the types of data which can be collected from students.[85]

- **System design**
  Electronic authentication systems can be designed in ways which limit function creep by creating barriers to wider use. This usually has to be examined on a case by case basis. An example is where the personal information is distributed (such as a biometric on a smart card carried by the user) rather than stored in a central database.

- **Privacy oversight**
  One of the strongest controls on function creep is the establishment of privacy oversight mechanisms, such as Privacy Oversight Committees, regular privacy audits, privacy complaints monitoring etc.

All these tools are currently used by Government agencies and some private sector organisations. A combination of the three tools usually works as an effective deterrent to function creep.

If function creep is allowed to occur it represents a significant breach of privacy. Data which may have been collected for a worthwhile purpose following public consultation or negotiation, may later be used for completely different purposes, without the same level of public consultation and negotiation.

6.2.4. Potential for ongoing surveillance

Electronic authentication has an inherent privacy risk which has been difficult to avoid. In some forms of electronic authentication the user will effectively leave a 'trail' of all of their transactions. This may either be in the form of a record of all habits, movements, contacts, etc. or even in the form of real-time surveillance.

This is almost always an unintended consequence of electronic authentication.

An example is the use of a Digital Signature Certificate within a Public Key Infrastructure (PKI), where all uses of the digital certificate must be checked against a central Certificate Revocation List (CRL). Over time, the records of relying parties checking the CRL can build into a complete picture of use of the digital certificate, including the details of transactions, the times of transactions, the location and movements of the user, and even the habits and preferences of the user.

[85] See <http://www.ncver.edu.au/statistics/avetmiss40>.

This privacy issue has been difficult to overcome because it competes directly with the interests of relying parties and other stakeholders in the PKI, who want to maintain a record that they did actually check the CRL and that the CRL showed the digital certificate has not been revoked.

While the debate on this issue is ongoing, there is a growing recognition that the impasse may be resolved by the introduction of intermediaries (such as Validation Authorities (VAs)) who check CRLs on behalf of various relying parties, and issue a digitally signed receipt to the relying party confirming that they had taken the necessary steps to ensure that the digital certificate had not been revoked. The CRL would not show the identity of the relying parties, so it will reveal little about the activities of the individual. The relying party could obtain a receipt that could be used in any future disputes or legal action, to show that it acted responsibly at the time.

6.2.5. Restrictions on user choice

A major privacy risk in implementing electronic authentication is that restrictions are placed on user choice. If an institution only accepts one particular form of electronic authentication, or in a digital certificate based system, one particular digital certificate, opportunities for users to protect their own privacy can be severely limited.

This privacy risk is recognised by detailed regulatory requirements in the PKI environment, but is left up to institutions when using other forms of electronic authentication.

Ultimately, consumer choice represents one of the strongest forms of privacy protection. Restricting user choice to just one form of privacy intrusive electronic authentication will be seen as an infringement of privacy, unless the curtailment of choice can be justified on other public benefits grounds.

A typical solution is to allow user choice in the majority of situations but to restrict user choice in high security transactions.

6.2.6. Managing privacy issues

To manage the privacy issues identified in this paper, ANTA-FLAG and/or individual VET providers may have to undertake a coordinated approach to addressing privacy concerns in any implementation of electronic authentication.

The management of privacy issues is a recognised (and maturing) compliance task and a range of tools have been developed to assist in privacy management. These tools include:

- **Privacy Impact Assessment (PIA)**
  This assessment identifies privacy in specific sectors or applications. A PIA process is particularly useful for implementations of new technology or new processes. By using the PIA tool at the design stage of an implementation organisations can avoid privacy errors and the costs of rectification at later stages.
- **Privacy Management Strategy (PMS)**
  This tool is used to develop and implement a risk management strategy and practical action plan. Each privacy issues is allocated a response and action is delegated to individuals or organisations. The PMS includes a compliance timetable.

— **Privacy Oversight Structure**
This tool is used to develop a governance structure to oversee privacy issues arising throughout the life of the implementation. Many privacy issues cannot be ascertained at the design stage so reviews, audits and the establishment of oversight committees is often necessary.

— **Consultation**
Public and stakeholder consultation, education and training is often more important than ensuring technical compliance. Many privacy risks are perception risks rather than legal compliance risks and effective consultation can help identify and manage perception risks.

— **Privacy audit (non-complaints focussed)**
Reviewing the effective adoption and use of complying processes and documentation on a regular basis (including independent audits) is a useful tool in identifying and managing privacy risks, and raising public confidence in the management of privacy within new technology projects.

— **Privacy complaints handling**
Although many organisations have effective complaints handling mechanisms in place, some customisation (and additional staff training) on specific privacy risks can help to ensure that privacy complaints are dealt with sensitively and professionally, and that systemic complaints and serious issues are dealt with appropriately.

6.3. Legal liability

6.3.1. Legal liability issues in PKI transactions

Legal liability issues are recognised as one of the important categories of 'unfinished business' in the development of electronic authentication in Australia and other jurisdictions. Most legal analysis concentrates on the legal liability issues which arise between the parties in a PKI transaction, although some of these issues may have broader relevance to other forms of electronic authentication.

In Australia, the National Office for the Information Economy (NOIE) has responsibility for considering these legal liability issues and their potential solutions. NOIE asked the National Electronic Authentication Council (NEAC) to report on this issue, and NEAC produced two reports on specific legal liability issues which arise in PKI transactions:

- **Legal Liability and E-Transactions – 21 August 2000**[86]
  This report examined the adequacy of current Australian law and private law mechanisms for managing the allocation of liability among three parties to a PKI: a Subscriber, a Certification Authority (CA) and a Relying Party (RP). NEAC found that Australian law generally provided adequate guidance for allocation of liability among those parties. A notable exception was where a CA may owe a duty of care to a RP who is not known to the CA (either because the RP does not consult the CA's certificate repository or Certificate Revocation List (CRL) or does so anonymously). The report also found that it was unclear whether private law mechanisms (such as contractual liability provisions, disclaimers and insurance) could provide adequate certainty to manage liability allocation in the relationship between the CA and a RP, and that more research on this point was required. The uncertainty related to the extent to which a CA can effectively impose liability limitations on a RP by notice or disclaimer in a digital certificate or by an online contract (if the RP consults a certificate repository or CRL), and the effect on some contractual allocations of liability between Certification Authorities and Relying Parties of common law and statutory consumer protection rules (such as those contained in the *Trade Practices Act 1974 (Cth)*).

- **The Legal Liability of Parties to a PKI Transaction – 8 May 2002**[87]
  This second report re-examined the legal liability concerns raised in the initial research, with the assistance of three case studies of existing PKIs. The report examined documentation, disclaimers, contractual provisions etc. in greater detail than the initial report. However, no broad conclusions or recommendations can be drawn from the report and the legal position between CAs and RPs remains unclear.

These legal issues are causing considerable concern in other jurisdictions and little progress has been made in resolving this impasse.

---

[86] National Electronic Authentication Council (NEAC), *Legal Liability in E-Transactions*(21 August 2000) <http://www.noie.gov.au/publications/NOIE/NEAC/publication_utz1508.pdf>.

[87] National Electronic Authentication Council (NEAC), *The Legal Liability of Parties to a PKI Transaction* (8 May 2002) <http://www.noie.gov.au/publications/NOIE/Authentication/PKI_legal_report_May2002.pdf>.

In the United Kingdom, the Joint Information Systems Committee (JISC) has reported that they have encountered concerns over the legal 'significance' of a digital signature.

> 'If strong authentication technology is deployed in order to support commercial electronic transactions and strict access control with penalty clauses for breaches of security, then the technology must have sufficient backing in law to make the theory possible in practice. The crucial security service involved is "non-repudiation", which we defined as involving the recipient of a digitally signed message gathering sufficient evidence to ensure that the authenticated sender of the message cannot later deny having sent it, with trusted notarisation procedures and trusted time-stamps as the mechanisms to achieve this. The legal standing of the trusted services required to support this must be established (presumably involving licensing, audit and regulation) and the procedures for arbitrating disputes must be clearly laid down.'[88]

Until some of these legal liability issues are resolved, parties will have to rely on their rights being established through the contract. Typically, this will involve acceptance of a set of terms and conditions for the end user. Some examples of terms and conditions include MyFuture[89] and HeSA.[90]

Another example of terms and conditions can be found in the *University of California (UC) Guidelines on Management and Use of Digital Certificates*. Their *Sample Subscriber Agreement* states:

> 'The UC Certificate being issued is an important form of identification. With the appropriate authorization, I may use this UC Certificate to access applications or data made available to select groups within the UC Community. All of the information I have provided and all of the representations I have made in applying for this certificate are true. I will protect the private key associated with the certificate by storing it in a password-protected location. I will not allow anyone else access to my private key. I will inform the UC Certificate Authority immediately if I believe the security of my private key may have been compromised. I understand that the University of California reserves the right to revoke my UC Certificate if there is reasonable grounds for suspicion of misuse of the certificate or if my affiliation with the University of California terminates. To notify the UC Certificate Authority in the case where the private key may have been compromised, [provide specific procedures the Subscriber needs to follow for notification of the UC Certificate Authority in the case of a suspected compromise of the Subscriber's private key.'[91]

This disclaimer is an example of the culture which will need to develop around electronic authentication in the flexible learning environment. The 'student centred' nature of flexible learning also requires students to take a certain degree of responsibility regarding authentication and security.

---

[88] Joint Information Systems Committee (JISC), *Technologies to Support Authentication in Higher Education v5* (1996) <http://www.jisc.ac.uk/index.cfm?name=acn_support_authent>.

[89] <http://www.myfuture.edu.au>.

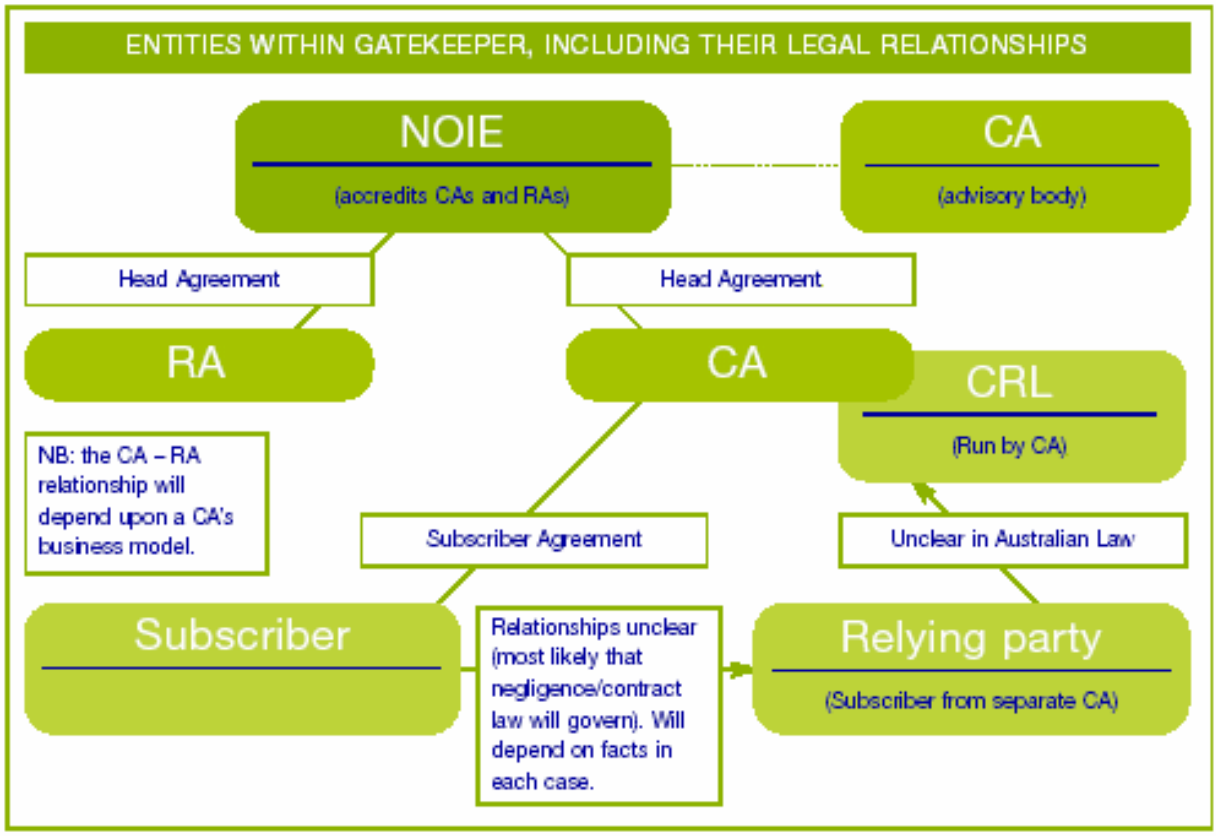
[90] <http://www.hesa.com.au>.

[91] University of California Office of the President *Why UC Must Invest in a Public Key Infrastructure (PKI): The Case for Digital Certificates* (May 2000) <http://www.ucop.edu/irc/auth/whypki.pdf>.

6.3.2. Managing legal liability in PKI transactions

The allocation of legal liability between parties in PKI transactions remains uncertain in Australia, and the relevant law reform process is stalled.

The legal uncertainty surrounding the allocation of liability between the parties is recognised as a major issue by the National Office for the Information Economy (NOIE). In *Online Authentication – A Guide for Government Managers*[92] they describe the legal relationships between the parties in a PKI. Note the legal uncertainty acknowledged in the following diagram (e.g. between Relying Parties and the Certification Authority(CA), and between Relying Parties and Subscribers):



Until the legal uncertainty is resolved, contractual clauses and disclaimers will be the chief tools used to manage legal liability. In this situation, it is likely that the allocation of legal liability will be biased towards institutions, and against individual learners.

[92] National Office for the Information Economy, *Online Authentication – A Guide for* Government *Managers* (July 2002) <http://www.noie.gov.au/publications/NOIE/online_authentication/OnlineGuideFinal.pdf>. Diagram available at page 55.

In *Online Authentication – A Guide for Government Managers*[93] NOIE provides the following important warning:

> 'NOIE will not accept liability for:
>
> - The use of a Gatekeeper certificate (e.g. an ABN-DSC[94]) where a government Agency was not a party to the transaction supported by the certificate (notably business-to-business transactions); or
> - An act or omission of a Gatekeeper accredited service provider in breach of its Head Agreement with NOIE, or its NOIE accredited Certificate Policy (CP), accredited Certification Practice Statement (CPS) or Subscriber Agreement.
>
> Also, in accrediting a Gatekeeper service provider, or its CP and CPS, NOIE gives no warranty as to:
>
> - The standard or suitability of any services thereby provided; or
> - The suitability of the CP and CPS and other Gatekeeper accredited documents for subscribers or relying parties. In particular, whenever appropriate, subscribers should be advised to consider seeking independent professional advice as to the risks and liabilities which may result from their signing a Subscriber Agreement or becoming party to a CP or CPS.'[95]

The recommendation that relying parties should seek 'independent professional advice' displays the significant consequences of the uncertain legal environment in which PKI is currently operating. It is onerous for small RTOs in the VET sector to pay for independent legal advice before relying on digital certificates to authenticate students, providers or other participants. A broader solution to these legal issues is required.

Galexia Consulting recommends that a 'holding pattern' can be maintained on liability issues (through reliance on contractual terms and perhaps the development of model contracts – see —*Recommendation 1* in *Chapter 9)*. However, the VET sector will require a more acceptable solution in the medium term and will need to participate in the electronic authentication law reform process – see —*Recommendation 7* in *Chapter 9*.

[93] Ibid.

[94] Australian Business Number Digital Signature Certificate.

[95] Ibid., footnote 92, page 49.

6.4. Electronic formation of contracts

There are two elements required in Australian law for the formation of a contract (whether or not it is an electronic contract). They are:

- An intention to create contractual relations; and
- An agreement (consisting of an offer, acceptance and consideration).

The *Electronic Transactions Act 1999 (Cth)*[96] (ETA) provides a legal framework for these two requirements to be met in electronic contracts. The Act is technology neutral, in that it enables electronic transactions to occur without prescribing particular types of technology. The key sections are:

- **Section 8 – General**
  A transaction is not invalid because it took place wholly or partly by means of one of more electronic communications.
- **Section 10 – Signatures**
  If the signature of a person is required, that requirement may be met by use of an electronic method as long as:
  - The method is used to identify the person and to indicate their approval of the transaction;
  - The method is as reliable as appropriate for the purposes of the transaction; and
  - The signature recipient consents.
- **Section 11 – Documents**
  A person can produce a document in the form of an electronic communication where other laws require the production of a paper document.
- **Section 12 – Records**
  If a person is required to record or retain information or documentation in writing, that requirement can be met by retaining or recording the information in electronic form.

The Act therefore resolves the majority of obstacles to the electronic formation of contracts, and a range of electronic mechanisms is now available for use in contract formation the VET sector. In the majority of situations, the formation of electronic contracts will be simple and automatic.

[96] See also *5.1.1 Electronic Transactions Act 1999 (Cth)* in this paper for more details.

Electronic contracts in the flexible learning environment can be formed quickly via the following methods[97]:

— **Email**
A user and a provider can enter into simple email communications representing each stage of the contract formation process (offer, acceptance and consideration). This process could be performed on an ad hoc basis in plain text. Alternatively, the process can be customised and partly automated through the use of a pro forma email containing key terms and conditions, requiring only a limited number of additional text fields to be completed.

— **Interactive attachments**
A provider can supply an electronic contract as an 'interactive attachment' (such as a Portable Document Format (PDF) form) to an email which must be completed and returned by the user. The revised electronic version of the attachment would be the 'contract' once it was received by the provider, subject to the provision of consideration (payment or a payment promise).

— **Interactive web sites**
A user can visit a provider's web site and view the standard terms and conditions of a particular contract. Using interactive forms they can complete various fields until a revised contract can be presented which is acceptable to both parties (the process of accepting and rejecting changes will usually be automated on the provider's system, and some fields such as key terms and price may not be accessible for editing in such a system without additional communication). The user will indicate their acceptance of the final version of the contract by clicking on a 'confirm' button and consideration will be provided by an online payment system or through a payment promise.

— **'Click-wrap' agreements**
'Click-wrap' agreements are similar to the above process, although there is usually no opportunity to alter any terms and conditions in the agreement. A user simply completes their own relevant details and confirms acceptance of the standard terms and conditions of the agreement, usually by clicking a 'confirm' field on a web site or in a dialog window.

— **Electronic agents**
A user can configure an electronic agent (a software application that combines user preferences and 'artificial intelligence' to perform and learn specific tasks) to find the best price on a particular learning object available via the Internet and begin the process of forming an electronic contract via automated means. The user would simply confirm the transaction once the details of the agreement (delivery, price, payment method) had been prepared[98].

[97] This is not an exhaustive list and new methods for the electronic formation of contracts are constantly under development.

[98] For a more detailed explanation see Emily M. Weitzenboeck, *Electronic Agents and the Formation of Contracts,* Electronic Commerce Legal Issues Platform (2001) at <http://www.eclip.org/documentsII/elecagents/contract_formation.pdf>.

In each of these scenarios a variety of mechanisms can be used to authenticate the potential parties to the contract. The type of electronic authentication selected may provide greater certainty regarding the identity and attributes of the parties and greater integrity of the content of the communications. However, the over-riding test for the formation of electronic contracts remains the intention of the parties.

The remaining difficulties which may arise in the formation of contracts online will occur because of a lack of consent by 'signature recipients.' That is, some institutions and agencies may continue to insist on handwritten signatures on some documents and refuse to provide consent (as required by *section 10*[99]) to use whatever electronic system is proposed by the other party. Note, the consent requirement is limited to situations where a handwritten signature is required by an existing law, so this barrier may not be significant in the VET sector (it is more prevalent in the real estate and financial services sectors).

If contracts cannot be formed via electronic means in the online learning environment, the following difficulties may arise:

- **Difficulties in enforcing claims for outstanding payments**
  In a flexible learning environment, systems for collecting payments from learners may be complex. A student will not necessarily have a direct or physical relationship with every single institution they deal with, so the formation of contracts will have to take place via electronic means. The Australian Government Solicitor has warned that this is an area of potential concern: 'An educational institution accepts student applications online. An inability to reliably authenticate the identity of the student as a party to a contract for educational services may mean that the educational institution is unable to enforce a claim for outstanding payment for courses.'[100]

- **Difficulties in enforcing rules regarding student conduct**
  Students at many institutions enter into contractual arrangement regarding their conduct – such as providing written warranties that their submitted work is free from plagiarism. There are two concerns with this:

  - Firstly, such contracts may be more difficult to enforce if the contract has not been properly formed via electronic means; and
  - Secondly, these contracts have always been a form of deterrent, and electronic contracts of this nature may carry less psychological weight than their written equivalents.

- **Difficulties in contractual relationships with teachers**
  One of the benefits of the flexible learning environment is that VET providers and teachers can have a more flexible and distant relationship. These benefits will be lost if teachers have to complete substantial paperwork or attend physical appointments in order to form contracts.

---

[99] <http://scaleplus.law.gov.au/html/pasteact/3/3328/0/PA000170.htm>.

[100] Australian Government Solicitor, *Legal Aspects – Electronic Authentication* (2001), page 4.

— **Difficulties in enforcing rules regarding copyright of course materials**
Much of the current copyright system is based on the completion of hard copy forms. This layer of paperwork presents a barrier to flexible learning that may be overcome by developments in electronic copyright managements systems such as the development of Digital Rights Management Systems (DRMS).

Continued awareness raising and professional development across the VET sector will assist in the take-up of electronic contract formation. Many of the electronic authentication recommendations discussed in *Chapter 9* will enable the wider take-up of electronic contracts.

Chapter 7. Specific legal and regulatory issues

This chapter examines the legal and regulatory issues which arise when a particular transaction or relationship is considered.

Until an authentication model is chosen there are too many potential legal scenarios to provide a detailed response on each issue. However, we have noted the key issues and provided pointers to sources of further legal guidance.

7.1. Education materials – access to content and learning objects

This section examines the role of electronic authentication in content provision and content management.

It is expected that access to materials will be managed by a range of Learning Management Systems (LMS), Content Management Systems (CMS) and Digital Rights Management Systems (DRMS). However, there is the potential for an electronic authentication system (perhaps as part of a learner account or skills passport) to sit above these individual systems and help to interact with a variety of such systems used by different content providers.

The jurisdiction where the use of electronic authentication tools to restrict access to teaching materials and learning objects is most advanced is the United Kingdom.

The Joint Information Systems Committee (JISC)[101] is an independent advisory body that supports further and higher education in the United Kingdom by providing strategic guidance, advice and opportunities to use information technology to support teaching, learning, research and administration.

JISC has negotiated agreements with publishers and other data providers for electronic materials to be made available to the UK higher and further education community. Typically a community license and pricing structure is negotiated for a particular collection or dataset, and individual universities and colleges are offered the opportunity to take out a subscription at the negotiated price. The majority of these resources are accessed via a web interface.

To protect the interest of rights holders and to ensure that license agreements are fulfilled, JISC established a national access management service which allows properly authorised users from the subscribing institutions to gain access to licensed electronic content. This service, known as Athens[102], is an authentication implementation relevant to the Australian VET sector. It is specifically designed to assist in a flexible learning environment and is not tied to one particular education institution.

The Athens system provides users with ‘single sign-on’ to numerous online services and content throughout the UK and overseas. Athens was initially deployed in the Higher Education sector in 1996. The Athens service currently holds over 2 million user accounts from over 600 organisations and controls access to over 200 online services.

---

[101] Joint Information Systems Committee (JISC), *Access Management Service for UK Higher and Further Education (Information Memorandum)* (2002) <http://www.jisc.ac.uk/index.cfm?name=funding_4_02>.

[102] <http://www.athensams.net>.

The Athens project is designed to help in situations where individuals have different sets of credentials for access to different services For example, a typical student may have a username for local computing resources, a borrower number for the library, and a student number for access to student-orientated services.

Athens is, fundamentally, a central repository of organisations, usernames and passwords with associated rights. It has extensive account management facilities for organisations to create and manage usernames and passwords, and to allocate rights to individual users.

In the Untied States, there is also considerable activity in the use of electronic authentication tools to manage access to education materials. For example, the US Army utilises Public Key Infrastructure (PKI) to restrict access to education materials:

> 'The use of PKI also provides for a secure environment were personal information and course material is exchanged only between appropriate individuals. In the realm of distributed learning, the transmission of information must be secure. The use of encryption is one means to assure that tests, answer sheets, and training materials are sent and received only by the authorized individuals, and that the information is not accessed or modified along the way. This ensures that the learning environment is not compromised.'[103]

Another example of a project which recognises the relationship between education materials and electronic authentication is the University of California (UC) PKI project.[104] This project is designed to authenticate students, and staff to enable them to electronically access otherwise restricted journals and periodicals. One of the legal issues which arises in a PKI implementation of this nature, is that student records may have to be shared (often on a regular basis) with relying parties and other participants in the PKI, to ensure that the correct students are issued with digital certificates, and that digital certificates are revoked for students who have left the University.

In order to implement this system at University of California (UC), the institution had to comply with complicated federal laws, as can be seen in the following agreement posted to students. Similar privacy legislation applying to the use of student data applies in Australia.

> 'Because release of student records is governed by Federal law (The *Family Education Rights and Privacy Act* – FERPA[105]) and University policy, this understanding sets forth the conditions governing use of data exchanged between campuses for this purpose.
>
> Individually identifiable student records provided by campuses to [other parties] as part of the authentication infrastructure is personal data and will not be accessible or released to parties outside the supplying campus. An exception is the category of Information Resource Custodians, operating the University's PKI. Such individuals will not observe personally identifiable information except as necessary to maintain the PKI and confirm data integrity.
>
> Non-UC entities such as publishers will only be able to determine general class information about a student holder of a digital certificate, a key component of the PKI. These include student enrolment status, student type, and student status.'[106]

---

[103] Curnow, Freeman, Wisher, Belanich and Moses, United States Army Research Institute for the Behavioral and Social Sciences, *Training on the Web: Identifying and Authenticating Learners* (June 2002), <http://www.ari.army.mil/pdf/authenticatingLearners.pdf>.

[104] University of California Business and Finance Bulletin, *Guidelines on Management and Use of Digital Certificates* (November 1999) Note this project appears to be stalled. See <http://www.ucop.edu/irc/auth/auth-wg>.

[105] For more information on FERPA see <http://www.ed.gov/offices/OM/fpco/ferpa>.

During early stages of development of applications which use electronic authentication for education materials, there may be little guidance on some key legal issues. The following table provides pointers on legal guidance for a number of issues associated with electronic authentication and education materials:

Education materials – Legal Issues	**Legal guidance**[107]
Restricting access	• VET legislation – internal policies
Disability access	• *Disability Discrimination Act* • Common law (*Maguire v SOCOG*[108])
Copyright (especially DRMS)	• *Copyright Act* • *Copyright Amendment (Digital Agenda) Act 2000 (Cth)*
Privacy	• *Privacy Act 1998 (Cth)* • State/Territory privacy legislation • PKI Privacy guidelines • Gatekeeper privacy requirements

[106] The University of California Common Authentication project, *Draft Guidelines on* Management *and Use of Digital Certificates* (November 1999) <http://www.ucop.edu/irc/auth/digcerts-draft.pdf>.

[107] See *Chapter 5. The current legal and regulatory framework for electronic authentication in Australia* in this paper for more details.

[108] *Maguire v Sydney Organising Committee for the Olympic Games* H 99/115, Human Rights and Equal Opportunity Commission.

7.2. Education providers

This section examines the role of electronic authentication in relation to education providers. There is strong potential for the use of authentication in ensuring the qualifications and accreditation of education providers, both at the organisational and individual level.

Typically, one RTO may want to authenticate the credentials of other RTOs with which it has teaching arrangements in place. RTOs may also want to authenticate the credentials and identity of their remote teachers, assessors and supervisors. A Public Key Infrastructure (PKI) based system could assist in this process. For example, teachers would only have to register their accreditation once and be recognised by any institution. RTOs could 'rely' on the digital certificate without having to conduct further checks (apart from confirming that the digital certificate had not been revoked - which can be an automatic function of PKI enabled applications).

Once a provider has been authenticated, a similar process can authenticate other attributes, such as their right to view, enter, change and delete data (these attributes are often called authorisation or permissions). For example, the same digital certificate which is used to authenticate a teacher as accredited, may determine whether they are able to change results in the student administration system.

The implementation of authentication for education providers is a sensible first step in the VET sector. The advantages are:

- The population is smaller (as opposed to the population of students);
- The population is relatively stable, compliant and accessible;
- The technical resources available to the population are reasonably high;
- There is a track record of similar successful implementations in other sectors (e.g. HESA[109]); and
- The legal and regulatory issues are (slightly) less onerous (e.g. user choice is a less significant requirement).

Most of the legal issues which arise in this type of application fall into the 'legal liability' category (see *6.3. Legal liability*). The original accreditation body (and their Registration Authority (RA) in a PKI) carries a significant responsibility to ensure the qualifications, and the identity, are correct. It can be envisaged that an RTO may hire the services of a remote teacher without ever meeting the person (in the physical sense).

It will also be important in these circumstances to ensure that a system exists for reporting abuse (such as fake qualifications) and revoking digital certificates (such as lost/compromised tokens/smart cards). This will require a clear allocation of responsibility for digital certificate revocation.

Further legal issues will arise in the area of industrial relations. There has been little legal development to date regarding the relationship between industrial relations and authentication, but it can be envisaged that a teacher facing disciplinary proceedings in one education institution may have their digital certificate revoked, with significant personal consequences.

[109] See *4.2.1 Scenario 1 – Managing relationships between RTOs and service* providers in this paper.

The following table provides pointers to legal guidance for a number of issues associated with electronic authentication and education providers:

Education Providers – Legal Issues	Legal guidance[110]
Authentication of qualifications (e.g. Accreditation)	• Common law (see NEAC reports) • Contractual terms, disclaimers etc. (e.g. HESA documentation[111]) • VET legislation (re qualifications)
Industrial relations	• Workplace relations legislation (State/Territory and Cth)
Contracts	• *Electronic Transactions Act 1999 (Cth)*
Privacy	• *Privacy Act 1988 (Cth)* • State/Territory privacy legislation • OFPC PKI Privacy guidelines • Gatekeeper privacy requirements

7.3. Participants (Learners)

This section examines the electronic authentication of participants (learners) – including their identity, progress, and attributes.

There are two general reasons for pursuing a higher level of authentication for learners. The first is largely defensive – avoiding fraud and cheating (thus maintaining the integrity of the education system). The second is to provide greater convenience for learners.

A focus on the defensive approach to electronic authentication has led some commentators to consider the development of strong authentication as a means of addressing fraud and cheating before it becomes more widespread.

[110] See *Chapter 5. The current legal and regulatory framework for electronic authentication in Australia* in this research paper for more details.

[111] <http://www.hesa.com.au>.

Consider the approach taken by the US Army when considering their authentication needs for their electronic distance-learning program (a program for recruits and army reservists – one of the world's largest distance learning programs with more than one million participants undertaking training at any one time):

> 'The Army Training Support Center recognize that an increased reliance upon distributed learning systems accentuates the need to identify various forms of training compromise, such as obtaining questions beforehand or enlisting a proxy for test taking in un-supervised, web-based learning environments. There is no definitive evidence that such training compromise is currently a problem in the Army, but greater use of distributed learning in the future coupled with reported trends of high levels of cheating among high school students, the Army's prime enlistment pool, is reason for concern.'[112]

The alternative 'convenience' approach may lead to a discussion based on meeting the needs of the learners, rather than the institutions. Consider this alternative approach to electronic authentication from the US Career Management program:

> 'The Career Management Account pilot program, an initiative of the US Department of Labor, is currently using the PKI method to authenticate learners who wish to create an account for the purpose of storing and managing all of their lifelong learning and career information. The Career Management Account program is part of America's Career Kit, which was developed to assist people in procuring a job of their choice. In a Career Management Account, all of a person's work experience, training, and other related information is stored so the information can be easily shared with potential employers. This account is maintained and updated as needed. The use of PKI and other security methods allows for the creation of secure Career Management Accounts, a safe place to record lifelong learning and career development.'[113]

Whichever approach is taken (or indeed a combination of the two), it seems clear that authentication of learners will deliver substantial benefits to learners and institutions engaged in flexible learning activities. These benefits include:

- Reduced opportunities for cheating (plagiarism, identity fraud, theft or distribution of assessment tools);
- A general deterrent for cheating and other security breaches; and
- Greater student convenience through applications that build on the electronic authentication platform (such as single sign on across multiple providers).

How prevalent is cheating in the flexible learning environment? The case studies seem to indicate that educational institutions assess the rate of cheating in unsupervised assessment at about 10%. They are surprisingly comfortable with this level of cheating.

[112] Ibid., footnote 103, page 10.

[113] Summary of the presentation by Dr. David Pass, Career Management Account Team Leader, U.S. Department of Labor, Washington, DC.

This assessment has been confirmed in the Australian universities sector by the recent research of Martin Dick at Monash University.[114] This research involved a series of surveys of postgraduate and undergraduate IT students at Monash and Swinburne Universities.

The first task was to establish whether students found particular types of cheating acceptable or unacceptable:

Scenario	Undergraduate Acceptable %	Postgraduate Acceptable %	Average %
Resubmitting an assignment from a previous subject in a new subject	51	40.2	45.6
Submitting a friend's assignment from past running of the subject	36.2	21.6	28.9
Hiring a person to write an assignment for you	4	3.9	3.95
Copying another student's assignment from their computer without their knowledge and submitting it	4.6	5.9	5.25
Copying material for an essay from the Internet	10.9	7.8	9.35
Hiring someone to sit an exam for you	2.4	1	1.7

[114] ITICSE 2002 Working Group, *Addressing Student Cheating* <http://www.csse.monash.edu.au/~mdick/ITICSEWorkingGroup/>.

A more challenging task was to determine whether students had themselves participated in the type of cheating discussed previously. The anonymous nature of the survey helped to achieve reliable results:

Scenario	Undergraduate cheated %	Postgraduate cheated %	Average %
Resubmitting an assignment from a previous subject in a new subject	28.2	15.5	21.85
Submitting a friend's assignment from past running of the subject	28.7	17.5	23.1
Hiring a person to write an assignment for you	3.1	1	2.05
Copying another student's assignment from their computer without their knowledge and submitting it	6.9	3.9	5.4
Copying material for an essay from the Internet	18.9	15.5	17.2
Hiring someone to sit an exam for you	2.9	0	1.45

Finally, the researchers asked students whether they personally knew other students who had participated in the identified categories of cheating:[115]

Scenario	Undergraduate Know of it %	Postgraduate Know of it %	Average %
Resubmitting an assignment from a previous subject in a new subject	38.1	29.1	33.6
Submitting a friend's assignment from past running of the subject	44	41.7	42.85
Hiring a person to write an assignment for you	10.8	11.7	11.25
Copying another student's assignment from their computer without their knowledge and submitting it	21.4	13.6	17.5
Copying material for an essay from the Internet	27.9	22.3	25.1
Hiring someone to sit an exam for you	4.3	3.9	4.1

[115] Note: The original survey included many more categories of cheating than those summarised here.

From the previous results, it is clear that some forms of cheating are surprisingly widespread, and even extreme forms of cheating (such as hiring a person to write an assignment) are prevalent. Some of the results relating to use of the Internet and computers point to a higher potential for cheating in a flexible learning environment

Another useful aspect of the research was that the surveys asked students to identify reasons for cheating (and reasons for not cheating).

Reasons to cheat	Likelihood to cause cheating		
	UG %	PG %	Avg%
Will fail otherwise	62	54	58
Not enough time	62	52	57
Too great a workload at university	60	52	56
Ca not afford to fail	54	48	51
Assignments are too hard	54	46	50
Afraid of failing	54	46	50

Reasons not to cheat	Likelihood to prevent cheating		
	UG %	PG %	Avg %
Want to know what your work is worth	82	88	85
Pride in your work	82	86	84
Can get good marks without cheating	80	80	80
Against your moral values	76	80	78
Penalties if caught are too high	72	72	72

Note that the results in the previous two tables diverge slightly from the results of similar surveys in the United Kingdom (discussed in more detail below), where one of the identified reasons for cheating was that the 'system' made it easy to cheat.

Despite the results of the Monash study, our case studies and additional research indicate that there is no general consensus about whether or not online learning provides greater opportunity for cheating, or indeed provides greater opportunities for detecting cheating. Much appears to depend on the type of assessment chosen (and the level of interaction or 'nuisance' which results) rather than the method of authentication chosen.

Also, institutional culture does not appear to be a significant factor in deterring cheating:

> 'Several cheating scandals in military academies have been reported despite the honor codes in place at those institutions. For example, at the U.S. Naval Academy in 1992, 24 midshipmen were expelled, and 47 were punished after an investigation revealed their involvement with circulating advance copies of an electrical engineering exam.'[116]

[116] DeWan, *Failing grade* for *cheaters,* Newsday, May 1994 <http://www.newsday.com/other/education/ny-cheaters-conflict.story>.

An additional source of useful information on cheating is the JISC study in the United Kingdom. In the second half of 2000 the JISC Committee for Awareness, Liaison and Training (JCALT) commissioned a study of the human and organisational issues associated with network security by South Bank University and the University of Glasgow.[117]

The respondents were asked to rate a group of different types of plagiarism and cheating with regard to the degree of seriousness:

Type of cheating	Rating as 'serious'
Helping someone to cheat, forgetting to cite a source for a quotation, copying material from the web, copying a book without citing it and paraphrasing parts of a book and not citing it	75%
Submitting material for one assignment similar to something already submitted, obtaining an essay and submitting it as your own work, doing an assignment with help from friends not on the course and citing things one has not read	50%
Help from people not on the course	30%

Respondents were then asked to choose from a set of statements about why some students copy others' work. Students' poor time management was the most selected answer, with about two thirds of respondents choosing this option. Students 'needing more help' was also a popular choice. Importantly from an electronic authentication perspective, about one third of students attributed cheating to work not being checked, the low risk of being caught, and the system of work and assessments 'encouraging' it. Few attributed cheating to how difficult the courses were, or deadlines or light punishments.

> 'Respondents tended to underestimate the effect of their actions on others. A few people do get a lot of viruses, but there was evidence of quite widespread bad practice, and that users do not fully understand the institutional cost of viruses. Many people seem not to read policies, and on the whole policies seem to be viewed quite negatively. Users are confused about backups, recognising their importance but not consistently making them. Risky password practices are alarmingly common. Impersonation is underestimated as a risk. Users do not fully recognise the risks associated with sending confidential information by email. Although ignorance and uncertainty were quite widespread, users did seem motivated to security.'[118]

The US Army (in the *Training on the Web: Identifying and Authenticating Learners* study discussed previously) found a similarly high level of cheating. Their response is worth noting, as it sets out a multi-pronged approach, of which authentication is only a small part.

---

[117] JISC Committee for Awareness, Liaison and Training Programme (JCALT), Identification of Human and Organisation Issues Concerning Network Security (March 2001) http://www.litc.sbu.ac.uk/jcalt/report.pdf.

[118] Ibid., page 5.

The US Army advisory panel made a series of general guidelines for solutions to 'training compromise' (cheating):[119]

- Use third party supervision. One issue that was discussed regarding third party supervision was how this may conflict with the 'anytime, anywhere' training goal of Army distributed learning programs;
- Use learning management tracking systems to collect audit trails in computer-based environments;
- Design tests using randomised items;
- For computer-based testing, use 'no print/capture' options[120], limit the number of times a person can attempt a test, implement a 'test mode' on the computer, and/or track where the test taker has been online;
- Implement PKI so only specific students can access courseware and tests; and
- Periodically verify the test taker through biometric or biographical measures.

These recommendations exemplify the 'defensive' approach to using authentication for learners. A good example of the alternative 'convenience' approach is the work of the IMS Global Learning Consortium.[121]

The IMS is involved in the development of a Career Management Account System (a type of learning and career development passport). The prototype provides a central repository containing all relevant career information (such as transcripts, performance reviews, sample work product), and an area for storing additional biographical data. The Career Management Account System (CMA) has two parts, the CMA digital certificate (which provides access control and security) and a personalised portfolio that can be accessed via the digital certificate.

Each 'Life-long Learner' creates, manages, and owns an individual portfolio containing the following data:

- **Static Biographical**
  Describes invariant characteristics such as date of birth.
- **Dynamic Biographical**
  Describes variant characteristics of the individual such as current address or email information.
- **Self-Reported**
  Information under the direct control of the Life-long Learner and modifiable by them regardless of source such as a writing sample, a computer aided design work product, or a transcript furnished to the Life-long Learner by a third party and entered into their Portfolio by the Life-long Learner.

[119] Ibid., footnote 103.

[120] This limits opportunities for tests to be shared with future students.

[121] <http://www.imsproject.org>.

— **Third Party Validated**
Information placed in the Portfolio with the permission of the Life-Long Learner but under the control of a validating third party such as a certifying training provider or degree granting educational institution. The obvious example is a transcript but also includes test and evaluation scores and may be extended to include performance reviews and personnel evaluations and health certifications as well.

All access to the CMA and to portfolios is under a strong public key infrastructure and requires full digital certification. Key fields in each record in the portfolio are separately encrypted to prevent direct identification of individuals from non-specific information.

In this system there are four potential stake-holders:

— **Life-long Learners**
Can review information in their portfolio at any time under direct and secure access. Furthermore such learners can create 'views' of their portfolio information in a manner similar to creating a resume or curricula vitae by using portfolio elements as building blocks. These views can be made available either to a 'public' view that is generally accessible or to 'specific' views restricted to one or more recipients.

— **Recipients**
May include prospective employers, advisors and evaluators. Recipients have secure access to views provided to them by learners.

— **Providers**
Those parties that, at the request of the learner, provide information to an individual portfolio (these are the providers of third party validated information such as transcripts and test results).

— **Systems Managers**
The maintainers of the CMA and its security apparatus.

In this system, the information is stored on a central database, and the PKI helps to manage access to that database. However, it is possible to develop a distributed system (also relying on PKI) where the portfolio would be retained by the learner on a smart card, token, PC or other device. Such a system would help deliver the full potential of a learning passport, without many of the privacy issues raised by a central database.

Both the 'defensive' and 'convenience' approaches to electronic authentication could deliver significant benefits for learners in a flexible learning environment. There do not appear to be any significant specific legal and regulatory issues for learners, beyond the generic issues discussed in *Chapter 6. General legal and regulatory issues*.

The following table provides pointers to legal guidance for a number of issues associated with the use of electronic authentication for learners:

Education Participants (learners) – Legal Issues	**Legal guidance**[122]
Authentication of learners for class participation (e.g. access to materials, online coursework)	• OFPC PKI Privacy guidelines • Gatekeeper privacy requirements
Authentication of learners for assessment	• OFPC PKI Privacy guidelines • Gatekeeper privacy requirements
Authentication of learners for a learning passport and records of achievement	• VET legislation • Qualification Authority legislation (where applicable)
Cheating (plagiarism, identity fraud)	• VET legislation • *Cybercrime Act 2001 (Cth)*
Contracts	• *Electronic Transactions Act 1999 (Cth)*
Privacy	• *Privacy Act 1998 (Cth)* • State/Territory privacy legislation • OFPC PKI Privacy guidelines • Gatekeeper privacy requirements

[122] See *Chapter 5. The current legal and regulatory framework for electronic authentication in Australia* in this paper for more details.

7.4. Assessment

This section examines the role of electronic authentication in enabling assessment to take place in an online environment – free from the usual physical forms of supervision. It also considers the integrity of the assessment components of flexible learning, to assess whether electronic authentication will be acceptable for assessment purposes, including the avoidance of fraud, time stamping etc.

The US Army training program (described previously) provides a range of distance and online assessment options. They have considered the potential for authentication in assessment, and have concluded that a system of 'gates' may be required in order to ensure integrity.[123] These 'gates' include:

- **Learning Interactions**
  Training design needs to provide the right interactions at the right time. Interactions are reciprocal events requiring two objects (e.g., student and instructor) and two actions (e.g., an email and a reply). Such interactions foster behaviours in which individuals and groups influence one another. The hallmark of interactions is that they must result in the transfer of knowledge or a change in intrinsic motivation.

- **Natural Points**
  Interactions provided for learning can also act as natural points for identification, authentication and monitoring of participants within the conversational framework of the learning activities. Instructional design can provide for validation actions at these points without unduly interrupting the flow or distracting from the intent of the learning activities.

- **Social Interactions**
  Providing social interactions in the learning environment can create a sense of community and personal involvement while allowing positive identification of learners. Creating opportunities to acquaint learners with each other, the instructor, and subject matter experts increases the situational awareness of each participant and decreases the feelings of isolation often associated with distributed delivery. Some examples are the inclusion of personal essays, chat rooms, social greeting time and instructor office hours in the virtual learning environment.

- **Continuous Assessment**
  Distributed learning can be an outstanding enabler of continuous learning because of the ability to participate while widely dispersed in time and geographic location. Learning can be accomplished as needed rather than in an episodic, higher directed fashion. However, in order to truly embrace continuous learning, the design must include the associated continuous assessment required to determine what is required and when. This continuous assessment interaction provides many more opportunities to gather information about the learner and increase the level of confidence that the learner has, in fact, grasped the required concepts.

[123] Summary of the presentation by Dr. Mike Freeman, Director, Advanced Training Concepts, Computer Science Corporation, Atlanta, GA. Also see Curnow et al., footnote 103.

In practice, it seems likely that these types of 'gates' or 'interactions' will allow assessment to take place in an online flexible learning environment. The integrity of the assessment will be increased by the number of interactions which involve authentication (making it difficult for cheating students to slip through the cracks). There do not appear to be any specific legal obstacles to adopting this approach.

The following table points to sources of legal guidance for assessment issues:

Assessment – Legal Issues	Legal guidance[124]
Authentication of learners for assessment	• OFPC PKI Privacy guidelines • Gatekeeper privacy requirements
Authentication of learners for a learning passport and records of achievement	• VET legislation • Qualification Authority legislation (where applicable)
Cheating (plagiarism, identity fraud)	• *Cybercrime Act 2001 (Cth)*
Contracts	• *Electronic Transactions Act 1999 (Cth)*
Privacy	• *Privacy Act 1998 (Cth)* • State/Territory privacy legislation • OFPC PKI Privacy guidelines • Gatekeeper privacy requirements

7.5. Relying parties

This section examines the issues raised by electronic authentication for relying parties – third parties who rely on the electronic authentication system for authentication (of identity or attributes) integrity, non-repudiation, and/or confidentiality.

Relying parties in the VET sector may include:

— **Employers**
Employers need to be confident that the qualifications of current and prospective employees are accurate. They may have legal obligations to ensure that staff meet certain minimum qualifications (e.g. first aid qualifications for transport staff). However, they will also have a broader interest in the nature of the employee's achievements, the currency of qualifications (i.e. year of completion), the marks achieved, and in some cases the identity and authenticity of the education provider.

— **Recruitment agencies**
Recruitment agencies have the same needs as employers. However they may also have additional legal obligations (through warranties provided to employer clients) to ensure the accuracy of qualifications.

[124] See *Chapter 5. The current legal and regulatory framework for electronic authentication in Australia* in this paper for more details.

— **Licensing authorities**
There are numerous fields of employment where a licence is required. The authority which issues the licence (such as the Australian Securities and Investments Commission which issues financial services licences for financial planners, insurance brokers etc.) needs to be confident that the qualifications have been obtained and are up to date.

— **Other VET providers**
In order for electronic authentication and flexible learning to succeed, VET providers will have to be able to trust two important aspects of the system. Firstly, any student enrolled by one institution may be automatically authenticated by other VET providers (see *Chapter 8. Models for electronic authentication in VET* for how this could work in practice) without requiring all the normal enrolment steps. Secondly any assessments or qualifications which are cross recognised under the flexible learning framework may be automatically authenticated without reliance on traditional paper based systems.

— **Other education institutions**
There is significant crossover between secondary education and VET, and VET and higher education. Authentication of assessment, providers, learners and qualifications (especially for cross recognition of partial qualifications) will become an essential requirement of flexible learning as the traditional divisions between the three sectors become less distinct.

The reliance on electronic authentication by third parties (such as employers who may be relying on evidence of qualifications) is an area which raises significant legal concerns. The Australian Government Solicitor recognised this in the following advice to ANTA-FLAG:

> 'An educational institution might commission a Certification Authority (CA) to provide certification products and services to its students. The institution might face breach of contract if it or its students breach the terms of a subscriber agreements with the CA. Subscriber Agreements usually seek to shift liability in relation to certification products and services from the CA to the Subscriber, so the institution may face liability arising from loss incurred by a third party or the student. If the certification products and services do not allow access to products and services by the disabled - e.g. the sight impaired - the institution may face liability for disability discrimination. If the institution makes false representations to the CA (e.g. providing incorrect student identity information) or to students (e.g. about the performance of a CA or its products and services) which lead to loss or damage, the institution may be liable in negligence or estoppel. If it is held to be carrying on a business, it may also be liable for breach of implied statutory terms, or misleading or deceptive conduct under the *Trade Practices Act 1974 (Cth)*.'[125]

Many of the detailed legal issues can only be considered individually, or at least only within the context of a particular electronic authentication model (see *Chapter 8. Models for electronic authentication in VET*).

[125] Ibid., footnote 100, page 5.

Until an electronic authentication model is chosen only limited guidance on legal issues can be considered.

Relying Parties – Legal Issues	Legal guidance[126]
Protection of privacy within the authentication system when information is exchanged between learners (or other participants) and third parties	• OFPC PKI Privacy guidelines • Gatekeeper privacy requirements
Allocation of liability for losses resulting from the failure of authentication	• Contract • Common law (see NEAC reports)
Authentication of learners for a learning passport and record of achievements	• VET legislation • Qualification Authority legislation (where applicable)
Contracts	• *Electronic Transactions Act 1999 (Cth)*
Privacy (general)	• *Privacy Act 1998 (Cth)* • State/Territory privacy legislation • OFPC PKI Privacy guidelines • Gatekeeper privacy requirements

[126] See *Chapter 5. The current legal and regulatory framework for electronic authentication in Australia* in this paper for more details.

7.6. Transactions – subscription, payment and enrolment

This section examines the impact of electronic authentication on the integrity of transactions, such as subscription, payment and enrolment.

Subscription, payment and enrolment are common transactions which are common to ain a wide range of government and business activities. The legal issues which arise in these transactions are not specific to flexible learning.

The majority of legal issues raised in these transactions are now subject to clear legal guidance. However, some of the law in this field remains unsettled, including the allocation of liability in PKI transactions.

The following table provides pointers to the main legal documents relevant to electronic authentication and flexible learning transactions:

Transactions – Legal Issues	Legal guidance[127]
Identity fraud	• *Cybercrime Act 2001 (Cth)*
Payment system fraud	• EFT Code of Conduct, Standards
Formation of contract	• *Electronic Transactions Act 1999 (Cth)*
Liability for unauthorised transactions	• EFT Code of Conduct • Contractual terms • Common law (see NEAC reports)
Privacy	• *Privacy Act 1988 (Cth)* • State/Territory privacy legislation • OFPC PKI Privacy guidelines • Gatekeeper privacy requirements

[127] See *Chapter 5. The current legal and regulatory framework for electronic authentication in Australia* in this paper for more details.

Chapter 8. Models for electronic authentication in VET

This paper identifies a requirement for the VET sector to develop appropriate and effective electronic authentication arrangements.

In this chapter Galexia Consulting describes five potential models for the development and implementation of electronic authentication in the VET sector:

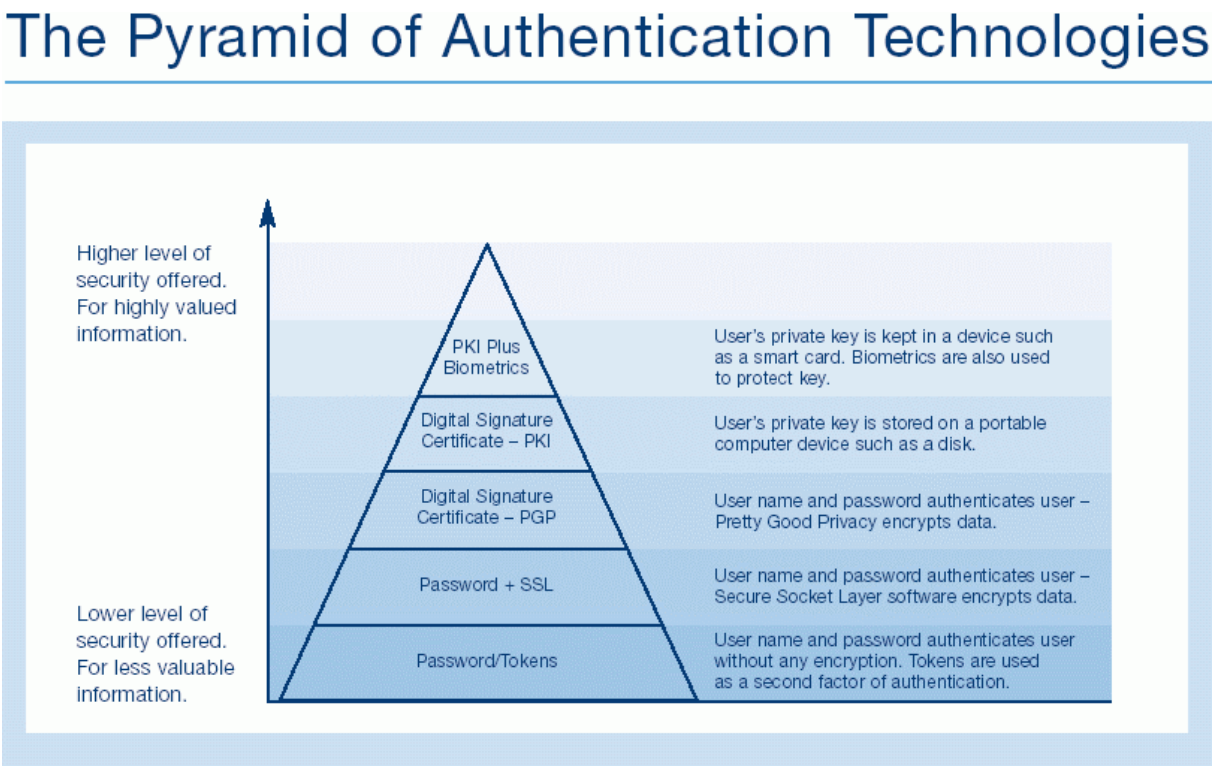
- *Authentication Model 1 – Ad hoc arrangements*
- *Authentication Model 2 – Tool-box of electronic authentication solutions*
- *Authentication Model 3 – Tool-box of electronic authentication solutions – with limited centralised functions*
- *Authentication Model 4 – Tool-box of electronic authentication solutions – with some centralised functions plus standards*
- *Authentication Model 5 – Central development or approval of electronic authentication solution*

Authentication Model 1 – Ad hoc arrangements

In this model, arrangements are similar to the current approach in the VET sector. Different forms of electronic authentication are used in individual applications. The choice of electronic authentication tool may be based on availability, the level of understanding of participants, or in some cases on a risk and cost/benefit analysis.

Some guidance is available for participants to make cost/benefit assessments in Australia. For example, NOIE have provided the following diagram[128] to assist organisations choose an appropriate electronic authentication tool:

[128] National Office for the Information Economy, *Trusting the Internet: Small business guide to e-security* (July 2002), <http://www.noie.gov.au/publications/NOIE/trust/trusting_the_internet.pdf>. Diagram available at page 13.



This 'ad hoc' model is currently utilised in the Australian VET sector. Numerous institutions have implemented their own electronic authentication system (e.g. TAFE Tasmania), and small networks of VET providers have also formed mini authentication networks (such as the six printing and graphic arts VET providers participating in an 'Electronic Skills Passport'[129]).

Authentication Model 1 – Ad hoc arrangements	
Pros	**Cons**
No additional expenditure required	Overall costs (such as overlaps in development costs) may be high
Allows 'market' to dictate technology	No control on quality of individual authentication
Low risk approach	May cause interoperability barriers
Can wait for other sectors to develop more sophisticated models (e.g. may piggyback on other PKIs at a later date)	No level playing field for small RTOs
	No progress on legal and regulatory issues - Risk that flexible learning initiatives will not progress

[129] <http://www.skillspassport.net>.

Authentication Model 2 – Tool-box of electronic authentication solutions

In this model a central body (potentially ANTA) would provide access to a tool-box of electronic authentication solutions which are considered suitable for use in the VET sector. This could be through an 'approved' vendor list and/or a web portal with descriptive information and links to vendor solutions (perhaps with case studies).

A further option would be to explore bulk purchasing arrangements for the VET sector through a competitive tender process. However, decisions to purchase solutions from the electronic authentication tool-box and their practical implementation would be determined by individual VET providers (or small networks/consortiums).

Authentication Model 2 – Tool-box of electronic authentication solutions	
Pros	**Cons**
Potential for discounted products	Little impact on overall quality
Chosen electronic authentication solutions would be suitable (and potentially customised) for VET	No progress on legal and regulatory issues - Risk that flexible learning initiatives will not progress
VET providers would have a one stop shop for purchasing tools	No level playing field

Authentication Model 3 – Tool-box of electronic authentication solutions – with limited centralised functions

In this model, ANTA (or a similar body) would provide additional functions for the VET sector regarding electronic authentication. Rather than simply acting as a conduit between VET providers and electronic authentication vendors, they would add an additional layer of technical support, education, and professional development. They may conduct research and evaluations which would provide guidance. However the impact on the quality of electronic authentication in the sector may be limited as there would not be a central function to drive a particular electronic authentication solution.

This model is similar to the model being investigated in the higher education sector in Australia through the Collaborative Online Learning and Information Services (COLIS) project. [130] This project was funded by DETYA (now DEST) to achieve the following objectives:

- Establish a test bed for the development of collaborative online learning and information services develop a scalable standards based model for institutional interoperability which enables the seamless sharing of online learning and scholarly information resources;
- Contribute more fully to the work of the Instructional Management System (IMS) Global Learning Consortium; and
- Link with international software companies, corporate management systems providers, learning management systems, content producers, and national government agencies

The COLIS Consortium consists of Macquarie University, University of Newcastle, University of New England, University of Southern Queensland and the University of Tasmania.

Although this project is being undertaken in the higher education sector, some of the work is instructive for the VET sector and flexible learning in particular. Their early conclusions are that the following components are required to establish a successful flexible learning environment:

- Interactive tools to support a range of authoring environments;
- Student-centric interfaces for customised/personalised learning and training;
- Transparent means of importing learning objects and learning content from distributed repositories to centralised and distributed learning management systems;
- Strong authentication and authorisation processes;
- Interaction between disparate learning management systems;
- Search/discovery capacity across distributed information resources including libraries, museums, archives, commercial information services and the Web, together with learning object repositories;
- Digital asset management systems;

[130] <http://www.colis.mq.edu.au/>.

- Digital rights management infrastructure, which tracks and records the use and re-expression of resources and permits trade where necessary;
- Agreed application profiles for the application of multiple metadata schema to support digital asset management systems;
- Flexible web publishing systems; and
- Strong delivery platforms.

The work of COLIS has helped to establish some of the more detailed technical requirements for electronic authentication to succeed. This model could provide similar benefits in the VET sector. However, COLIS is yet to address legal and regulatory issues.

Authentication Model 3 – Tool-box of electronic authentication solutions – with limited centralised functions	
Pros	**Cons**
Helps promote understanding and awareness	Does not address legal and regulatory issues - Risk that flexible learning initiatives will not progress
Research can identify and solve issues and obstacles	Will not necessarily result in inter-operability or cross recognition
Technical support can help balance the level playing field	Does not ‘drive’ take up across the whole sector

Authentication Model 4 – Tool-box of electronic authentication solutions – with some centralised functions plus standards

In this model a central body would emerge with a stronger role in driving inter-operability of electronic authentication within the VET sector. By adding standards to the tool-box and other functions, the central body can ensure the majority of authentication solutions are suitable for the VET sector and will work together.

When it moves beyond its early pilot stage, the COLIS case study noted previously in *Authentication Model 3.* may follow this model as it includes reliance on the underlying IMS protocols, which may become a de facto standard for electronic authentication in the education sector.

In Europe, this model has been adopted through the *Task Force – Authentication, Authorisation Coordination for Europe* (TF-AACE) project.[131]

This project encourages and supports cooperation between education providers and other project teams by developing and deploying interoperable authentication and authorisation infrastructures and services for the education community in Europe.

The Task Force provides a forum for exchanging experiences and knowledge in the area of authentication and authorisation technologies and their deployment. TF-AACE also coordinates the education community's contribution to the standardisation process through liaison with the appropriate standards groups (e.g. IMS and Internet2).

Authentication Model 4 – Tool-box of electronic authentication solutions – with some centralised functions plus standards	
Pros	**Cons**
Strong potential for interoperability	Some costs now incurred by central agencies, without guarantee of wide take-up
Strong potential that solutions will be suitable for VET	Some legal and regulatory issues will remain unresolved, despite the wide adoption of standards
Greater likelihood of take-up in the VET sector	

[131] Trans European Research and Education Networking Association (TERENA), *Authentication and Authorisation Coordination for Europe Task Force (TF-AACE), Terms of Reference* (8 April 2002) <http://www.terena.nl/tech/task-forces/tf-aace/tf-aace-tor.html>.

Authentication Model 5 – Central development or approval of electronic authentication solution

This is the most ambitious model, and involves making central decisions about the adoption of electronic authentication across the whole VET sector, determining appropriate electronic authentication solutions, and liaising and coordinating with other sectors (such as higher education).

An example of this model being adopted is JISC, in the United Kingdom. JISC has helped to establish a large scale authentication system through the Athens project.[132] JISC plays a role in upgrading and expanding authentication services in the sector. There is a migration strategy from ad hoc arrangements, to 'single sign on' services, to electronic authentication enabled by PKI.

This electronic authentication model may deliver a range of benefits to flexible learning. Applications could also include a national skills passport to help tie together the various electronic records in the sector from the learner's perspective.

This model is also contemplated in the IMS Global Learning Project in the following scenario:[133]

> 'Prior to admission of a learner to a university there is a selection process involving the learner, university admissions tutors at up to 6 universities and an intermediary body, with which learners deal directly. As a result of the process, admission to a course is agreed and learner data with validated qualification information is created and lodged with the university profile server.
>
> At the point of enrolment the learner adds to information stored with personal information and preferences. As a learner progresses through a course the learner profile server is given data on marks achieved and the course context. If a course is shared with another provider then that other provider can interoperate with the profile server across the Internet to store marks achieved in the context of that provision.
>
> During a course a learner may wish to move from one provider to another, for example studying the first year at one university and the second and subsequent years at a university with a nearly equivalent course. Admission to the second university involves looking at the course content and prerequisites and learner achievement for each course or module to determine whether the prerequisites for the course at the second university have been met. This in turn requires examining the detail of context and marks at different granularities in different areas of the course. As learners may take time out of courses between years, detail needs to be relevant to the instance of the course that was actually followed and that will be followed.

[132] <http://www.athensams.net>.

[133] Note: Although this hypothetical involves a university, the scenario is also relevant for the VET sector.

> For a learner studying a course with an industrial placement component it is desirable that detail of the learner's abilities in particular areas, can be provided to potential placement providers (employers) to assist them with selecting appropriate candidates. At the end of a course information about a learner's achievements, both on the course and in other areas can be provided, under the learner's control, to prospective employers. When the learner applies to take courses at other institutions in the future, a record of qualifications and abilities can be made available.'[134]

Although this model appears ambitious, the building blocks are available. Underlying 'defacto standards', such as the IMS protocols have been developed, and there is a range of electronic authentication solutions which could be customised for use in the VET sector.

Authentication Model 5 – Central development or approval of electronic authentication solution	
Pros	**Cons**
Avoids the costs of ad hoc arrangements developing (and the difficulties of untangling such arrangements in the future)	Significant up front development costs and ongoing maintenance costs – business case needs analysis is required
Ensures sector wide interoperability	Requires significant leadership and awareness raising
Potential for interoperability with other sectors	Some risk of being 'first mover' rather than waiting for another sector to implement a national solution
Potential to resolve majority of legal and regulatory issues through central action – law reform and model clauses	Mobile/transient student population may make VET an unsuitable sector for first implementation
Ensures a level playing field for all RTOs	Some legal uncertainty will remain regarding allocation of liability

[134] IMS Global Learning Consortium Inc, *IMS Digital Repositories White Paper* [version 1.6] (21 August 2001) <http://www.imsproject.org/imsdr_whitepaper_v1p6.html>.

Chapter 9. Findings and Recommendations

- *Recommendation 1 – Develop an electronic authentication strategy for the VET sector*
- *Recommendation 2 – Rely on contractual terms until law and future strategy are settled*
- *Recommendation 3 – Determine role of ANTA*
- *Recommendation 4 – Increase awareness of electronic authentication in the VET sector*
- *Recommendation 5 – Coordinate with other education sectors*
- *Recommendation 6 – Establish an electronic authentication agency for the VET sector*
- *Recommendation 7 – Participate in law reform process*
- *Recommendation 8 – Further research*

During the research for this paper, Galexia Consulting confirmed that there are a number of legal and regulatory obstacles to the successful development and implementation of electronic authentication for flexible learning in the VET sector.

The main issues are:

- Legal uncertainty caused by the continuing absence of a general regulatory framework for electronic authentication (a situation which we expect to continue in the medium term); and
- Legal uncertainty regarding the allocation of liability between participants in authenticated transactions as part of a Public Key Infrastructure.

A number of other legal issues have been resolved in Australia, including those surrounding electronic payments and the difficult issue of forming contracts via purely electronic means (i.e. without paper copies or handwritten signatures).

This paper has identified the importance of privacy issues in electronic authentication and discusses strategies to ensure that privacy is protected in the majority of transactions and electronic authentication scenarios.

The importance of particular legal issues depends on the electronic authentication model adopted in the VET sector. This paper identifies five potential models for electronic authentication in the flexible learning environment.

There are benefits for the VET sector in migrating to a strong, centrally managed, coordinated electronic authentication model. These include:

- **Reduction in cheating**
  There is potential for significant reduction in opportunities to cheat in the VET sector if strong electronic authentication systems are developed. Electronic authentication may provide a deterrent to cheating through strong registration processes (which help to reduce opportunities for identity fraud) and improvements in message integrity during interactions between learners and VET providers.

- **Improved user convenience**
  There is potential for significant enhancement to user convenience, simplicity, customisation and service if a sector-wide electronic authentication solution is developed. For example, a system which provided 'single sign on' for all VET providers could reduce the number of login names and passwords which participants have to remember, and the development of a skills passport could provide a convenient, portable mechanism for carrying strong evidence of qualifications. These improvements in user convenience are probably of greater benefit than the potential impact on cheating.

- **Improved system integrity, operability and flexibility**
  There is potential for a sector wide electronic authentication solution to provide significant advantages over the current system of ad hoc electronic authentication initiatives. These benefits include greater trust and confidence in the integrity of the system, greater interoperability between applications across the sector, and greater flexibility for participants as they move between VET providers.

- **Improved cross recognition of assessment and qualifications**
  Electronic authentication may enhance trust and confidence in the cross recognition of assessment and qualification – a major objective in flexible learning.

A strong national electronic authentication solution across the entire VET sector will not be achieved quickly. Our recommendations contemplate a staged migration path.

The Australian VET sector has not yet advanced beyond *Authentication Model 1* (ad hoc arrangements). The Australian non-VET sector (e.g. higher education) is slightly more advanced and is presently positioned between *Authentication Model 3* (tool-box plus limited support) and *Authentication Model 4* (tool box plus standards).

Other jurisdictions are more advanced, especially the United Kingdom where they are close to successfully implementing *Authentication Model 5* – a centrally developed and approved electronic authentication solution across the entire education sector.

It is our conclusion that electronic authentication (and hence flexible learning) is unlikely to advance further in the VET sector without implementation of *Authentication Model 5.* We have set out the following recommendations to assist ANTA CEOs and their Ministers for Education develop migration path - a planned and scaleable way forward.

Recommendation 1 – Develop an electronic authentication strategy for the VET sector

It is recommended that FLAG advise ANTA CEOs that it is important to develop an electronic authentication strategy for the VET sector and take a high level policy decision to pursue that strategy. This will require further exploration of appropriate electronic authentication models for the VET sector. The models described in ***Chapter 8. Models for electronic authentication in*** VET may provide a useful starting point.

ANTA CEOs should determine how such a strategy will be developed. This research paper may assist participants in the VET sector to understand the strategic issues for electronic authentication and determine an appropriate strategy. If an authentication strategy is not selected, the VET sector runs the risk of drifting while other jurisdictions make progress in building trust and confidence in their flexible learning environments.

Recommendation 2 – Rely on contractual terms until law and future strategy are settled

Until some of the legal issues surrounding electronic authentication have been settled (see Recommendations 6 and 7 below), and while developing an electronic authentication strategy for the VET sector, it will be important to deal with current legal issues with the resources available. In practice, this will require a reliance, within current ad hoc arrangements, on the following tools:

- General education about legal issues;[135]
- Contractual terms to allocate legal liability between parties in any transaction relying on electronic authentication; and
- General privacy policies.

It is recommended that FLAG advise ANTA CEOs that it is necessary to provide some interim guidance to the sector on model contractual clauses and model privacy policies which take electronic authentication legal issues into account.

The development of the model contractual clauses and model privacy policies could be co-ordinated by ANTA and distributed via communication channels already developed for the Australian Flexible Learning Framework.

[135] Similar to the information currently provided in the Flexible Learning Legal Kit, with more detail on electronic authentication legal issues <http://flexiblelearning.net.au/legal/kit.html>.

Recommendation 3 – Determine role of ANTA

There is a need to determine the role of ANTA within the context of a national electronic authentication framework for the VET sector.

In other jurisdictions, progress has been assisted by the presence of a single body with a clear role to lead and drive the process – such as JISC in the United Kingdom. An alternative role is to provide insight and coordination, without necessarily being the final decision maker – this is closer to the role which COLIS plays in the higher education sector in Australia.

In the absence of a clear leader, the sector has a tendency to drift. This was the experience in the higher education sector prior to the introduction of the COLIS project:

> 'Over the past five years a great deal has been written about authentication and authorisation, but effective solutions have proved elusive. It is significant that most service stakeholders in the higher education environment generally assume that it is 'someone-else's-problem-to-solve.' The principal problem continues to be the lack of conceptual and practical understanding of how to match people and resources using schema based on directory services. There is also a lack of understanding of the type of directory services required to sustain a distributed services environment.'[136]

Strong, centralised, leadership and coordination will build momentum behind electronic authentication, while opportunities will still exist for commercial vendors to compete for market share by providing the highest quality electronic authentication tools.

Our recommendation is that FLAG advise ANTA CEOs that there is a need for a centralised body to provide strong national leadership, similar to JISC in the United Kingdom, which is capable of decision making on behalf of the VET sector.

[136] Neil McLean, Macquarie University Library, *Interoperability convergence of online learning and information environments* (2001) <http://www.colis.mq.edu.au/news_archives/convergence.pdf>.

Recommendation 4 – Increase awareness of electronic authentication in the VET sector

There is a danger that the Australian VET sector will fall behind other education sectors (especially overseas) through the absence of a wide understanding of the importance of electronic authentication.

In the higher education sector, COLIS recognises the significance of education and awareness:[137]

- Different 'world-views' of the nature of the problem being solved between librarians and IT directors, with librarians regarding it as a matter of access to global information resources and IT directors viewing it as being primarily a matter of security and access control;
- A fundamental blurring of the distinction between authentication and authorisation;
- A lack of appreciation of the role of directory services in terms of access management relating to people, resources and services;
- A preoccupation with institutional access management protocols at the expense of much needed distributed services architectures and heavy reliance on proprietary directory solutions which do not scale; and
- Little concept of how portal technologies link and take advantage of directory services.

It is recommended that a nationally co-ordinated program of general awareness raising and detailed professional development for key participants in the VET sector is undertaken.

Recommendation 5 – Coordinate with other education sectors

We recommend the VET sector coordinates its electronic authentication activities with other education sectors, especially higher education considering their advanced state (through COLIS).

The process of consultation and coordination should begin immediately, and may be enhanced by some joint projects (e.g. in relation to the skills passport) or joint research (e.g. research on international developments).

[137] Neil McLean, Macquarie University Library, *Libraries and E-Learning: Organisational and Technical Interoperability* (March 2002) <http://www.colis.mq.edu.au/news_archives/lib_e_learning.pdf>.

Recommendation 6 – Establish an electronic authentication agency for the VET sector

The required work on electronic authentication in the VET sector needs a commercial foundation. It may require the establishment (or seed funding) of a third party agency to develop an electronic authentication solution for the VET sector. In the United Kingdom this role is performed by a commercial provider (Athens). However, other options may need to be explored in Australia due to the smaller scale of the sector. These options might include:

1. Asking one existing institution (such as a large TAFE) to play a leadership role and coordinate and develop solutions.
2. Forming a not for profit organisation (and providing it with seed funding) or attaching an appropriate program to an existing VET not for profit organisation.
3. Issuing a request for tender and directly funding the most appropriate respondent.

It is important to re-state that the costs of allowing existing ad hoc arrangements to continue and spread may be quite high in the long term. Untangling existing arrangements at a later stage and attempting to replace them with an inter-operable solution will be costly. These potential costs should be borne in mind when considering this recommendation.

Recommendation 7 – Participate in law reform process

The VET sector would benefit from more active participation in the law reform process surrounding outstanding legal issues in electronic authentication.

We recommend maintaining a watching brief on relevant law reform, and active participation in that process (through submissions, seminars, meetings with key regulators etc.).

Two key law reform processes at this time are:

1. **National Authentication Technology Framework**
   A process (coordinated by NOIE) examining the broad legal and regulatory framework for electronic authentication.
2. **Legal Liability in Electronic Authentication**
   A process (begun by NEAC and now coordinated by NOIE) examining the allocation of legal liability in PKI transactions.

Recommendation 8 – Further research

Further research may be required on a range of strategic issues in electronic authentication in the VET sector

This may include:

1. Research matching specific legal issues against the chosen authentication model (ie a more detailed legal paper than the current document, once broad strategic decisions have been made about the likely electronic authentication solution).
2. Development of common contractual clauses across the VET sector to allocate legal liability in electronic authentication.
3. Research on the cross recognition of qualifications and the inter-relationship between cross recognition, VET legislation and electronic authentication.
4. Research on international developments – both from a legal and a strategic perspective.
5. Research on jurisdiction issues for cross recognition and cross border transactions. For example, the application of privacy law when learner and VET provider are located in different states.

Table of Authorities

Codes of Conduct

Gatekeeper

Guidelines

Legislation

NEAC Reports

Reports

Standards

Glossary and Acronyms

ABN-DSC

Australian Business Number Digital Signature Certificate

AICTEC

Australian Information and Communication Technology Education Committee

AFL Framework

Australian Flexible Learning Framework – <http://www.flexiblelearning.net.au> – see also *1.2. Background* in this paper.

ANTA

Australian National Training Authority – <http://www.anta.gov.au>.

ASIC

Australian Securities and Investments Commission – <http://www.asic.gov.au>.

Athens

The *Athens Access Management System* provides authentication services to the UK Higher Education and Further Education community. Athens provides education users with single sign on to numerous web-based services throughout the UK and overseas. Athens is a system which combines the functions of authentication and authorisation, but not profiling. This combination of authentication and authorisation is termed access management in the title of the Athens service and in its documentation <http://www.athens.ac.uk/>.

Authentication

See *Chapter 2. What is electronic authentication?.*

AVETMISS

Australian Vocational Education and Training Management Information Statistical Standard - <http://www.ncver.edu.au/statistics/avetmiss40>.

Biometric

Biometric verification is any means by which a person can be uniquely identified by evaluating one or more distinguishing biological traits.

Certificate

See Digital certificate.

Certification Authority (CA)

An authority trusted and authorised to issue and revoke digital certificates.

Certificate Revocation List (CRL)

A list of digital certificates that have been revoked or suspended prior to their expiry date.

Certificate Practice Statement (CPS)

A statement of practices that the PKI and its customers must conform to.

COLIS

Collaborative Online Learning and Information Services – <http://www.colis.mq.edu.au>.

CMS

Content Management System.

Cryptography

The science of transforming clear, meaningful information into an enciphered, unintelligible form using an algorithm and a key.

DEST

Department of Education Science and Training – <http://www.dest.gov.au>.

Digital certificate

An electronic document signed by a CA which associates a subscriber (by identification and/or attribute information) with a key pair (by specifying the public key of that key pair)

DRMS

Digital Rights Management System

Digital signature

A Digital signature is an electronic mark (block of data encrypted with a private key, and which can only be decrypted with a public key) that only the sender of an electronic transmission can make but which is easily recognised as belonging to the sender.

Directory Services

Used to store information about users, including their public key.

EdNA

Education Network Australia – <http://www.edna.edu.au>.

Electronic authentication

See *Chapter 2. What is electronic authentication?*

ETA

Electronic Transactions Act 1999 (Cth) – See *5.1.1.*

EVAG

The EdNA VET Advisory Group (EVAG) is now known as FLAG. This change occurred during 2001.

Federated Administration

'Federated administration is a way of making authentication, authorisation, attributes, etc. useful to other domains that are willing to trust the information in a lightweight, distributed fashion. This allows for items of information that are established in one domain to be trusted in another domain based on the trust relationship between the two domains. Doing so can reduce administrative burdens for all parties concerned without relying on a central authority or similar service to perform extensive operations. A registry service is often still needed to host agreements reached by the federation, trusted information about which members are in the federation, or who is authoritative for which entity.'[138]

FLAG

Flexible Learning Advisory Group

Gatekeeper accreditation

Accreditation by NOIE of a CA or RA granted on the basis that they meet the criteria set out in the Gatekeeper accreditation documents.

Hash

A user digitally signs a message by encrypting a hash of the message with the signing private key. The message is submitted to a hash function (a mathematical computation) and the output is known as the hash.

IMS Project

Instructional Management Systems (IMS) Global Learning Consortium, Inc – <http://www.imsproject.org>

Internet2

Internet2 is a collaboration among more than 100 US universities to develop networking and advanced applications for learning and research. Internet2 intends to investigate and develop new ways to use the Internet and the Internet2 infrastructure for its educational purposes. Internet2 is investigating 'Distributed learning modules.' Internet2 may also help realise the Instructional Management System (IMS), a standard process for using the Internet in developing and delivering learning packages and tracking outcomes – <http://www.internet2.edu/>.

IPP

Information Privacy Principle – See *5.1.2 Privacy Act 1998 (Cth) – Commonwealth Public Sector requirements.*

JISC

Joint Information Systems Committee – <http://www.jisc.ac.uk/>

[138] <http://shibboleth.internet2.edu/shib-faq.html>.

Kerberos

Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. Kerberos lets a user request an encrypted "ticket" from an authentication process that can then be used to request a particular service from a server. The user's password does not have to pass through the network.

Key pair

A pair of asymmetric cryptographic keys (i.e. one decrypts messages which have been encrypted using the other) consisting of a public key and a private key.

LDAP

Lightweight Directory Access Protocol – See *Directory Services*.

LMS

Learning Management System.

NCVER

National Centre for Vocational and Education Research – <http://www.ncver.edu.au>.

NOIE

National Office for the Information Economy – <http://www.noie.gov.au/>.

NPP

National Privacy Principle – See *5.1.3. Privacy Act 1988 (Cth) – Private sector requirements.*

PIN

Personal Identification Number.

Private Key

The part of a two part cryptographic key-pair that is to be safeguarded by the owner (to ensure confidentiality, integrity, authenticity and non-repudiation). A private key can be used to generate a digital signature or decrypt encrypted information.

Public key

The published part of a two part cryptographic key-pair, which other users can make use of to send the owner encrypted documents and verify the owner's digital signature. Public keys are embedded in digital certificates.

Public Key Infrastructure (PKI)

Public Key Infrastructure – the total security management system (including hardware, software, people, processes and policies) used in verifying, enrolling and certifying users of a security application – see *2.3.*

Qualification Authority (QA)

Accreditation providers for participants in the VET sector – See *1.2.*

Registration Authority (RA)

An entity responsible to the Certification Authority for local identification of subscribers' identities.

Relying Party (RP)

See *7.5.*

RTO

Registered Training Organisation.

Shibboleth Project

'Shibboleth, a project of Internet2, is developing architectures, policy structures, practical technologies, and an open source implementation to support inter-institutional sharing of web resources subject to access controls. In addition, Shibboleth is developing a policy framework that will allow inter-operation within the higher education community.' See <http://shibboleth.internet2.edu/>.

SIS

Student Information System.

Smart card

A plastic card containing a microprocessor – may be used to store and securely access a digital certificate – see also *Token.*

Subscribers

Digital certificate holders.

Subscriber Agreement

The agreement between a subscriber and a CA for the provision of digital certificate services.

SSL

Secure Sockets Layer.

SSO

Single Sign On.

Token

A physical object, sometimes containing sophisticated electronics, which is required to gain access to a system – see also *Smart card.*

Trusted third party

An organisation providing security related services and activities to one or more entities in a given security infrastructure.

Validation Authority (VA)

See *6.2.4.*

VET

Vocational Education and Training.

Web Initial Sign-on (WebISO)

<http://middleware.internet2.edu/webiso/>.

Recommended Reading

Athens, *Access Management Service for UK Higher Education and Further Education community* <http://www.athens.ac.uk/>.

Australian National Training Authority (ANTA) (EdNA VET Advisory Group), *Flexible Learning for the Information Economy: Australian Flexible Learning Framework for the Vocational Education and Training System 2000 – 2004* (2000) <http://flexiblelearning.net.au/aboutus/aflframework2000.pdf>.

Australian National Training Authority (ANTA), *Flexible learning and the law* (2002 Information kit) <http://www.flexiblelearning.net.au/legal/kit.html>

Australian National Training Authority (ANTA), *A discussion starter for the next national strategy for vocational education and training 2004-2010* (January 2003) <http://www.anta.gov.au/images/publications/National_strategy-discussion_starter.pdf>.

Coalition for Networked Information, Clifford Lynch, Ed., *A White Paper on Authentication and Access Management Issues in Cross-organizational Use of Networked Information Resources* (Revised Discussion Draft 14 April 1998) <http://www.cni.org/projects/authentication/authentication-wp.html>.

Collaborative Online Learning and Information Systems (COLIS), *Website* <http://www.colis.mq.edu.au>.

Collaborative Online Learning and Information Systems (COLIS), Neil McLean (Macquarie University Library), *Interoperability convergence of online learning and information environments* (2001) <http://www.colis.mq.edu.au/news_archives/convergence.pdf>.

Collaborative Online Learning and Information Systems (COLIS), Neil McLean (Macquarie University Library), *Libraries and E-Learning: Organisational and Technical Interoperability* (March 2002) <http://www.colis.mq.edu.au/news_archives/lib_e_learning.pdf>.

Corporation for Research and Educational Networking (CREN), *PKI Resources* <http://www.cren.net/crenca/pkiresources/>

Corporation for Research and Educational Networking (CREN), *PKI-Lite Environment* <http://www.cren.net/crenca/pkilite/>

Crisp & Kearns, *Legal and Regulatory Framework - Research Report* (March 2001) <http://www.flexiblelearning.net.au/regulation2/Research_Report_Final.doc>

Curnow, Freeman, Wisher, Belanich and Moses (United States Army Research Institute for the Behavioral and Social Sciences), *Training on the Web: Identifying and Authenticating Learners* (June 2002), <http://www.ari.army.mil/pdf/authenticatingLearners.pdf>.

IMS Global Learning Consortium, *IMS Digital Repositories* Specification [version 1.0 final] (30 January 2003) <http://www.imsproject.org/digitalrepositories/>.

IMS Global Learning Consortium, *IMS Digital Repositories White Paper [version 1.6]* (21 August 2001) <http://www.imsproject.org/imsdr_whitepaper_v1p6.html>.

IMS Global Learning Consortium, *IMS Learner Information Package Specification [version 1.0]* (March 2001) <http://www.imsproject.org/profiles/>.

Internet2, EDUCAUSE, *eduPerson Object Class* <http://www.educause.edu/eduperson/>.

Internet2, *Shibboleth Project (Website)* <http://shibboleth.internet2.edu/>.

Internet2, *Shibboleth Architecture [Version 5 Draft]* (May 2002) <http://shibboleth.internet2.edu/docs/draft-internet2-shibboleth-arch-v05.pdf>.

Internet2, *Shibboleth Frequently Asked Questions (FAQ)* <http://shibboleth.internet2.edu/shib-faq.html>.

Internet2, *Shibboleth Project (Sample Campus Account Management Policy)* (May 2002) <http://shibboleth.internet2.edu/samplepolicy/>.

ITICSE 2002 Working Group, *Addressing Student Cheating* <http://www.csse.monash.edu.au/~mdick/ITICSEWorkingGroup/>.

Joint Information Systems Committee (JISC), *Website* <http://www.jisc.ac.uk/>.

Joint Information Systems Committee (JISC), Legal Information Service, *Website* <http://www.jisc.ac.uk/legal/>.

Joint Information Systems Committee (JISC), *Access Management Service for UK Higher and Further Education (Information Memorandum)* (2002) <http://www.jisc.ac.uk/index.cfm?name=funding_4_02>.

Joint Information Systems Committee (JISC), *Authentication, Authorisation and Accounting (AAA) Programme* <http://www.jisc.ac.uk/index.cfm?name=programme_aaa>.

Joint Information Systems Committee (JISC), Committee for Authentication and Security (JCAS), *Website* <http://www.jisc.ac.uk/index.cfm?name=jcas_home>.

Joint Information Systems Committee (JISC), Committee for the Information Environment (JCIE), *Website* <http://www.jisc.ac.uk/index.cfm?name=jcie_home>.

Joint Information Systems Committee (JISC), Committee for the Information Environment (JCIE), Alan Robiette, *The Future of Authentication for JISC Services* (Discussion Paper April 2002) <http://www.jisc.ac.uk/index.cfm?name=jcie_authentication>.

Joint Information Systems Committee (JISC), Committee for the Information Environment (JCIE), Alan Robiette, *Sparta: the Second-Generation Access Management System for UK Further and Higher Education* (Discussion Paper September 2000) <http://www.jisc.ac.uk/index.cfm?name=jcie_sparta>.

Joint Information Systems Committee (JISC), Committee for the Information Environment (JCIE), Alan Robiette, *X.509 certificates: frequently asked questions* (February 2002) <http://www.jisc.ac.uk/index.cfm?name=jcie_x509>.

Joint Information Systems Committee (JISC), *JISC Strategy 2001-05* (Supporting Paper) <http://www.jisc.ac.uk/index.cfm?name=strategy0105_supporting>.

Liberty Alliance, *Liberty Architecture Overview [version 1.1]* (15 January 2003) <http://www.projectliberty.org/specs/liberty-architecture-overview-v1.1.pdf>.

Monash University Information Technology Services, *Introduction to Digital Certificates* <http://www.its.monash.edu.au/security/certs/certintro.html>.

National Centre for Vocational and Educational Research (NCVER), *At a Glance: Flexibility through online learning* (2002) <http://www.ncver.edu.au/research/proj/nr1F12/nr1F12.pdf>.

National Electronic Authentication Council (NEAC), *Legal Liability in E-Transactions* (21 August 2000) <http://www.noie.gov.au/publications/NOIE/NEAC/publication_utz1508.pdf>.

National Electronic Authentication Council (NEAC), *The Legal Liability of Parties to a PKI Transaction* (8 May 2002) <http://www.noie.gov.au/publications/NOIE/Authentication/PKI_legal_report_May2002.pdf>.

National Office for the Information Economy (NOIE), *Gatekeeper Accreditation Information* <http://www.noie.gov.au/projects/confidence/Securing/GatekeeperAccreditation.htm>.

National Office for the Information Economy (NOIE), *Online Authentication – A Guide for Government Managers* (July 2002) <http://www.noie.gov.au/publications/NOIE/online_authentication/OnlineGuideFinal.pdf>.

National Office for the Information Economy (NOIE), *Towards a National Authentication Technology Framework* (May 2002) <http://www.noie.gov.au/publications/NOIE/Authentication/NATF_Discussion_paper_July2002.pdf>.

National Office for the Information Economy (NOIE), *Trusting the Internet – A small business guide to E-security* (July 2002) <http://www.noie.gov.au/publications/NOIE/trust/>.

Office of the Federal Privacy Commissioner (OFPC), *Guidelines to Information Privacy Principles* (October 1994) <http://www.privacy.gov.au/government/guidelines>.

Office of the Federal Privacy Commissioner (OFPC), *Guidelines to the National Privacy Principles* (September 2001) <http://www.privacy.gov.au/publications/nppgl_01.html>.

Office of the Federal Privacy Commissioner (OFPC), *Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to communicate or transact with individuals* (December 2001) <http://www.privacy.gov.au/publications/pki.rtf>.

TAFE Frontiers, *The Current Status of Online Learning in Australia* (2001) <http://www.tafefrontiers.com.au>.

Trans European Research and Education Networking Association (TERENA), *Authentication and Authorisation Coordination for Europe Task Force (TF-AACE), Terms of Reference* (8 April 2002) <http://www.terena.nl/tech/task-forces/tf-aace/tf-aace-tor.html>.

University of California (Office of the President), *Why UC Must Invest in a Public Key Infrastructure (PKI): The Case for Digital Certificates* (May 2000) <http://www.ucop.edu/irc/auth/whypki.pdf>.

University of California Common Authentication project, *Draft Guidelines on Management and Use of Digital Certificates* (November 1999) <http://www.ucop.edu/irc/auth/digcerts-draft.pdf>.

List of Consultations

Australian Council for Private Education and Training

Tim Smith
National Executive Officer

BlackBoard (USA)

Chris Etesse
Senior Director of Technology

Collaborative Online Learning and Information Services (COLIS)

Neil McLean
Director, IMS Australia

Columbia University (USA)

David Millman
Head of Technology, Columbia Digital Knowledge Ventures (DKV) (distance learning project)
Director, Digital Library, (R&D)

Educational Testing Service (USA)

Daniel Wakeman
Chief Architect, IT&S

National Office for the Information Economy (NOIE)

Tom Dale
General Manager, Regulation

TAFE NSW – New England Institute

Sam Meredith
Manager, Online Projects

TAFE Tasmania

Peter Higgs
Manager, Learning and Business Technologies

TAFE Virtual Campus – Office of Training and Tertiary Education – DET Victoria

Mark Bevelander
Unit Manger, Flexible Learning and Infrastructure
Office of Training and Tertiary Education – DET Victoria

University of Phoenix Online (USA)

Russ Paden
Vice President, Academic Services

WebCT (USA)

David Rosenbaum
Director of Marketing

Primary material sources – Where to go to find legislation

These links are sourced from http://scaleplus.law.gov.au.

Commonwealth Legislation

- Acts – Current Consolidations – http://scaleplus.law.gov.au/html/pasteact/browse/TOC.htm
- Statutory Rules – Current Consolidations – http://scaleplus.law.gov.au/html/pastereg/browse/TOC.htm

State and Territory Legislation

- Australian Capital Territory legislation – http://www.legislation.act.gov.au
- New South Wales legislation – http://www.legislation.nsw.gov.au
- Northern Territory legislation – http://www.nt.gov.au/lant/hansard/hansard.shtml
- Queensland legislation – http://www.legislation.qld.gov.au
- South Australia legislation – http://www.parliament.sa.gov.au
- Tasmania legislation – http://www.thelaw.tas.gov.au
- Victoria legislation – http://www.dms.dpc.vic.gov.au
- Western Australia legislation – http://www.slp.wa.gov.au/statutes/swans.nsf

Commonwealth Case Law

- High Court – http://www.highcourt.gov.au
- Federal Court – http://www.federalcourt.gov.au
- Administrative Appeal Tribunal – http://www.aat.gov.au
- Family Court of Australia – http://www.familycourt.gov.au
- Federal Magistrates Service – http://www.fms.gov.au
- Industrial Relations Court – http://www.austlii.edu.au/au/cases/cth/irc
- Migration Review Tribunal – http://www.mrt.gov.au
- National Native Title Tribunal – http://www.nntt.gov.au
- Superannuation Complaints Tribunal – http://www.sct.gov.au

State and Territory Case Law

- Australian Capital Territory SC – http://www.austlii.edu.au/au/cases/act/ACTSC
- New South Wales SC, CA, CCA – http://www.lawlink.nsw.gov.au
- Norfolk Is SC – http://www.austlii.edu.au/au/cases/nf/NFSC
- Northern Territory SC – http://www.austlii.edu.au/au/cases/nt/NTSC
- Queensland SC, CA, CCA – http://www.courts.qld.gov.au
- South Australia SC, CA, CCA – http://www.austlii.edu.au/au/cases/sa/SASC
- Tasmania SC, CA, CCA – http://www.courts.tas.gov.au/supreme
- Victoria SC, CA, CCA – http://www.austlii.edu.au/au/cases/vic/VSCA
- Western Australia – http://www.supremecourt.wa.gov.au

Contact

Framework Communications Team

Phone: 07 3247 5511

Fax: 07 3237 0419

Email: enquiries@flexiblelearning.net.au

Web: flexiblelearning.net.au

Australian Flexible Learning Framework

Supporting Flexible Learning Opportunities