Electronic Contract Administration – Legal and Security Issues Research Report

Report No. 2005-025-A

The research described in this report was carried out by the Australian Cooperative Research Centre for Construction Innovation.

Project Leader	Sharon Christensen (QUT LAW)
Team Members	Sharon Christensen, Bill Duncan (QUT LAW) Ed Dawson, Ernest Foo, Audun Josang (QUT IT/Security) Martin Betts, Debbie Smit (QUT BEE) Kerry London (UN)
Researchers	Kathryn O'Shea (QUT LAW) Judith McNamara (QUT LAW) Praveen Gauravaram (QUT IT/Security)
Project Affiliates	Ross Guppy, Michelle Walker (QDMR) Michael Austin, Dayv Carter (QDPW) Michael Hortz (BCC) Gerry Shutt, Geoff Gannon (JHG)

Research Program No:	A
Program Name:	Business and Industry Development
Research Project No.:	2005-025-A
Project Name:	Electronic Contract Administration – Legal and Security Issues
Date:	5 June 2007

Distribution List

Cooperative Research Centre for Construction Innovation
Sharon Christensen, Bill Duncan, Kathryn O'Shea, Judith McNamara (QUT LAW)
Ed Dawson, Ernest Foo, Audun Josang, Praveen Gauravaram (QUT IT/Security)
Martin Betts, Debbie Smit (QUT BEE)
Kerry London (UN)
Ross Guppy, Michelle Walker (QDMR)
Michael Austin, Dayv Carter (QDPW)
Michael Hortz (BCC)
Gerry Shutt, Geoff Gannon (JHG)

Disclaimer

The Client makes use of this Report or any information provided by the Cooperative Research Centre for Construction Innovation in relation to the Consultancy Services at its own risk. Construction Innovation will not be responsible for the results of any actions taken by the Client or third parties on the basis of the information in this Report or other information provided by Construction Innovation nor for any errors or omissions that may be contained in this Report. Construction Innovation expressly disclaims any liability or responsibility to any person in respect of any thing done or omitted to be done by any person in reliance on this Report or any information provided.

Please direct all enquiries to:

Chief Executive Officer
Cooperative Research Centre for Construction Innovation
9th Floor, L Block, QUT, 2 George St
Brisbane Qld 4000
AUSTRALIA
T: 61 7 3864 1393
F: 61 7 3864 9151
E: enquiries@construction-innovation.info
W: www.construction-innovation.info

Table of Contents

PREFACE

The Cooperative Research Centre (CRC) for Construction Innovation research project 2005-025-A *Electronic Contract Administration – Legal and Security Issues*, is supported by a number of Australian industry, government and university based project partners, including: Queensland University of Technology, Queensland Department of Public Works, Queensland Department of Main Roads, Brisbane City Council, University of Newcastle and John Holland Pty Ltd.

In support of this project's research aims and objectives, and as a deliverable for the project, this Report is intended to provide an overview of the current legal and security risks that may arise where Australian building and construction contracts are formed, administered and recorded within an electronic environment. Where appropriate, the Report also contains recommendations to minimise the legal and security risks that have been identified.

EXECUTIVE SUMMARY

The parties to the Cooperative Research Centre for Construction Innovation research project 2005-025-A *Electronic Contract Administration – Legal and Security Issues* (the 'E-contracting Project') have identified a need to develop guidelines for e-contracting in the construction industry. This Report considers the security and legal risks that result from the increasing adoption of information and communication technologies (ICT) in the construction industry for e-contracting purposes.

A range of legal and security issues may arise in connection with the electronic formation and administration of Australian construction contracts, and the electronic retention of construction project records. These issues were identified in the Literature Review for the E-contracting Project (available at http://www.construction-innovation.info/index.php?id=54)**.** This Report identifies the risks that result from those legal and security issues and makes recommendations to avoid or minimise the risks.

The legal and security risks associated with e-contracting in the construction industry are as follows:

- The time that an electronic contract has been formed may be uncertain.
- The place where an electronic contract has been formed may be uncertain.
- The authority of an individual to enter into a construction contract on behalf of another person or entity may be uncertain.
- Electronic communications may not satisfy statutory requirements for certain contracts to be in writing.
- Electronic communications may not satisfy statutory requirements for certain contracts to be signed.
- Depending on the terms of a construction contract, it may be uncertain whether electronic communications are effective to amend the contract.
- Depending on the terms of a construction contract, it may be uncertain whether electronic notices are valid.
- Disruptions to the availability of a project collaboration system may cause interference with the project.
- Incompatible technology may be used by the various contracting parties.
- Disputes may arise between the provider of an online collaboration system and the contracting parties in relation to the use of the system.
- Disputes may arise between the contracting parties regarding the use of the system.
- Disputes may arise in relation to the ownership of intellectual property associated with the project.
- The confidentiality of electronic records may be compromised during communication or retention.
- Electronic records created and maintained by a system may not be admissible in court as evidence in the event of a dispute.

- Electronic records created and maintained by a system may not be given the same evidential weight as paper records.
- There may be difficulty proving the time at which an electronic record has been communicated.
- The identity of the contracting parties may not be able to be authenticated.
- The process of disclosing relevant documents in the event of a dispute may be unmanageable as a result of multiple communication and record keeping methods.
- Parties may be in breach of their duty to preserve evidence if electronic records are not preserved.
- Parties may be in breach of their statutory obligations to maintain records if electronic records are not archived appropriately.
- Where a third party service provider is used, the contracting parties may not have access to electronic records after completion of the project.
- There is a risk that the statutory record keeping obligations of government agencies may be breached by using an online collaboration system.

This Report discusses each of the above risks and where appropriate, makes recommendations to eliminate or minimise the relevant risk. A proposed e-contracting architecture that addresses the identified security risks is also outlined in section 25 of this Report. The architecture incorporates security and functional features that will minimise the impact of the security risks that result from the formation, administration and recording of construction contracts in an electronic environment.

PART A: OVERVIEW

1. INTRODUCTION

1.1 Report structure

Part A of this Report is a general section intended to provide an overview of various legal and security matters relevant to e-contracting. It explains the background to the E-Contracting Project, its objectives and the research methodology that has been adopted. Part A examines the various aspects of an e-contracting process, the requisite security goals to be achieved and the various systems that may be used to conduct e-contracting. This part also describes the general legal principles that govern the electronic formation of contracts and the retention of electronic documents.

It is apparent from the general discussions in Part A that a number of legal and security risks may arise in connection with the electronic formation and administration of Australian construction contracts and the electronic retention of project records. Part B of this Report contains a detailed analysis of these legal and security risks and makes practical recommendations that may be implemented by industry to eliminate or minimise the identified risks.

Part C of this Report contains a proposal for an e-contracting system architecture that may be adopted to minimise many of the legal and the security risks associated with e-contracting. A final summary of the recommendations and conclusions in this Report is presented in a tabular format in Part D.

1.2 Background

The Cooperative Research Centre (CRC) for Construction Innovation research project 2002-067-A *E-business – Security and Legal Issues* (the 'E-tendering Project') identified a range of legal and security issues that may be encountered in electronic tendering in the construction industry. In addition to the issues that were identified for electronic tendering, the E-tendering Project revealed that if industry participants wished to proceed to the next stage of development, being the formation, administration and recording of contracts in a wholly electronic environment, further research in both the legal and computer security fields was warranted.

This Report is the outcome of that further research and is a deliverable for the E-contracting Project. The Report identifies the legal and security risks that may arise in connection with:

- the formation of construction contracts within an electronic environment;
- the electronic administration and management of construction contracts; and
- the management and retention of electronic records associated with construction projects.

Where appropriate, this Report also contains recommendations to minimise the legal and security risks that have been identified.

1.3 Research aims and objectives

The aims and objectives of the E-contracting Project are to:

- Identify the legal and security risks that arise when Australian building and construction contracts are formed, administered and recorded within an electronic environment; and
- Formulate practical recommendations that may be implemented by industry to minimise or eliminate the relevant legal and security risks.

1.4 Research methodology

Two phases of research were conducted for the E-contracting Project. The first phase involved case studies of electronic tendering systems used by the Brisbane City Council and the Queensland Department of Public Works.

The second phase of the project focussed on the legal and security risks resulting from electronic contract formation, administration and record keeping. The information, analyses and recommendations contained in this Report are the result of extensive research and investigations into e-contracting.

The research progressed through the undertaking and delivery of the following key project milestones:

- An extensive literature review of various national and international publications, legislation and court decisions relevant to e-contracting;
- A scoping study that identified and reviewed the security aspects of electronic collaboration systems currently used by construction industry participants in the administration and management of construction projects; and
- A case study report for John Holland Pty Ltd designed to assess the legal and security risks that may arise as a consequence of John Holland Pty Ltd's use of an online collaboration system to administer a significant construction project.

2. THE E-CONTRACTING PROCESS

2.1 General e-contracting process

In its broadest sense, e-contracting may be described as the process whereby any or all of the following activities take place within a purely electronic environment:

- the proposed parties to a contract negotiate and form their contract through the use of an electronic communication method;
- once the contract has been formed, the parties electronically administer and manage the contract (for example, the parties may use an online collaboration system to communicate with each other, deliver contractual notices, agree to contractual amendments, alter project drawings and provide project approvals); and
- upon completion of the contract, relevant project records and communications are archived using an electronic storage medium (as opposed to the traditional paper based method of record retention).

Each stage of the e-contracting process (as outlined above) gives rise to a number of legal and security risks. While the construction industry has been particularly receptive to the use of modern communication technologies to conduct business, it is essential that industry participants obtain an appreciation of the legal and security risks associated with e-contracting.

2.2 General legal principles governing the formation of electronic contracts

On a fundamental level, a contract is an agreement between parties that a court will enforce. An electronic contract or 'e-contract' may simply be described as a contract that has been formed through the use of electronic communications.

Under the general law, the following five basic elements must be present before a court will enforce a contract (Willmott, Christensen & Butler 2005):

- An offer;
- Acceptance of the offer;
- Certainty – from an objective viewpoint, a court must be able to ascertain what the parties have agreed;
- Intention – from an objective viewpoint, the parties must intend that their agreement will be legally binding; and
- Consideration – for a contract to be enforceable, it must be supported by consideration. Consideration may be generally defined as the price that is paid in return for a promise. To enforce a promise made by one party, the other party must do (or agree not to do) something in return for the promise.

These basic principles of contract law have been developed over the years through the judicial decisions of the courts. The current judicial trends indicate that these principles will apply to all contracts regardless of whether they are formed electronically, orally or through paper based communications. Many of the issues that arise for consideration relate to how these traditional contract law principles will apply to modern forms of technology.

In addition to traditional contract law principles each jurisdiction in Australia has passed uniform electronic transactions legislation based upon UNCITRAL's Model Law on Electronic Commerce 1996, aimed at addressing some of the legal uncertainties that have arisen from the increasing use of electronic communications to conduct transactions. In Queensland, the relevant legislation is known as the *Electronic Transactions (Queensland) Act 2001* (Qld) ('ETQA'). As electronic contracts are governed by both general law contractual principles and the ETQA, it is important to consider both these sources when determining the legal risks that may arise in electronic contracting.

The ETQA (and associated electronic transactions legislation around the country) adopts a 'minimalist' or 'light handed' regulatory approach. It is not designed to provide a comprehensive legal framework offering certainty for all legal aspects of electronic transactions, nor does it mandate the use of a particular form of technology (De Zilva 2003, p1010; Lawrence 2000, p89). The object of the ETQA (as set out in the Act) is to provide a regulatory framework that:

(a) recognises the importance of the information economy to future economic and social prosperity;

(b) facilitates the use of electronic transactions;

(c) promotes business and community confidence in the use of electronic transactions; and

(d) enables business and the community to use electronic communications in their dealings with government.

To give effect to these objectives, the ETQA relies on two fundamental principles: functional equivalence (meaning that equal treatment should be given to both paper based and electronic transactions); and technology neutrality (meaning that the law will not discriminate between different forms of technology).

These general principles are embodied by s 8 of the ETQA, which establishes that transactions are not invalid under a State law merely because they take place wholly or partly by one or more electronic communications. The way the ETQA defines a 'transaction' clearly includes contracts and agreements. However, this general rule can be displaced by more specific provisions that are contained in the ETQA. Accordingly, when considering the application of the ETQA to electronic contracts, regard must be had to specific provisions of the Act that may (subject to certain conditions being established) allow the following matters to be met electronically:

- a requirement to give information in writing (s 11 ETQA);
- a permission to give information in writing (s 12 ETQA);
- a requirement for a signature (s 14 ETQA);
- a requirement to produce a document (s 16 ETQA);
- a permission to produce a document (s 17 ETQA);
- a requirement to record information in writing (s 19 ETQA); and
- a requirement to keep a written document or electronic communication (ss 20 and 21 ETQA).

The interplay of the ETQA (and equivalent legislation in each Australian jurisdiction) and general law contractual principles gives rise to various legal risks and uncertainties for electronic contracting. These risks and uncertainties are considered in this Report.

2.3 E-contracting security requirements

While the security requirements of e-commerce and e-business generally have been explored (Knorr 2001; Rohrig 2004), the security requirements of e-contracting systems used in the construction industry have not been closely examined in the literature to date. An e-contracting system should satisfy the following security goals:

- **Confidentiality:** Confidentiality ensures the protection of electronic records in the e-contracting system from unauthorised disclosure or use. The identity of authorised parties will be determined by the agreement between the contracting parties.
- **Integrity:** Establishing the integrity of electronic records involves ensuring that they are not duplicated, modified or deleted.
- **Authenticity:** Authenticity ensures that the parties using or accessing the e-contracting system are who they purport to be. The contracting parties must authenticate themselves to the e-contracting system and their credentials need to be recorded and maintained.
- **Cryptographic non-repudiation:** Where cryptographic non-repudiation exists, parties cannot deny from a technical point of view having performed the action or actions attributed to them. For example, a party could not deny having entered into a contract, sending or receiving a message or updating an electronic record.

- **Availability:** Availability ensures that e-contracting systems and electronic records relevant to the contract are available to authorised parties when required.

Cryptographic mechanisms

This section lists the cryptographic mechanisms or tools that may be used to achieve the security goals of an e-contracting system. A more detailed description of these mechanisms is provided in the later sections of this Report:

- Internet security protocols such as Secure Socket Layer (SSL) or Transport Layer Security (TLS) assure the confidentiality and integrity of messages exchanged using an e-contracting system.
- The computation of a digital signature for an electronic record can assure the integrity, authenticity and non-repudiation properties of a record. Digital signature schemes are based on cryptographic hash functions and public key cryptography.
- Digital time stamping of an electronic record ensures the existence of the electronic record at a particular point of time. Digital time stamping schemes are based on cryptographic hash functions and public key cryptography.
- Logging and auditing of electronic records and communications made using an e-contracting system provide evidence of the existence of a record at a particular point of time and the identity of any computer user who has accessed or altered the record. Digital signatures and digital time stamps are more reliable methods of establishing these matters.
- The goal of availability is not met by cryptography.

2.4 Alternate ICT systems for e-contracting

There are several different ICT systems that can be used to conduct e-contracting in the construction industry. The type of system used to carry out an e-contracting process depends on factors such as the business needs of the organisation, the size of the organisation, the annual turnover of the organisation and the timeframe in which the project must be completed. In this section, some of the different systems for e-contracting are discussed.

1. E-contracting using email

E-contracts can be formed by the exchange of text documents using electronic communications such as email. Unless digital signatures are used (refer to section 17.2), e-contracts formed in this way are open to challenge in relation to the identity of the parties and the integrity of the documents.

The use of email communications also presents difficulties for contract administration and the archiving of electronic records relating to the contract:

- Email communication does not provide a comprehensive system of logging and auditing electronic records and communications. This may diminish the evidentiary value of electronic records (refer to sections 16 and 17 of this Report) and cause inefficiency in the disclosure process in the event of a dispute (as discussed in section **Error! Reference source not found.** of this Report).

- Email communication is inherently insecure (Kangas 2004). An email can be read and altered when in transit even before it reaches its destination. This is especially true when email service providers do not support secure Internet protocols such as Secure Socket Layer (SSL) or Transport Layer Security (TLS).
- Email communication does not facilitate collaboration on tasks relating to the administration of a construction project such as architectural designs and drawings.

2. E-contracting using 'click to agree'

Parties may enter into an e-contract using a 'click to agree' button on a website. The terms and conditions of the contract are displayed on a website operated by one of the contracting parties and the other party agrees to the contract by completing a form and clicking an 'I agree' button indicating acceptance of the relevant terms and conditions. When the 'I agree' button is clicked, the details of the consenting party are recorded on the web server maintained by the first party.

This type of contracting system is best suited for use in business to consumer transactions and is unlikely to be used by parties contracting in the construction industry, where a high degree of authentication and integrity is required in the contracting process. Additionally, 'click to agree' is a method of contract formation only and does not facilitate the electronic administration of a project. Electronic contract formation in the construction industry is more likely to take place using the same ICT architecture as is used to administer the construction project.

3. Forming contracts using XML

The text documents that form the basis of an e-contract may be written in XML, a mark-up language for documents containing structured information (Walsh 1998). XML is an abbreviation for extensible mark-up language. Structured information contains both content and some indication of what role that content plays. The development of XML-schema and XML-digital signature technologies and industry specific XML vocabularies has contributed to the progress of e-contracting. XML can be used to represent contracts in semi-structured formats. The World Wide Web consortium (W3C) has developed XML-compliant guidelines for digital signatures. Using XML, the content of the contract can be represented in a semi-structured format by classifying the contract into the following four groups:

Who: Information about the parties involved in the contract can be represented with XML. Roles such as 'project owner' and the 'contract winner' can be assigned to each party.

What: The product or service, which is the object of the contract, can be described in XML using industry specific XML vocabularies. The obligations that the parties need to fulfil can be described in a structured form.

How: The performance of the contract and the business process can be described using XML. The process and relation between the obligations are defined. For example, this can be the time of the product delivery. Rules of non-performance are defined such as which clause applies if a party does not fulfil its obligations.

Legal: Terms and conditions of a contract can be represented in a semi-structured format.

The advantage of using XML format for contracts is that contracts can be processed using machines and contracts can be imported into contract management and negotiation tools. The other advantage of using XML format for e-contracting is that better specification of the contract can be achieved using industry specific XML vocabularies. For example, XML can be used for a product description. The contract templates can be designed using the principles of XML-schema. The document structure of the contract and predefined clauses and terms can be specified using contract templates.

XML documents can be communicated by one party to the other using email or as part of an online collaboration system.

4. E-contracting using web-based collaboration systems

The limitations of the use of email and 'click to agree' for e-contracting suggest that a centralised e-contracting system, through which various activities such as tendering, contract formation, project management and archiving can be conducted, should be adopted in the construction industry.

The multidisciplinary nature of the construction industry has resulted in well documented problems with information and communication processing and low productivity (Nitithamyong & Skibniewski 2006). The management and administration of projects in the construction industry generate large numbers of records, from project plans and informal site discussions, to final documents such as designs and drawings. To facilitate the efficient management of records, the construction industry has begun to implement ICT solutions, improving coordination and collaboration among the companies involved in construction projects. The use of ICT for e-contracting in the construction industry can result in efficiencies for construction projects.

In the global construction industry, Internet-based collaborative products and tools are now commonly used to administer construction projects. The Internet is a mature communication system that enables the creation of advanced network applications. Collaboration systems refer to various combinations of software and hardware used to help people to collaborate. Wilkinson (2005) defines 'collaboration technology' as:

> A combination of technologies that together create a single shared interface between two or more interested individuals (people), enabling them to participate in a creative process in which they share their collective skills, expertise, understanding and knowledge (information) in an atmosphere of openness, honesty, trust and mutual respect, and thereby jointly deliver the best solution that meets their common goal.

Collaborative tools include enterprise portals and intranet applications, generic workspace or project team applications, web and video conferencing and online meeting applications, peer-to-peer file-sharing and real-time instant messaging. A collaboration system is an e-contracting system that uses collaborative tools and which is commonly implemented as a central online database that may be accessed by all participants in the project. As all electronic records are stored in the same place, users view the most recent documents as they are updated. These documents are shared via the Internet, so that paper document delivery is no longer required. The multi-task functionality of collaboration systems is not possible with email and 'click to agree' e-contracting systems.

E-contracting systems using the Internet and its associated technologies to manage construction projects are also referred to in the literature as web-based project

management systems (Nitithamyong & Skibniewski 2006). In this Report, these systems are referred to as online collaboration systems. The types of systems used by the construction industry can be classified into the following three types (Chan & Leung 2004):

- Fee-based collaboration systems;
- Build-it yourself solutions; and
- Web-enabled software.

Fee-based collaboration systems

Most web-based systems used in the construction industry are designed by application service providers (ASPs) who charge users a fee over a period of time for the use of the system. The benefits of fee-based collaboration systems include low implementation costs, minimal human expertise in using the ICT tools, simple computer system requirements and easy application upgrades. The other significant advantage of using online collaboration systems with a subscription fee is that a party can administer multiple projects using the same system within the subscription period. The drawback of these types of systems is that the functional and security features of the system are provided by the ASP rather than the client who subscribes to the system for a period of time (Chan & Leung 2004).

Build-it yourself solutions

A large scale enterprise that can afford high investment costs can develop its own proprietary web-based collaboration system to meet its own business goals and to maintain its own unique business style. Several drawbacks have been identified in relation to build-it-yourself-solutions:

- This approach best fits companies that can invest heavily, as they have a long-development life cycle for the system and outsourcing (Chan & Leung 2004).
- The functionality of build-it yourself solutions may need to be changed continually depending on the requirements of different construction projects. It is likely that the requirements of different construction projects demand some sort of flexibility in the functionality of the collaboration system to carry out projects in the construction industry. Accordingly, construction companies need to invest knowledge, skills and finance to upgrade their systems suitable for different construction projects.

Web-enabled software

The last type of collaboration system is web-enabled software which is bought by a party who maintains and uses the software permanently. The party incurs high initial costs and requires ICT knowledge to maintain and use the software. In addition, web-enabled software solutions also suffer from the same limitation as build-it yourself solutions in that they may require constant upgrading or change.

As can be seen from the above discussion of the three types of web-based collaboration systems, subscribing to an online collaboration system which is provided by an application service provider facilitates project collaboration at an affordable price and with the professional services of the service provider. Accordingly, most of the web-based systems used in the construction industry to

carry out projects are developed by a third party service provider who charges a subscription fee for the use of the system for a certain period of time.

General shortcomings of existing online collaboration systems

While online collaboration systems have the potential to satisfy the desirable security requirements for e-contracting, some of the systems that are presently available have a range of security deficiencies. Some of the security problems that can be identified include:

- A number of systems do not use secure Internet Protocols such as SSL or TLS when transmitting electronic records and documents over the Internet. Accordingly, the confidentiality and integrity of these records and documents may not be assured.
- The archiving procedures adopted by a number of systems are unclear and few systems adopt time stamping procedures after project completion, which would ensure that the integrity of project documents and records is maintained.
- From a practical perspective, system users often send electronic records using systems outside of the online collaboration system. If this occurs, the security and integrity of those records cannot be assured.
- The authentication systems used by some online collaboration systems do not provide a sufficient level of authentication for e-contracting. Generally, the authentication system used by most systems is password based and does not incorporate additional security features such as password history and expiry mechanisms. Location based access control systems (which would provide a higher level of user authentication) are generally not used.

2.5 General legal principles governing the retention of electronic documents

During the administration and management of a construction project various documents relating to the project will be created. There are several legal considerations that arise in relation to the parties' obligations to retain these documents. Firstly, parties may have an obligation to retain records pursuant to various Commonwealth and State Acts. Secondly, in the event of a dispute between the parties that results in litigation, the parties will be under an obligation to disclose to each other documents they have or have had in their possession that are relevant to the dispute. The process for disclosing documents in Australia is known as either discovery or disclosure depending on the jurisdiction. Thirdly, if parties wish to rely on documents as evidence in court they will need to satisfy the requirements as to the admissibility of documents as evidence. Further, even if the documents are admissible as evidence a court may attach less weight to them (for example if there is doubt as to their authenticity).

Where documents are created and retained electronically uncertainties arise as to the application of these legal obligations. This Report will consider these uncertainties in the context of the electronic administration of construction projects.

PART B: RISKS AND RECOMMENDATIONS

3. TIME OF CONTRACT FORMATION

3.1 Risk

Where a construction contract has been formed by an exchange of electronic communications, there are legal uncertainties that make it difficult to determine the precise point in time that the contract has been formed. The reason it may be important to determine the time of contract formation is that once an offer to enter into a contract has been accepted it becomes irrevocable. Accordingly, up until the point in time that the offer has been accepted (being the time that the contract is formed), the offeror is free to withdraw the offer. In the context of electronic communications, the legal rules that govern when acceptance of an offer is effective are unclear.

General law contractual principles

Under general law contractual principles, the general rule is that the acceptance of an offer (which constitutes the formation of a contract) is effective at the time it is communicated to the offeror. When communication takes place, it is said that at this point in time there is a 'meeting of the minds' of the parties as they have reached agreement or consensus upon the terms of the contract (Hill 2002, p4).

However, an exception to this rule is the 'postal acceptance rule'. The postal acceptance rule generally applies where the post is used as the method of communication between the parties. If the rule applies, then the general position is changed such that the acceptance of an offer becomes effective and the contract is formed at the time the acceptance is *posted*, rather than at the later time when the acceptance is *communicated* to the offeror.

For electronic communications, there has been no definitive statement by the courts about whether the postal acceptance rule will apply to email or to various other relatively recent communication technologies. It has, however, been established that the rule will not apply to communications by telephone, telex and facsimile. The only judicial consideration of this issue in connection with modern communication technologies appears in the first instance judgment of the Singapore High Court in *Chwee Kin Keong v Digilandmall.com Pte Ltd* [2004] 2 SLR 594. The comments made in the case were not necessary to decide the relevant issues before the court, therefore the judge did not give any final views about how this important issue should be determined. However, the various statements made in this case appear to suggest that in the case of emails, it may be inappropriate for the postal acceptance rule to apply. For transactions that are conducted over the world wide web, it was suggested that as these transactions are 'almost invariably instantaneous and/or interactive', the logical default rule should be the usual position that acceptance will be effective when it is received (at [101]).

The application of the postal acceptance rule to modern communication technologies has been debated by numerous academic commentators and a wide range of differing opinions have been proffered on the subject. Ultimately, the applicability of the postal acceptance rule to electronic communications remains uncertain, particularly in light of the broad range of technologies that may be used to conduct electronic contracting.

Even if it can be assumed that the postal acceptance rule does not apply and that acceptance is effective when communicated to an offeror, there is a further debate about when 'communication' actually occurs. For example, if the acceptance is sent by email, the various options for when the email is communicated may include: the time when the recipient reads the message, the time that the message is downloaded to the recipient's computer, or the time when the message is received by the recipient's ISP (Christensen 2001, p33).

Accordingly, significant uncertainties remain under the general law when determining the time that an electronic construction contract has been formed. Unfortunately, these uncertainties have not been clarified by legislation.

Electronic Transactions (Queensland) Act 2001 (Qld)

There are provisions in the ETQA (and other equivalent Commonwealth, State and Territory legislation) that attempt to clarify when an electronic communication is dispatched and when it is received. Sections 23 and 24 of the ETQA are reproduced below:

> **23 Time of dispatch**
>
> (1) If an electronic communication enters a single information system outside the control of the originator of the communication, then, unless otherwise agreed between the originator and the addressee of the communication, the dispatch of the communication occurs when it enters the information system.
>
> (2) If an electronic communication enters successively 2 or more information systems outside the control of the originator of the communication, then, unless otherwise agreed between the originator and the addressee of the communication, the dispatch of the communication occurs when it enters the first of the information systems.
>
> **24 Time of receipt**
>
> (1) If the addressee of an electronic communication has designated an information system to receive electronic communications, then, unless otherwise agreed between the originator of the communication and the addressee, the time of receipt of the communication is the time when it enters the information system.
>
> (2) If the addressee of an electronic communication has not designated an information system to receive electronic communications, then, unless otherwise agreed between the originator of the communication and the addressee, the time of receipt of the communication is the time when it comes to the attention of the addressee.

One of the main problems with these provisions is that while they do state when an electronic communication is dispatched and when it is received, they *do not*, in a contractual framework, state whether it is the sending or the receipt of the electronic communication that completes the formation of a contract (Hill 2001, p46; Thomson 2003, p27; De Zilva 2003, p1020). The ETQA provisions could therefore be viewed by a court as either supporting the usual rule that acceptance is effective upon communication, or be seen to leave the question of when an acceptance is effective to general law contractual principles (Christensen 2001, p38).

Accordingly, the ETQA does not resolve whether or not the postal acceptance rule will apply to electronic communications. Even if it could be assumed that acceptance

of an offer is effective upon communication, s 24 of the ETQA does not definitively settle all relevant timing issues. Some of the additional problems that arise under the legislation include:

- Under the ETQA, the effective time of receipt of an electronic communication depends upon whether or not the addressee has *designated* an information system to receive electronic communications. It is unclear when an addressee can be said to have effectively *designated* an information system. For example, for designation to occur, does an offer have to specifically state an email address to which the acceptance should be sent, or will the automatic inclusion of a return email address in an email message be enough for designation to occur? (Giles 2000, p12).

- If an addressee has designated an information system, then receipt of an electronic communication is generally effective when the communication enters the designated information system. The ETQA definition of an 'information system' is extremely broad – it is defined to mean 'a system for generating, sending, receiving, storing or otherwise processing electronic communications.' Depending upon the relevant context, this definition may mean any number of things.

- If an addressee has not designated an information system, then generally speaking the time of receipt is 'when it comes to the attention of the addressee'. Questions arise as to when this occurs – for example, is it necessary that the addressee actually read the communication? Clause 14 of the Revised Explanatory Memorandum to the *Electronic Transactions Bill 1999* (Cth) suggests this is not necessary. It provides that:

  > The term "comes to the attention of the addressee" does not mean that a communication must be read by the addressee before it is considered to be received. An addressee who actually knows, or should reasonably know in the circumstances, of the existence of the communication should be considered to have received the communication. For example, an addressee who is aware that the communication is in their electronic mail 'box' but who refuses to read it should be considered to have received the communication.

  It has been suggested that even this clarificatory statement is still not sufficient to resolve the question of when an electronic communication 'comes to the attention of the addressee' (Thomson 2003, p27). However, the statement does appear to reflect some of the rules that have developed under the general law which recognise that on occasion, it may be necessary to deem a person to have received a communication (Hill 2002, p8).

In summary, under both the general law and the ETQA, legal uncertainties exist when determining the precise point in time that a construction contract will be formed by electronic communications.

Risk Example

Company A wished to enter into a contract with Company B. On Friday 8 June A sent an email to B offering to enter into a contract with B upon the terms attached to the email. B sent a return email to A accepting the terms of A's offer, which was sent by B at 9.00am on Tuesday 12 June.

Due to bottlenecks in communication lines, B's email did not reach A's internet service provider until 4.30pm on Tuesday 12 June. B's email was not downloaded to A's employee's computer until 8.30am on Wednesday 13 June. A's employee did not actually read the email until 10.30am on Wednesday 13 June.

On Tuesday 12 June, A's board of directors met and decided they no longer wished to enter into a contract with B. A sent a facsimile to B withdrawing its offer to enter into the contract which B received at 5.00pm on Tuesday 12 June.

Is A's withdrawal of offer effective? There are several possible answers:

(1) If the postal acceptance rule applies B's acceptance would be effective and the contract formed at 9.00am on Tuesday 12 June. A's withdrawal of offer is not valid.

(2) If acceptance is not effective until it is communicated to A, the position depends upon when 'communication' occurs:

(i) if communication occurs when the message was received by A's ISP - the contract was formed at 4.30pm on Tuesday 12 June. A's withdrawal of offer is not valid.

(ii) if communication occurs when the message is downloaded to A's employee's computer or when A's employee reads the message, A's withdrawal of offer is valid as A may revoke its offer at any time prior to the communication of acceptance.

3.2 Resolution

It is recommended that the simplest way to avoid the legal uncertainties surrounding the time of electronic contract formation is to include clear provisions in the contractual offer that specify how acceptance is to be communicated and when an acceptance of the offer will be deemed to be effective (O'Shea & Skeahan 1997, p262; Hill 2002, p10). Appropriately drafted provisions would avoid the uncertainties under both the general law and the ETQA about the time that a contract is formed.

In addition to ensuring that appropriate timing provisions are included in a construction contract, from an evidentiary perspective it is important to ensure that the date and the time that electronic communications take place are accurately recorded. One technical mechanism that may be adopted for secure time recording is digital time stamping (as discussed in section 18 of this Report).

4. PLACE OF CONTRACT FORMATION

4.1 Risk

As discussed in section 3, there are legal uncertainties that make it difficult to determine the precise point in time that an electronic construction contract has been formed. It is unclear whether acceptance of an offer to enter into the contract takes place at the time the acceptance is sent by the offeree, or at the time that it is communicated to the offeror. These uncertainties also mean that it is difficult to determine *where* the contract is formed.

The reason why it may be important to ascertain the place where a particular contract has been formed is that the place of contract formation may provide a court with jurisdiction to hear and determine a dispute under the contract. A court may assume jurisdiction over a contractual dispute in a number of circumstances, including where the contract is made within the jurisdiction, governed by the law of the forum, or broken within the jurisdiction (Hill 2001, p49).

Section 25 of the ETQA addresses *where* an electronic communication is taken to have been dispatched and received, unless otherwise agreed by the originator and addressee of the electronic communication. Section 25 of the ETQA provides:

> **25 Place of dispatch and receipt**
>
> (1) Unless otherwise agreed between the originator of an electronic communication and the addressee of the communication -
>
> (a) the communication is taken to have been dispatched from the originator's place of business; and
>
> (b) the communication is taken to have been received at the addressee's place of business.
>
> (2) For subsection (1) -
>
> (a) if the originator or addressee of the communication has more than 1 place of business, and 1 of the places (the ***relevant place***) has a closer relationship to the underlying transaction the communication is about – the relevant place is taken to be the originator's or addressee's only place of business; and
>
> (b) if the originator or addressee has more than one place of business, but paragraph (a) does not apply – the originator's or addressee's principal place of business is taken to be the originator's or addressee's only place of business; and
>
> (c) if the originator or addressee does not have a place of business – the place where the originator or addressee ordinarily resides is taken to be the originator's or addressee's place of business.

Section 25 of the ETQA does not solve the current problem, as it does not state whether it is the place of sending, or the place of receipt of the electronic communication that is the place of formation of a contract (Hill 2001, pp53-4). It is therefore apparent that when a construction contract has been formed electronically, it may be difficult to determine the place where the contract was formed.

Risk Example

Company A has its principal place of business in Queensland. A wishes to enter into a subcontract with Company B, whose principal place of business is located in New South Wales. A sends an email to B offering to enter into a subcontract with B upon the terms attached to the email. B then sends a return email accepting the terms of the offer.

If acceptance of the offer is effective at the time the acceptance is sent by B, the contract is formed in New South Wales. Alternatively, if acceptance of the offer is effective at the time that it is communicated to A, the contract is formed in Queensland.

4.2 Resolution

The majority of significant electronic construction contracts will contain clauses where the parties agree to submit to the jurisdiction of the courts of a particular place (either a State of Australia or a particular country), and to the applicable law that will govern the contract. Where the governing law and jurisdiction is clearly specified and has a

logical connection with the contract, it is highly unlikely that a court would disturb the agreement that has been reached by the parties on this issue.

Although it may be difficult to determine the actual place where an electronic construction contract has been formed, this problem will have minimal legal relevance where appropriate jurisdiction and governing law clauses are included in the construction contract.

5. ATTRIBUTION OF ELECTRONIC COMMUNICATIONS – AUTHORITY TO CONTRACT

5.1 Risk

In an electronic environment, it will be important to authenticate the identity of the sender of an electronic communication. Section 19 of this Report deals with the various security measures that may be adopted to effectively authenticate a person's identity.

In the context of electronic contract formation, it will also be important to ensure that a party who purports to enter into a contractual relationship via electronic communications is authorised to enter into the contract. This issue is touched upon by the ETQA and other mirroring electronic transactions legislation around the country. Section 26 of the ETQA provides:

> **26 Attribution of electronic communications**
>
> (1) For a State Law, unless otherwise agreed between the purported originator of an electronic communication and the addressee of the communication, the purported originator of the communication is bound by the communication only if it was sent by the purported originator or with the purported originator's authority.
>
> (2) Subsection (1) does not limit a State law that provides for:
>
> (a) conduct engaged in by a person within the scope of the person's actual or apparent authority to be attributed to another person; or
>
> (b) a person to be bound by conduct engaged in by another person within the scope of the other person's actual or apparent authority.

In the context of forming electronic construction contracts, this means that a 'purported originator' will only be bound by:

- an electronic offer to enter into a contract; or
- an electronic acceptance of an offer,

if the purported originator sends the offer or acceptance themselves, or if the person who sends the relevant communication on their behalf was authorised to do so.

Section 26 of the ETQA is not controversial, as it does not change the operation of existing agency laws or the provisions of the *Corporations Act 2001* (Cth), that determine when a person or company will be bound by a contract. If a person who sends an offer or acceptance communication has actual or apparent authority to bind the 'purported originator', or (in the case of companies only), they can be assumed to have such authority under the *Corporations Act 2001* (Cth), then the 'purported originator' will be bound by the communication.

Accordingly, the fact that a construction contract may be formed by electronic communications does not alter the existing laws that determine whether a person is authorised to enter into a contractual relationship on behalf of another person or entity.

5.2 Resolution

Regardless of whether a construction contract is formed in an electronic or paper based environment, the contract parties must still carry out their usual due diligence procedures to establish that the individuals who are purporting to enter into a contract on behalf of another person or organisation possess the actual or apparent authority to enter into the contract.

6. STATUTORY REQUIREMENTS FOR GUARANTEES TO BE IN WRITING

6.1 Risk

Where a construction contract has been formed by electronic communications and the contract contains a guarantee, there is a risk that the guarantee will not be enforceable if the electronic communications do not satisfy certain statutory provisions that require guarantees to be 'in writing'.

As a general principle, the law does not require a binding contract to be established by any particular communication method. Most contracts may be formed by any number of communication methods including, for example, by post, facsimile or even orally. However, in most jurisdictions in Australia there are legislative requirements for certain types of contracts to be in writing, including guarantees. These types of provisions are designed to prevent the perpetration of fraud and are based on the original English Statute of Frauds 1677. Equivalent legislation exists in most common law countries including, for example, the United States of America, New Zealand and Singapore.

In the context of guarantees, in Queensland s 56(1) of the *Property Law Act 1974* (Qld) generally provides that a guarantee is only enforceable if it is evidenced in writing. Section 56 states:

> No action may be brought upon any promise to guarantee any liability of another unless the promise upon which such action is brought, or some memorandum or note of the promise, is *in writing*, and signed by the party to be charged, or by some other person by the party lawfully authorised. [emphasis added]

(Similar statutory provisions exist in the Northern Territory, Victoria, Western Australia and Tasmania. Section 50(1) of the Consumer Credit Code also provides that 'A guarantee must be in writing signed by the guarantor'). Whether an electronic communication satisfies these writing requirements must be considered by reference to both the ETQA and general law contract principles.

Electronic Transactions (Queensland) Act 2001 (Qld)

Section 11 of the ETQA purports to allow requirements of writing to be satisfied by electronic communications. If this section applies, then the statutory requirement for a guarantee to be in writing would be satisfied by electronic communications. Section 11 provides:

11 Requirement to give information in writing

(1) If, under a State law, a person is required to give information in writing, the requirement is taken to have been met if the person gives the information by an electronic communication in the circumstances stated in subsection (2).

(2) The circumstances are that -

(a) at the time the information was given, it was reasonable to expect the information would be readily accessible so as to be useable for subsequent reference; and

(b) the person to whom the information is required to be given consents to the information being given by an electronic communication.

The operation of s 11 is impacted upon by certain terms that are defined within the ETQA itself. The relevant defined terms include:

> ***State law*** means - (a) any law in force in the State, whether written or unwritten; or (b) any instrument made or having effect under a law mentioned in paragraph (a)… (Schedule 2 ETQA)
>
> ***give information*** includes, but is not limited to, the following – (a) make an application; (b) make or lodge a claim; (c) give, send or serve a notification; (d) lodge a return; (e) make a request; (f) make a declaration; (g) lodge or issue a certificate; (h) make, vary or cancel an election; (i) lodge an objection; (j) give a statement of reasons. (s 10 ETQA)
>
> ***electronic communication*** means – (a) a communication of information in the form of data, text or images by guided or unguided electromagnetic energy; or (b) a communication of information in the form of sound by guided or unguided electromagnetic energy, if the sound is processed at its destination by an automated voice recognition system. (Schedule 2 ETQA)
>
> ***consents*** includes consent that can reasonably be inferred from the conduct of the person concerned, but does not include consent given subject to conditions unless the conditions are complied with. (Schedule 2 ETQA)

There has been only one judicial decision that has considered the application of the Australian electronic transactions legislation to a statutory requirement for an agreement to be in writing (*Faulks v Cameron* (2004) 32 Fam LR 417). However, the court did not devote significant time to the issue – it simply appeared to presume that printed emails were writing. As there has been little judicial consideration about how s 11 of the ETQA may apply to a guarantee that has been formed by electronic communications, the position on this issue remains unclear.

A number of legal issues may arise when trying to rely on s 11 of the ETQA to establish that a guarantee formed by electronic communications is in fact a guarantee that is 'in writing':

- **Commencement:** Firstly, it should be noted that the ETQA (and other associated electronic transactions legislation in Australia) will not apply to a transaction that takes place before the legislation came into force. To obtain the benefit of the legislation, the contract must have been formed on or after the date that the legislation commenced.

  (The *Electronic Transactions Act 1999* (Cth) commenced on 15 March 2000; most of the ETQA commenced on 1 November 2002; the *Electronic Transactions Act*

2000 (NSW) commenced on 30 November 2001; the *Electronic Transactions (Victoria) Act 2000* (Vic) commenced on 1 September 2000; the *Electronic Transactions Act 2000* (Tas) commenced on 1 June 2001; the *Electronic Transactions (Northern Territory) Act 2000* (NT) commenced on 13 June 2001; the majority of the *Electronic Transactions (Australian Capital Territory) Act 2000* (ACT) commenced on 1 July 2001; the *Electronic Transactions Act 2000* (SA) commenced on 1 November 2002; and the *Electronic Transactions Act 2001* (WA) commenced on 2 May 2003).

- **A requirement for writing**: Section 11 of the ETQA can only apply where there is a State law that *requires* a person to give information in writing. Section 56(1) of the *Property Law Act 1974* (Qld) may not be a relevant State law, as it does not actually *require* a guarantee to be in writing. Instead, the legislation simply provides that the guarantee will not be enforceable (Nikolich 2003, p31). However, it is suggested that this issue would be resolved by interpreting a 'requirement' to give information in writing, to include a provision that sets out consequences for an absence of writing (Christensen, Duncan & Low 2002, p61).

- **Giving information in writing:** It has been suggested that as s 11 of the ETQA only operates where a State law requires a person to 'give information' in writing, the section may not apply to the formation of a contract of guarantee, as this is very different to the scenario where a law actually requires a person to provide information (Christensen, Duncan & Low 2002, p60). Although the ETQA definition of 'give information' is not exhaustive, none of the actions contained in the definition remotely relate to the formation of a contract. Accordingly, there may be some uncertainty as to whether the ETQA permits the conclusion of a contract of guarantee in electronic as opposed to written form (Nikolich 2003, p31).

- **Consent:** For s 11 of the ETQA to apply to a guarantee, the person to whom the information is required to be given must have consented to the information being given by an electronic communication. It is clear that consent may be express or implied from conduct. However, it is generally uncertain when conduct may be construed as the giving of consent. Although consent is unlikely to be implied simply because a person has previously used electronic communications, consent may very well be inferred where the parties have previously conducted similar transactions electronically (Nikolich 2003, p29).

- **Accessibility for subsequence reference:** For the ETQA to apply, at the time the information was given, it must have been reasonable to expect the information would be readily accessible so as to be useable for subsequent reference. It is suggested that this would be satisfied if the contracting parties store the information such that it is able to be later accessed, retrieved and read (Christensen, Duncan & Low 2002, p61).

Until further judicial guidance on some of these issues is obtained from the courts, it is unclear whether s 11 of the ETQA can be relied upon to establish that a guarantee that has been formed by electronic communications satisfies the statutory requirements for a guarantee to be in writing.

General law contractual principles

Although some uncertainty remains about whether s 11 of the ETQA will apply to a guarantee that has been formed by electronic communications, general law contractual principles have sufficiently evolved to recognise that a guarantee that has

been formed by an exchange of electronic communications will be in writing once the relevant electronic communications have been printed.

There has only been one judicial determination in Australia about whether general law principles allow electronic communications to satisfy a statutory writing requirement (*McGuren v Simpson* [2004] NSWSC 35). The decision held that an email was capable of constituting an acknowledgment 'in writing' for the purposes of the *Limitation Act 1969* (NSW), as the relevant defendant in the case was able to produce a printed email sent to him by the plaintiff. The court was prepared to construe the provisions of the *Limitation Act 1969* (NSW) in a manner that accommodated technological change.

The fact that a printed email will constitute 'writing' for the purposes of a Statute of Frauds writing requirement is supported by decisions in other common law jurisdictions, including the United States of America (where a long line of decisions have maintained this position) and also Singapore. Accordingly, under general law principles it is relatively clear that the printed form of an electronic document will be sufficient to satisfy the requirement of s 56 of the *Property Law Act 1974* (Qld) for a guarantee to be in writing. In the case of purely electronic communications that are never printed and therefore never take physical form, the general law and the literature is unclear on whether these communications would be viewed as 'in writing'. The issue is yet to receive significant judicial attention, largely due to the fact that where electronic documents have been produced as evidence, they have always been produced in printed form.

6.2 Resolution

Where a construction contract has been formed by electronic communications and the contract contains a guarantee, once the electronic communications have been printed the general law will recognise that the guarantee is 'in writing' as required by s 56 of the *Property Law Act 1974* (Qld) (and other equivalent statutory provisions). If the contract remains purely in electronic form and is never printed, there are significant risks that the guarantee would not be enforceable as it may not be 'in writing'.

However, s 56 of the *Property Law Act 1974* (Qld) also requires a guarantee to be signed. As a consequence of the legal uncertainties surrounding the recognition of electronic signatures (discussed in section 7 below) it is recommended that at this point in time, to avoid the risk of a guarantee being unenforceable, all guarantees should continue to be entered into in paper form and be physically signed using handwritten signatures.

7. STATUTORY REQUIREMENTS FOR GUARANTEES TO BE SIGNED

7.1 Risk

Where a construction contract has been formed by electronic communications and the contract contains a guarantee, there is a risk that the guarantee will not be enforceable if the electronic communications do not satisfy statutory provisions that require guarantees to be signed.

Generally, the law does not require contracts to be signed. Accordingly, for the majority of contracts no hand-written or other form of signature is required for the contract to be valid and binding. However, as outlined in section 6 above, s 56(1) of

the *Property Law Act 1974* (Qld) requires a guarantee (or some memorandum or note of the promise) to be 'signed' in addition to being 'in writing'. This risk must be assessed by reference to both the ETQA and general law contract principles. However, it is important to first consider the various ways that a party may 'sign' an electronic document.

How can an electronic document be signed?

(a) Electronic signatures

The term 'electronic signature' is usually used to describe signatures incorporated in a document by electronic or cryptographic means. Some examples of electronic signatures include: the type-written name of a signatory in an email or document, the pasting in of a scanned version of the signer's signature, clicking an 'I Accept' button, the use of a user id and password, or the use of cryptographic technology such as digital signatures.

Electronic signatures may identify the person who has appended the signature to the document and (as discussed further below) may indicate the person's agreement to the content of the document in the same way as a handwritten signature. The examples of electronic signatures listed above (other than digital signatures) are not able to assure both the sender's identity and the integrity of documents. However, an advantage of these types of signatures is that, in many cases, they are in human readable form and can be easily understood by people.

(b) Digital signatures

A digital signature is a signing technology based on public key cryptography. Public key cryptography involves the use of two keys, a private key and a public key. Each individual in the system has a private key which only they know and they distribute the corresponding public key to the public. When an electronic document is digitally signed a secure cryptographic hash function is used to create a hash code of the original document and the hash code is signed using the private key of the signatory. The output of this signing function is known as a digital signature.

The person who needs to verify a digital signature requires the communicated document, the digital signature and the public key of the signatory of the document. To verify the signature, the same hash function is run over the communicated document and a verification algorithm using the public key is run over the digital signature. The output of the verification algorithm is compared to the hash code of the communicated document and if they are the same, then the signature is verified as being a valid signature of the holder of the private key and the integrity of the message is confirmed.

Electronic Transactions (Queensland) Act 2001 (Qld)

Section 14 of the ETQA allows signature requirements to be met in the context of electronic communications. Under this provision, if a State law requires a person's signature, this requirement is met for an electronic communication if the following three conditions are satisfied:

- a method is used to *identify* the person and to indicate the person's *approval* of the information communicated (ie, the 'method' would be an electronic or digital signature);

- having regard to all relevant circumstances when the method was used, the method was *as reliable as was appropriate* for the purposes for which the information was communicated; and

- the person to whom the signature is required to be given has *consented* to the requirement being met by using the method.

The intricacies of this provision are yet to be considered in sufficient detail by the courts. Only one Australian case has considered the effectiveness of an electronic signature under Australia's electronic transactions legislation and this case did not relate to a guarantee (*Faulks v Cameron* (2004) 32 Fam LR 417). The decision involved emails that ended with the type-written words 'Regards Angus' and 'Regards Angus Cameron'. The court had to determine whether the emails were 'signed' as a consequence of the *Electronic Transactions (Northern Territory) Act 2000* (NT) (a provision that is almost identical to s 14 of the ETQA). With surprisingly little analysis, it was held that the emails had been signed. The court was satisfied that:

> …the printed signature on the defendant's emails identifies him and indicates his approval of the information communicated, that the method was reliable as was appropriate and that the plaintiff consented to the method. I am satisfied that the agreement is 'signed'… (at page 426).

This decision suggests that the ETQA may easily allow even the most basic form of electronic signature to satisfy a statutory signing requirement. However, the decision must be treated with caution as it has not sufficiently addressed the following issues that may arise in connection with s 14 of the ETQA:

- **A requirement for a signature:** Section 56(1) of the *Property Law Act 1974* (Qld) does not actually *require* a guarantee to be signed - it simply provides that if the guarantee is not signed it will not be enforceable. Section 14 of the ETQA will only apply if a State law can be said to *require* a person's signature. However, this issue may be avoided by adopting a broad interpretation to include the situation where a failure to have a signature results in adverse consequences (Christensen, Duncan & Low 2002, p71). The decision in *Faulks v Cameron* (2004) 32 Fam LR 417 supports this argument.

- **Identification and approval:** Under s 14 of the ETQA, the signature method used does not have to verify the integrity of the information sent in an electronic communication, it need only identify the person and indicate their approval of the information communicated. *Faulks v Cameron* (2004) 32 Fam LR 417 indicates that a simple electronic signature may, depending upon the circumstances, be sufficient to *identify* the person and to indicate the person's *approval* of the information communicated. It is suggested that both electronic signatures and the more secure method of digital signatures would satisfy this requirement of the ETQA (Christensen, Duncan & Low 2002, p72).

- **Reliability and appropriateness of the signature method:** The reliability of the signature method used is the crucial issue under the ETQA. In the context of establishing that a particular signature method is reliable, the ETQA does not prescribe that any particular form of technology be used. This is a deliberate policy decision that has been made by the legislature. However, this does create uncertainty as parties may be unable to make an assessment of which signature method is appropriate for use on a transaction by transaction basis (De Zilva 2003, p1016).

Accordingly, there is a risk that a particular signature method may not be considered reliable or appropriate in the context of a particular transaction. This is especially the case as the courts have yet to sufficiently consider the issue (Davidson 2004, p30). It is suggested that the critical factors that may impact upon reliability is the ability of the signature method to authenticate the document and to maintain the integrity of the document for later reference (Christensen, Duncan & Low 2003, p12).

- **Consent:** For s 14 of the ETQA to apply to a guarantee, the person to whom the signature is required to be given must have consented to the signature requirement being met by the use of the signature method. A requirement for consent applies to a number of the ETQA provisions and absent express consent, it is generally unclear when conduct may be construed as the giving of consent. In the context of signatures, consent must be given to 'the method' used to satisfy the signature requirement. It is possible that proper 'consent' in this context may be narrower than a simple consent to the use of electronic communications (Christensen, Duncan & Low 2002, p73).

- **Commencement:** The ETQA (and other associated uniform electronic transactions legislation in Australia) will not apply to a transaction that takes place before the legislation came into operation.

Accordingly, while s 14 of the ETQA may potentially be relied upon to establish that a guarantee that has been signed with an electronic or digital signature has been 'signed' for the purposes of the *Property Law Act 1974* (Qld), there is no absolute certainty on this point.

General law principles

Under the general law there are also uncertainties about whether an Australian court would hold that an electronic or digital signature is a sufficient signature for the purposes of s 56 of the *Property Law Act 1974* (Qld), such that there is a continuing risk that a guarantee that has been formed by electronic communications may not be enforceable.

There has only been one judicial decision in Australia about whether general law principles will allow an electronic signature to satisfy a statutory signing requirement (*McGuren v Simpson* [2004] NSWSC 35). This case considered whether an email was capable of constituting an acknowledgment in writing and 'signed' for the purposes of the *Limitation Act 1969* (NSW), as the defendant in the case produced a printed email sent to him by the plaintiff which contained the plaintiff's type-written name. In holding that this was a sufficient signature, the court applied a well known doctrine called the 'authenticated signature fiction'. This doctrine may be explained as follows:

> Where the name of the party to be charged appears on the alleged note or memorandum, for example, because it has been typed in by the other party, the so-called 'authenticated signature fiction' will apply where the party to be charged expressly or impliedly acknowledges the writing as an authenticated expression of the contract so that the typed words will be deemed to be his or her signature. This principle has no application to a document which is not in some way or other recognisable as a note or memorandum of a concluded agreement. (at [22])

As the plaintiff's name appeared in the email and the email contained an authenticated expression of a prior agreement, the email was found to be a note of a

concluded agreement and in effect, the plaintiff's type-written name was deemed to be a signature.

The difficulty with relying on this decision to argue that an electronic signature will be sufficient in all cases, is that for the authenticated signature fiction to apply, the signatory must have expressly or impliedly indicated that he or she recognises the writing that contains their name as being an expression of the will to contract (Christensen, Duncan & Low 2002, p3). The decisions of the courts indicate that the authenticated signature fiction may be relied upon for certain types of contracts, but the various States and Territories of Australia have not adopted a uniform approach to the issue and there is yet to be a decision that has applied the authenticated signature fiction to a guarantee.

Accordingly, although there are decisions in the United States and Singapore that have held a type-written name in an email will satisfy a Statute of Frauds requirement for an agreement to be signed, there remains uncertainty as to the approach that an Australian court will adopt in connection with guarantees. This would particularly be the case where the signature sought to be relied upon is a person's email address that is automatically included upon the sending of an email communication.

In the case of digital signatures, there have been no judicial decisions in any jurisdiction that address whether or not a digital signature will satisfy a statutory signing requirement. Whether or not a digital signature will be sufficient under Australian law is unclear. It is suggested that as a digital signature has the potential to fulfil almost all of the traditional functions that are performed by a hand-written signature, a digital signature should be sufficient to satisfy s 56 of the *Property Law Act 1974* (Qld) (Christensen, Duncan & Low 2002, p54). The Law Commission for England and Wales also shares this view (Beale & Griffiths 2002, pp473-4).

Given the relative ease with which some courts have accepted electronic signatures as satisfying a statutory signing requirement, it may be suggested that the increased security provided by digital signatures should lead to the conclusion that a digital signature will be sufficient. However, until the issue has been determined by the courts, the position with respect to digital signatures remains unclear.

7.2 Resolution

Section 14 of the ETQA may potentially be relied upon to establish that a guarantee that has been signed with an electronic or digital signature has been sufficiently 'signed' for the purposes of s 56 of the *Property Law Act 1974* (Qld). However, the main difficulties that may be encountered when relying upon the ETQA are establishing that:

- consent was given to the use of the signature method; and
- having regard to all relevant circumstances at the time the signature method was used, the signature method was as reliable as was appropriate for the purposes for which the information was communicated.

Until there are further judicial decisions on the application of s 14 of the ETQA, it is difficult to determine how the courts will approach these issues. In light of the current uncertainties that exist under both the general law and ETQA, it is recommended that at this point in time, all guarantees should continue to be entered into in paper form and be physically signed using handwritten signatures. This is the only way at present to avoid the risk that an electronic guarantee may be unenforceable.

If, notwithstanding the risks and recommendations made in this Report, contracting parties still wish to enter into guarantees via electronic communications, at the minimum the contract should contain provisions whereby the parties:

- expressly consent to the use of the relevant electronic signature method; and
- agree that the particular signing method to be used is considered both reliable and appropriate. (It should be noted, however, that such a provision would not prevent a court from making its own assessment of the reliability and appropriateness of the signature method that has been used).

8. ELECTRONIC AMENDMENTS TO CONSTRUCTION CONTRACTS

8.1 Risk

Depending on the terms of a construction contract, it may be uncertain whether electronic communications are effective to amend the contract. A variation or amendment of a contract is, in itself, a further contract between the parties. Accordingly, aside from issues that relate to the validity of electronic communications, the persons purporting to enter into an agreement to amend the contract must be duly authorised to do so. If a contract does not adequately address the status of electronic communications in this context, the potential risks to the contract parties include:

- Email traffic passing between the parties may potentially give rise to an effective amendment of the contract, if the persons exchanging the communications have the actual or apparent authority to contractually bind the contract parties. This risk is incrementally increased where the parties engage in regular email or other electronic communications in the day to day administration of their contract.
- Even if a party wishes to be bound by an electronic agreement to amend the contract, depending on the terms of the contract an electronic agreement may or may not be effective.

Construction contracts commonly require any amendments to the contract to be in writing and may even require the writing to be signed. Often times the provisions that govern the delivery of contractual notices are broad enough to encapsulate all other communications by the parties, including an agreement by the parties to amend the contract. If this is the case, then whether or not an electronic amendment of the contract is effective will be determined in accordance with the notice provision in the contract and the conduct of the parties (refer to the discussions in section 9 below).

If a construction contract is silent on the issue and simply requires amendments to be written and signed, it is possible that the ETQA and general law contractual principles may still recognise an electronic agreement to amend the contract as being in writing and signed. These issues are discussed further below.

Contractual writing requirements

Where a contract is silent on the issue of electronic communications but requires contractual amendments to take place in writing, a number of provisions in the ETQA are relevant to determining whether or not electronic communications may satisfy this contractual writing requirement. The competing arguments about whether the ETQA assists in this scenario are similar, but not identical to the discussions in section 6.1 of this Report in relation to statutory requirements for guarantees to be in writing. The arguments are not identical because in the current context, the requirement for

amendments to be agreed in writing stems from an existing contract between the parties, as opposed to a statutory provision.

The following provisions of the ETQA are relevant to this issue:

- s 11 ETQA – in certain circumstances, where a State law *requires* a person to give information in writing, the requirement is taken to be met if the person gives the information by an electronic communication. The relevant circumstances are that at the time the information was given it was reasonable to expect the information would be readily accessible so as to be useable for subsequent reference, and that the person to whom the information is to be given has consented to the information being given by an electronic communication.
- s 12 ETQA – in certain circumstances, where a State law *permits* a person to give information, the person may give the information by an electronic communication. The relevant circumstances are similar to those outlined above in s 11 of the ETQA.
- s 8 ETQA – this section generally provides that a transaction (including a contract and agreement) is not invalid under a State law merely because it took place wholly or partly by one or more electronic communications. This general rule can be displaced by more specific provisions that are contained in the ETQA.

A number of arguments have been raised to suggest that where a contract specifically requires amendments to be agreed in writing, the ETQA may not be effective to validate an agreement to amend a contract that has been reached via electronic communications. Briefly, those arguments include:

- **State law:** Sections 11 and 12 of the ETQA can only apply where it is a 'State law' that permits or requires information to be given in writing. It is clear that the concept of a 'State law' embraces not only statutes that have been enacted by Parliament, but also general law contractual principles. However, in the situation at hand, it is the contract between the parties which requires a variation or amendment to be agreed in writing, rather than a requirement or a permission under a statute or the general law.

  Accordingly, it may be argued that ss 11 and 12 of the ETQA cannot apply, as there is no relevant 'State law' that requires or permits the giving of the relevant information in writing. However, an alternative argument that may be raised is that a contractual provision that requires amendments to be communicated in writing does constitute a requirement under a 'State law', as general law contractual principles would give effect to the parties' contractual arrangements and require that a valid amendment to the contract take place in writing.

- **Giving information in writing:** Sections 11 and 12 of the ETQA only apply where there is a requirement or a permission to 'give information' in writing. Although the ETQA definition of 'give information' is not exhaustive, none of the actions contained in the definition resemble the formation of a binding agreement between two parties to amend an existing contract. Indeed, it has been argued that the very concept of 'information' is different to the expression of a will to be bound by an agreement. Although the definition of what it means to 'give information' is not exhaustive, it may be ambitious to argue that the concept extends to exchanges between parties that bring about the formation of a contract or an agreement to amend an existing contract (Sheridan & Rigotti 2001, pp48-9; Christensen, Duncan & Low 2002, p60). If these arguments are valid, ss 11 and 12 of the ETQA would not apply to validate an agreement to amend a contract that has been reached through electronic communications.

- **Consent and accessibility for subsequence reference:** Even if there is scope for ss 11 or 12 of the ETQA to apply in the present scenario, it must also be established that there was consent to the amending agreement being reached electronically, and that at the time the information was given, it was reasonable to expect the information would be readily accessible so as to be useable for subsequent reference.

- **The ETQA general rule:** If ss 11 and 12 of the ETQA do not apply, then s 8 of the ETQA may apply. This section would generally provide that the agreement to amend the contract is not invalid merely because it has taken place wholly or partly by one or more electronic communications. However, there are countervailing arguments to the effect that s 8 of the ETQA should not be able to be relied upon to give effect to an electronic amendment of a contract where the contract specifically requires that all amendments to the contract must be in writing. These arguments include: that this may override the general law position that the parties have the right to contractually determine the mode and manner in which amendments to the contract are to take place, and that s 8 of the ETQA should be interpreted as being subservient to any laws which provide for a result that is contrary to s 8 of the ETQA (Sheridan & Rigotti 2001, p49).

Ultimately, until there is further judicial analysis by the courts, it is unclear whether or not the ETQA can be relied upon to establish that an electronic agreement to amend a contract is in 'writing'. However, under the general law it is probable that the amending agreement will be in 'writing' if the electronic communications are printed.

Case law in other jurisdictions supports this conclusion. For example in England, an Industrial Tribunal case has held that an employment agreement was effectively amended by email exchanges, where the terms of the employment agreement required any variations to be 'in writing and signed by the parties' (*Hall v Cognos Ltd* (Industrial Tribunal Case No. 1803325/97)). It was argued that the emails did not constitute an effective variation of the employment agreement as the emails were not in writing and signed. These arguments were rejected by the tribunal, which was satisfied that:

> …an e-mail is "in writing and signed by the parties" once it is printed out. The position might (it is not necessary to make any finding on this point) be different if the e-mail was only retained temporarily on the computer's hard disk storage system. The documents that were, however, produced from the computer are clearly in writing and bear the signatures of both 'Sarah' and 'Keith'. The fact that those signatures are printed, rather than hand-written, is not in my view material. For those reasons, I reject [the] submission that the relevant e-mail messages are incapable, as a matter of law, of having any modifying effect on the specific contract between the parties. (at [5])

Accordingly, the fact that an amendment agreement has been reached by email or other electronic communications will not necessarily preclude a finding that the agreement is in 'writing'.

Contractual signature requirements

The analysis of whether or not an electronic amendment agreement can be said to be 'signed' is similar to the discussions in section 7 of this Report (relating to statutory requirements for contracts to be signed).

While it appears that s 14 of the ETQA may potentially be relied upon to establish that an electronic amendment agreement that has been authenticated by an

electronic or digital signature has been 'signed', the main issues that may be encountered in this context are:

- whether a contractual requirement for the variation to be signed can be said to be a signature requirement under a 'State law';
- whether consent has been given to the use of the signature method; and
- whether, having regard to all relevant circumstances at the time the signature method was used, the signature method was as reliable as was appropriate for the purposes for which the information was communicated.

As previously noted, until there are further judicial decisions on the application of s 14 of the ETQA it is difficult to determine how a court will approach these issues. However, under the general law, there is authority in England to the effect that email communications containing type-written names at the end of the messages are effective to amend an agreement that requires all amendments to be in writing and signed (*Hall v Cognos Ltd* (Industrial Tribunal Case No. 1803325/97)). Accordingly, if a contract is silent on the issue of electronic communications, the fact that an amendment agreement has been reached by email or some other electronic communication method may not necessarily preclude a finding that the agreement has been 'signed'.

8.2 Resolution

Until the courts have had the opportunity to consider the various provisions of the ETQA, it is difficult to conclude whether the ETQA may be relied upon to establish that an electronic agreement to amend a construction contract will constitute an agreement that is in 'writing' and 'signed'. However, under the general law, there is authority to suggest that an electronic agreement that has been printed and authenticated by an electronic signature (or potentially a digital signature) will amount to an effective amendment of the construction contract as it is in writing and signed.

To avoid these uncertainties, is vital for contracting parties to expressly address the issue of electronic communications in their contract documents. Parties may wish to include separate provisions that deal specifically with amendments to the contract, or may wish to deal with the issue through the more generalised notice and communication provisions in their contract. In either case, the contractual provisions must be clear as to which communications under the contract may and may not take place in electronic form. The various matters that should be considered when drafting these provisions are discussed in detail in section 9.2 below.

9. ELECTRONIC NOTICES

9.1 Risk

Construction contracts invariably contain contractual provisions that govern the delivery of notices under the contract. Depending on the terms of the construction contract, it may be unclear whether electronic notices are valid.

In the unlikely event that a contract is absolutely silent as to communications under the contract, it is possible that the ETQA and general law contractual principles may recognise the validity of a notice that has been delivered by electronic means. As far as the ETQA is concerned, one of the main issues to be considered is whether from the conduct of the parties and the surrounding circumstances, the parties have impliedly consented to notices being given in electronic form (Mallesons 2003).

However, where a contract contains a specific notice provision that does not refer to electronic notices, it would be unlikely that a court would uphold an electronic notice as valid. This would most likely be the case unless the parties have continuously carried out their contractual obligations in reliance on electronic notices, such that one party would suffer detriment as a consequence of an electronic notice being held to be invalid. Ultimately, the issue would be resolved by interpreting the contractual notice provision and by reviewing the conduct of the parties.

Due to the legal uncertainties that surround the validity of electronic notices, it is imperative for construction contracts to include appropriately drafted provisions that clearly identify the parties' intentions in relation to electronic communications. Regardless of whether or not the parties to a construction contract wish to be bound by electronic communications, the only way to clarify this issue is to incorporate clear provisions within the contract.

9.2 Resolution

To avoid the legal uncertainties about the status of electronic notices, construction contracts must contain clear provisions setting out the parties' agreement as to how valid notices may be given under the contract. It is recommended that when drafting notice provisions, regard should be had to the following matters:

- The contracting parties must first decide whether they wish to be bound by any electronic notices. If they do not wish to be bound, then the contract should clearly exclude electronic communications as a valid form of notice delivery. This is particularly the case if the parties otherwise use electronic communications for day to day correspondence.
- If the contracting parties do wish to utilise electronic communications for delivering notices, they should consider whether they wish to contractually avail themselves of effective electronic communications for some, but not all contractual notices (for example, the parties may wish more important communications such as variations to the contract and notices of default to be delivered in paper form). The communications that are to remain paper based should be clearly excluded by appropriate contractual provisions (Briggs & Brumpton 2001, p30). Ultimately, the contract must make it abundantly clear which notices and communications can and cannot be delivered electronically.
- The electronic communication method to be used should be identified and the relevant electronic addresses and details of authorised recipients should be stated.
- To rely on various provisions of the ETQA it is important to establish that the parties have consented to the use of electronic communications. Accordingly, the parties should expressly consent to the use of electronic communications, but only to the extent specified in the contract.
- From a legal perspective it can be difficult to determine the time that an electronic notice has been received. Although various email systems may provide the functionality to track emails and generate received and read notifications, these notifications are generally unreliable and may even be blocked by the recipient of an email communication. The contract should include a timing provision to govern when electronic communications will be deemed to have been received by the parties. The nature of the provision will, to a large extent, depend on the electronic communication method being used and the commercial acceptability of the proposed provision to both contract parties.

- A construction contract will invariably contain requirements for notices and other communications to be in writing and signed. The contract should deem those notices and communications that the contract allows to be delivered by electronic means, to be in writing and signed. In relation to electronic signatures, the contract should identify the precise signature method to be used (for example type-written names, scanned handwritten signatures etc), the parties should consent to the use of that method and acknowledge that they consider the method to be both reliable and appropriate.
- Where the contracting parties use an online collaboration system for electronic communications, it is conceivable that the system may become temporarily unavailable at some stage during the life of the contract. To cater for this occurrence, the parties may wish include a contractual provision setting out alternative communication protocols to be followed in the event that the system becomes unavailable.

10. AVAILABILITY OF THE PROJECT COLLABORATION SYSTEM

10.1 Risk

Where a construction project is administered electronically using an online collaboration system, the project may be disrupted if the online collaboration system is unavailable for any length of time. The system could be unavailable because of technical difficulties or, if the system is provided by a third party service provider, because the service provider has ceased business.

10.2 Resolution

To avoid uncertainty about the parties' liability in the event the online collaboration system becomes unavailable, the contract with the service provider should include provisions regarding disruptions to the system (Wilkinson 2005, pp115-117). The types of provisions that should be considered include:

- Details of any scheduled service disruptions to the collaboration system;
- The notification that is required to be given to the users of the system in the event of any unscheduled downtime;
- What will happen in the event of the system crashing; and
- Arrangements to take place in the event the service provider becomes insolvent, which may include a right to transfer the contract for provision of the system to an alternative service provider.

It is further recommended that the users of the system should consider whether they require interruption to business insurance that covers them for liability in the event they suffer loss as a consequence of the collaboration system becoming unavailable (Berning & Diveley-Coyne 2000).

11. COMPATIBILITY OF TECHNOLOGY

11.1 Risk

If the parties use incompatible technology to process electronic records, there may be difficulty ensuring that each party's view of the records is consistent with the other party's view. For example, where the parties use different versions of the same collaboration system to carry out a construction project, it is possible that some of the

software components available in the latest version of the system may not be available in the previous version. Accordingly, the integrity of the electronic record is not assured.

Risk Example

The parties to a construction contract use a collaboration system for the administration of the project. Company A uses the latest version of a collaboration system and Company B uses an older version of the system. When A sends a project record to B, the record does not appear to B to be the same as the record sent by A. This is because the formatting appears differently in the old version of the system.

In addition, the record sent by A included a construction diagram created using a special tool only available on the new version of the system. Because the older version of the system cannot read the diagram it does not appear on the record as viewed by B when using the older version of the system.

Risk Example

Following on from the previous example, A and B now use the same version of the collaboration system. However while their computer systems both use the Microsoft Windows operating system (Windows OS), they use different versions of Windows OS. The particular collaboration system used has backward compatibility with some software applications such as Microsoft Word in the latest version of Windows OS but does not have backward compatibility with applications using older versions of Windows OS. As a result, project records created using the latest version of Windows OS may appear with different formatting and possibly with different content on the collaboration system installed on the computer system using the older version of Windows OS.

This problem may also occur when the parties use different operating systems, for example Linux and Windows, if the backward compatibility does not work in one of the operating systems.

There is an additional risk that the performance of collaboration systems designed for computers running a 32-bit version of Windows OS may become slow when they are run using a 64-bit version of Windows OS. In this case, there may be possible project completion delays from the parties that use a slower operating system to run the collaboration system.

11.2 Resolution

The following recommendations are made to avoid questions as to the integrity of electronic records arising as a result of a lack of compatibility of software and operating systems:

- A collaboration system designed to run on computers with 32-bit processors should only be used on computers with 32-bit processors (even if it can run on computers with 64-bit processors).
- All collaborating parties should use the same version of the collaboration system.

- If the collaboration system has backward compatibility with some of the applications in the operating system, then it is recommended that all the parties use the same operating system to make the best use of those features of the operating system.
- Companies using online collaboration systems to carry out e-contracting should follow the best practice standards of using information technology as recommended by the Information Technology Infrastructure Library (ITIL) (http://www.itilpeople.com/). ITIL is a set of best practice standards for IT service management owned by the United Kingdom's central computer and telecommunications agency (CCTA) and currently maintained by the Office of Government Commerce.

12. DISPUTES BETWEEN THE SERVICE PROVIDER AND THE CONTRACTING PARTIES

12.1 Risk

Disputes may arise between the contracting parties and the provider of the collaboration system (who may be a third party or one of the contracting parties) regarding the use of the system. For example, the level of service provided may not be of the standard represented by the service provider or expected by the users of the system. In the event a dispute arises, further disagreements may occur, for example regarding the use of the project collaboration system or the use of the contracting party's branding and data for promotional purposes by the service provider.

Risk Example

Company A is the head contractor for a large construction project. The project is administered using an online collaboration system provided by Company B. A has several subcontractors involved in the project who also need to use the online collaboration system. The agreement between A and B provides for the use of the system by other parties involved in the construction project. However, due to the number of subcontractors, the system is not able to handle the load of a large number of users simultaneously accessing the system.

12.2 Resolution

It is recommended that to minimise disputes arising due to uncertainty about the rights and obligations of the service provider and the users of the system, the service provider should enter a contract with all of the proposed users of the project collaboration system. The types of provisions that should be part of the agreements include the following (Wilkinson 2005, p111):

- The levels of service to be provided should be specified including specifications as to security, backup systems, integrity of data, audit trails, access controls, technical specifications, system availability, software upgrades, customer support and end-user training;
- The users of the system should be granted a licence to use the system in relation to the project;
- Parameters should be established to govern the use of the project data by the service provider and the project participants;

- The ownership of the copyright in the project collaboration system technology should be specified;
- Any right of the service provider to use the project participant's branding and data should be specified;
- The service provider should be indemnified against the unauthorised use of the collaboration system;
- The parties should be under a specific duty of confidentiality which should include the security of user names and passwords;
- Any limitations upon the liability of the service provider should be specified; and
- The responsibility for the storage of data upon completion of the project should be allocated to one or more of the parties.

It is further recommended that where a project collaboration system is to be used by consultants who are not parties to the original agreement with the service provider, those consultants should enter into end user licence agreements for the use of the system containing similar provisions to those listed above (Wilkinson 2005, p116).

13. DISPUTES BETWEEN THE CONTRACTING PARTIES

13.1 Risk

There is a risk that the parties to a construction project may become involved in disputes as a result of the electronic administration of the project. For example, parties may breach the confidentiality of documents. Breaches of confidentiality may be more widespread because of the ease of copying and distributing electronic documents (breaches of confidential information are considered in section 15 below). Intellectual property infringements may also be more likely as a result of the electronic sharing of plans and drawings. (Intellectual property infringements are considered separately in section 14 of this Report).

13.2 Resolution

It is recommended that the contractual arrangements between project participants should contain provisions in relation to the electronic administration of the project. The contract should include:

- Provisions regarding the ownership of the database, obligations of confidentiality and commercial advantage (Briggs & Brumpton 2001, pp30-31) (confidentiality is considered in more detail in section 15);
- A clause deeming electronic records kept by the project collaboration system to be admissible as evidence and prima facie accurate (Reed 2001, p91); and
- Provisions relating to the ownership of intellectual property in project drawings and designs (considered in section 14 below).

14. INTELLECTUAL PROPERTY

14.1 Risk

Where drawings are submitted electronically and stored on a project collaboration system, disputes may arise in relation to the intellectual property in the drawings.

The general legal position is that the author of designs and drawings is the owner of the copyright in them (s 35 *Copyright Act 1968* (Cth)). The parties may agree to an assignment of the copyright in the designs and drawings to the contractor or owner of the building or to a licence being granted for the use of the designs and drawings for the purposes of the project (s 196 *Copyright Act 1968* (Cth)). The usual position is that the designer retains the copyright in the design and grants a licence to the client and other project participants to use the design in relation to the project (Wilkinson 2005, p121). Even if the agreement between the designer and the contractor does not provide for such a licence, there would be an implied licence to use them for the project (*Concrete Pty Ltd v Parramatta Design & Developments Pty Ltd* [2006] HCA 55). Construction projects normally provide for the ownership of copyright in the designs and drawings relating to the project.

The legal position would not normally change as a result of the use of an online collaboration system, however, where drawings are submitted electronically and stored on the collaboration system, there may be a greater risk that intellectual property rights in drawings will be infringed given the ease with which copies of the drawings can be made and shared.

There is a further risk that if designs and drawings are amended extensively by online collaboration, that the ownership of the copyright in the design or drawing no longer rests with the original designer (Wilkinson 2005, p121).

Risk Example

Company A is the head contractor for a large construction project. The project is administered using an online collaboration system. A appoints Company B as the project architect and Company C as the project engineer. The agreement between A and B provides that B retains copyright in all designs and drawings relating to the project and B grants a licence to A to use the designs and drawings for the project. During the approval process for a particular design relating to the project, extensive changes to the original design prepared by B are made using the online collaboration system by employees of both A and C. As a result of the changes it can no longer be certain that B is the author of the final design.

C uses the design as the basis of a design for another project on which it is working.

B wishes to bring an action for copyright infringement against C. B can only bring an action for copyright infringement if it is the owner of the copyright (s 115 *Copyright Act 1968* (Cth)). Further, as C may be a joint owner of the design it may not have infringed copyright by using the drawing.

14.2 Resolution

To minimise the risk that drawings will be circulated electronically without acknowledgement of copyright, designers should take practical steps to protect their copyright in drawings. The following practical steps are recommended (Wilkinson 2005, p121):

- Designers should include a copyright disclaimer and statement of permitted use on all drawings;
- Drawings should include a copyright statement and the designer's name and logo; and
- Drawings should be watermarked with the designer's name and logo.

To avoid doubt arising as to the ownership of the copyright in project drawings, the agreement between the project participants should specifically deal with the ownership of copyright in the project drawings. For example, the contract may provide that the designer retains the copyright in the drawings and grants a licence to the client and other project participants to use the drawing in relation to the project.

The contract between the project participants should also specify that the provisions regarding the ownership of the project drawings apply regardless of the extent of the collaboration between the parties in the development of the drawings.

15. CONFIDENTIALITY

15.1 Risk

Confidentiality refers to electronic records being able to be accessed, used, copied or disclosed by the people who are authorised to access, use, copy or disclose them and when there is a legitimate necessity to access, use, copy or disclose the contractual information.

There is a risk that the confidentiality of electronic records may be compromised during communication or retention. There is a significant risk involved in leaking the user credentials when the contracting parties establish contracts or transfer contractual documents using a web-based email service without using appropriate encryption technology to encrypt the email messages. In this case, it could be possible for unauthorised personnel to view the user credentials such as a user name and password. In addition, email messages can be intercepted or misdelivered and read by unauthorised personnel (Garfinkel et al 2005). It is also important to protect the confidentiality of the electronic records when they are archived. They must only be able to be accessed by or disclosed to authorised personnel.

Risk Example

Company A transmits a highly confidential document relating to a construction project to Company B by email. During the transmission, the email is intercepted by a malicious third party who makes public the contents of the document to the commercial detriment of both A and B.

15.2 Resolution

It is recommended that the agreements between the project participants and the agreements between the project participants and the service provider of a collaboration system should include provisions imposing on the parties a specific duty of confidentiality. The duty of confidentially should extend to the security of user names and passwords.

It is further recommended that the SSL protocol or its next versions, TLS 1.0 or TLS 1.1, be used in order to ensure the confidentiality of an electronic record when it is transmitted from one computer to the other across the internet. SSL is the most common standard for secure Internet communications (Freier et al 1996). SSL uses public key cryptography to ensure the confidentiality and integrity of documents sent over a communication network.

The document confidentiality security property for the documents in the system ensures that only authorised users may access documents. Many documents that are stored and created within a collaboration system may contain sensitive

information that should not be shared with unauthorised users. The implementation of an access control policy such as a role-based access control system assists the document confidentiality security property by only allowing authorised users based on their roles to access data within the collaboration system. The use of authentication mechanisms such as restricted access to the systems using the Internet protocol (IP) addresses and user name and password mechanisms can also assist in achieving the confidentiality of the documents. Cryptographic mechanisms such as encryption algorithms may be used to provide this aspect of the document confidentiality feature for stored documents.

16. ADMISSIBILITY AS EVIDENCE

16.1 Risk

The management of a construction project results in the creation of a large number of records. There is a risk that records created and maintained electronically may not be admissible in court as evidence in the event of a dispute. The key reasons electronic records may be inadmissible are that they may be considered to be hearsay or they may not be considered to be an authentic copy of the record that is to be produced.

General legal principles regarding evidence in Australia

Evidence is the means by which facts in dispute in any court proceedings are proved. To be admissible the evidence must be relevant either to prove a fact in dispute, to the credibility of a witness or to the reliability of other evidence; and must not be inadmissible by reason of some particular rule of law such as the rule against hearsay (Laryea 1999, para 8).

The rules as to inadmissibility that are relevant in an electronic environment are the rule against hearsay and the best evidence rule.

If the evidence is admissible, it is then for the court to determine the weight to be attached to the evidence. Even though the evidence may be admissible, it may be given less weight by the court if it does not tend to be believable or reliable (National Archives of Australia 2004).

The rules of evidence vary depending on the court in which the litigation takes place. There are different rules of evidence in each State and Territory and in the Federal jurisdiction. Proceedings in Federal courts are governed by the *Evidence Act 1995* (Cth) and the rules of the relevant court. The provisions of the *Evidence Act 1995* (Cth) are mirrored in the New South Wales and Tasmanian Acts and apply by agreement in the Australian Capital Territory. The Acts based on the Commonwealth Act are known as the uniform Evidence Acts. Proceedings in other State courts are governed by the relevant State Evidence Act. The relevant evidence Act in each State is listed in the table below.

Jurisdiction	**Legislation**	**UEA Y/N**
Federal (including ACT)	*Evidence Act 1995* (Cth)	Y
New South Wales	*Evidence Act 1995* (NSW)	Y
Northern Territory	*Evidence Act 1939* (NT)	N

Queensland	*Evidence Act 1977* (Qld)	N
South Australia	*Evidence Act 1929* (SA)	N
Tasmania	*Evidence Act 2001* (Tas)	Y
Victoria	*Evidence Act 1958* (Vic)	N
Western Australia	*Evidence Act 1906* (WA)	N

Hearsay rule

The hearsay rule will apply to exclude electronic records that contain a statement made by a person where the record is sought to be admitted as proof of the truth of the statement (Forbes 2004, p300). As a result of the hearsay rule, a question may arise as to whether emails and other electronic project records are inadmissible in court.

The hearsay rule will not apply to computer generated data, such as meta-data and audit trails (Wolfson 2005, pp157-9). In the case of computer generated records what will be necessary is to prove the accurate working of the computer that generated the record.

The hearsay rule will not impact on the admissibility of electronic documents such as the construction contract, notices and contract variations as they are sought to be relied on as proof of the terms of the contract or of the giving of the notice and not as proof of a statement made by a person. For such documents the possible barrier to admissibility may be proving the authenticity of the record, in other words that the electronic record is an accurate copy of the document to be produced in court.

Risk Example

Company A is the head contractor for a large construction project. Company B is appointed to provide engineering services to the project. The project has encountered unexpected flooding of the building site. Z, an engineer employed by B, makes a statement in an email to A that his inspection of the site suggests the flooding is due to the faulty drainage works completed by another contractor, Company C. A now wishes to institute legal proceedings against C to recover damages for the flooding which they believe was due to C's faulty drainage works. The engineer is no longer available to give evidence and A wishes to use the email as evidence that the flooding was the result of the drainage works.

As the email is sought to be relied on as proof that the drainage works were responsible for the flooding as stated by the engineer the hearsay rule will apply. The email will not be admissible unless one of the exceptions to the hearsay rule applies.

Business records exception

In civil proceedings there is an exception to the hearsay rule known as the business records exception. The relevant provision establishing the business records exception in each jurisdiction is set out in the table below.

Jurisdiction	Section
Uniform Evidence Acts	s 69
Northern Territory	s 26D
Queensland	s 92
South Australia	s 45A
Victoria	s 55
Western Australia	s 79C

The business records exception allows records to be admitted where they form part of the record of an undertaking and were made from information supplied by a person who had personal knowledge of the matters. In Queensland, Northern Territory, South Australia, Victoria and Western Australia the person making the statement is required to be called as a witness unless they are unavailable. The grounds on which the maker of the statement will be considered to be unavailable differ in each jurisdiction. In Queensland, for example, the grounds for unavailability are that the person is dead, out of the State or their attendance is not reasonably practicable, they cannot be found, they have no recollection due to the passing of time, or they would not be permitted to be cross-examined. There is no requirement under the uniform Evidence Acts that the maker of the statement give evidence.

Electronic records are likely to fall within the business records exemption if they are created within a routine controlled and documented business process or as part of the ordinary administration of the organisation. It is likely that project records and email communications between the parties will be admissible as business records, as they are part of the record of the undertaking. An email was held to be admissible as a business record in *Rickard Constructions Pty Ltd v Rickard Hails Moretti Pty Ltd* [2004] NSWCC 30). In *Cooper v Bankstown-Lidcombe Health Service (Lidcombe Hospital)* [1998] NSWCC 30 computer stored records of golf scores kept by a golf club were admissible as business records. Applying the rationale in the *Lidcombe* case it is suggested that the argument that project records are part of the business undertaking will be strengthened where the records are maintained by an online collaboration system that is used for the purposes of administering the project by the parties.

Representations in electronic communications

The uniform Evidence Acts also contain an exception to the hearsay rule for electronic mail, faxes, telegrams, lettergrams and telexes. The exception only relates to the identity of the sender, the date of the message and the destination of the message. It does not relate to the contents of the message (s 71 uniform Evidence Acts). Due to the use of the narrow term ‘electronic mail’ the exception is likely to be restricted to email and may not apply to other forms of electronic communication such as electronic data interchange, internet relay chats, computer based instant messaging and phone text messaging (ALRC 2005 pp150-155). It is not clear whether the exception will apply to electronic communications taking place via an online collaboration system. There is no equivalent to s 71 in the legislation in the States and Territories which are not covered by the uniform Evidence Acts.

Computer generated data

In Queensland, South Australia and Victoria there is an exception to the hearsay rule for statements contained in documents produced by computers. Computer generated records will be admissible if the requirements of the relevant section are satisfied. The relevant sections are listed in the table below. What is required is a certificate that the statement was produced during the regular use of the computer, the data was supplied to the computer in the ordinary course, there has been an absence of computer malfunction and the statement reproduced information supplied to the computer in the ordinary course.

Jurisdiction	**Section**
Queensland	s 95
South Australia	s 59B
Victoria	s 55B

It is not clear whether the statutory exception for computer produced documents applies where the computer merely acts as a storage device for existing documents or whether it is restricted to situations in which computers process information which results in new information. Reynolds (1994) argues that the statutory exception is only intended to apply to the latter situation and not to documents which are merely stored by computers.

In jurisdictions where there is no exception for computer generated evidence the common law position will be relevant, the hearsay rule will not apply to computer generated records that do not involve any significant human involvement (*Castle v Cross* [1984] 1 WLR 1372; Forbes 2004, p337) or that are generated by a computer acting as a calculator or scientific instrument (*Mehesz v Rdeman* (no 2) (1980) 26 SASR 244; *R v Weatherall* (1981) 27 SASR 238 at 247; *R v Wood* (1982) 76 Cr App R 23; Forbes 2004, 338). Computer generated records will be admissible if the accurate working of the computer system that generated the record can be proven. The accurate working of the computer system can be proven by evidence given by the programmer, the operator of the program or other evidence that the computer was competently maintained and that any malfunction has not affected the material produced by it (Halsbury 1991, para 195-4015). The common law exception may be applicable to computer generated records such as meta-data and audit logs (Wolfson 2005, pp157-9).

Risk Example

Company A uses an online collaboration system to administer a construction project. The system is used by the company to send electronic communications to Company B which is a subcontractor involved in the project. Z is the site engineer employed by A on the project. Z sends an electronic communication to B providing information as to the state of the building works at the time the communication is sent. A and B are now involved in a dispute relating to the project and A has commenced legal proceedings. A wishes to rely on the electronic communication in court as evidence of the state of the building works at the time. Z has since been dismissed from his employment with A and A is reluctant to call Z as a witness because he may be hostile to A's case.

The email may be admissible as a business record. However, in States other than those where the uniform Evidence Acts apply, A will be required to call Z as a witness because he is available to give evidence. In jurisdictions where the uniform Evidence Acts do apply A will be able to rely on the electronic communication as evidence without calling Z as a witness.

Alternatively, in Queensland, Victoria and South Australia, the electronic communication may arguably be admissible without Z being called as a witness as a computer generated record under the relevant statutory exception.

In the Northern Territory and Western Australia the electronic communication would not be admissible without calling Z as a witness. The common law exception in relation to computer generated evidence applies only to electronic records generated without significant human involvement or where the computer is merely acting as a scientific instrument.

Risk Example

Company A receives an email from Y who is an employee of Company B. The email contains admissions that support A's case against B in the litigation of their dispute. B now denies that the email was sent by Y. In UEA jurisdictions, A can rely on the message detail in the header of the email as evidence of the identity of the sender of the message. (Considerations relevant to how much weight the court will attach to such evidence are examined in section 17 of this Report). In other jurisdictions the statutory or common law computer generated records exception may be applicable. The identity of the sender may be revealed by the meta-data attached to the email. (Again the weight to be attached to such meta-data will depend on considerations examined in section 17).

If the electronic communication in question was not sent by ordinary email but by using some other means such as an online collaboration system s 71 of the uniform Evidence Acts may not apply because of the use of the narrow term 'electronic mail' in the provision. In that case A would need to rely on the common law exception in relation to the meta-data associated with the communication.

Best evidence rule

The best evidence rule provides that where a document is tendered as evidence, the original document is required and a copy will not suffice (*Ormychund v Barker* (1745) 26 ER 15). According to the best evidence rule a copy would only be admissible if the original was unavailable and the copy was authenticated (Laryea 1999, para 44). The best evidence rule has now been abrogated by the operation of statute and the common law (*Butera v Director of Public Prosecutions for the State of Victoria* (1987) 164 CLR 180, 186). Provided the authenticity of electronic records can be established and their integrity proved the best evidence rule should not prevent them from being admissible. It is for the courts to determine the evidential weight to be given to copies of documents (Davidson 1999, p29).

Section 97 of the *Evidence Act 1977* (Qld) provides that where in any proceeding a statement contained in a document is proposed to be given as evidence it may be proved by the production of a copy of that document authenticated in such manner

as the court may approve. In addition, Part 7 of the *Evidence Act 1977* (Qld) contains provisions in relation to the admissibility of copies of documents in court proceedings. The relevant provisions abolishing or abrogating the best evidence rule in the various jurisdictions are listed in the table below.

Jurisdiction	**Section**
Uniform Evidence Acts	s 51
Northern Territory	S 14
Queensland	s 97
South Australia	s 45C
Victoria	s 46
Western Australia	Nil

Where a party wishes to rely on a digitised copy of a paper record, in order for it to be given maximum weight as evidence, the party will need to be able to demonstrate that the copy has not been tampered with, that it is an authentic reproduction and that the integrity of the information in the copy is maintained in a reliable way (Queensland State Archives 2006).

Authenticity

An electronic record will not be admissible unless it can be proven that the record produced in court is an authentic copy of the record (*Butera v Director of Public* Prosecutions for the State of Victoria (1987) 164 CLR 180). Authenticity is used in this section of the Report in its legal sense, that is proving the document is what it purports to be, rather than in the technical sense (as defined in section 2.3). In practice, in order to meet this requirement, courts generally only require oral evidence that the computer system was operating correctly at the time unless evidence to the contrary is produced by the other party (Reed 2001, p90). Accordingly, issues relating to the authenticity of a record (in the legal sense) are dealt with in more detail in section 17 of this Report which considers the weight that a record may have as evidence. The two key risks (aside from the general concern to establish the integrity of an electronic record) in relation to authenticity of electronic records result from the digitisation of paper records and the printing of electronic records.

Where a paper record is digitised (by being scanned into a computer) the digitised record may be inadmissible if the party relying on it cannot satisfy the court that it is an authentic copy of the electronic record.

Where a paper copy of an electronic record, such as an email, is sought to be admitted, there may be a question as to the authenticity of the record. However, the courts routinely allow print outs of electronic evidence to be admitted as evidence because such evidence is generally not disputed by the other party (Public Records Office Victoria 2003). If the other party disputes the evidence the court must assess the admissibility and weight of the record. One reason for disputing the admissibility of the print out may be if the original electronic record contains information such as

meta-data which is not included in the print out (Davidson 1999, p29; *Armstrong v Executive Office of the President* 810 F Supp 335 (D.D.C. 1993)).

16.2 Resolution

Participants in a construction project can take several steps to maximise the likelihood of electronic records being admissible as evidence in court.

To improve the possibility of an electronic record being admissible as a business record, parties should ensure that the electronic record is 'part of a record relating to [the] undertaking' (s 92 *Evidence Act 1977* (Qld)). It is likely that email communications and project records will be found to be part of the record relating to the undertaking. Records retained by an online collaboration system are highly likely to be admissible as business records.

Where paper records are digitised, parties will need to be able to demonstrate the authenticity, integrity and reliability of the electronic record. Recommendations are made in sections 17.2 and 19.2 below in relation to these matters.

As discussed in section 13 of this Report the agreement between the project participants using an online collaboration system should include a provision deeming electronic records kept by the system to be admissible as evidence and prima facie accurate (Reed 2001, p91).

To avoid the potential of paper copies of electronic records being found to be inadmissible, ideally parties should maintain original electronic records that can be relied upon in court in the event of a dispute.

If paper records are digitised for record keeping purposes then it is recommended that a system for establishing that the resulting electronic record is a complete and accurate copy of the paper record be followed. For example, where paper records are scanned onto a computer, one must ensure that the scanner reproduces the digital format of the paper records accurately. That is, the electronic records should be intelligible and look like the paper records. There may be inaccuracies if the scanner has defects in its font, colour or other settings. Additionally, the computers used to store digitised records should correctly record the details of the personnel who scanned the paper records along with the correct time and date, together with the time stamp for the electronic records. This ensures electronic data origin authentication of the parties who scan the paper documents. It is also recommended that digital signatures be applied to digitised records in order to ensure not only a strong form of authenticity and integrity of the electronic records but also cryptographic non-repudiation. To ensure a strong form of cryptographic non-repudiation, these digital signatures may also be time stamped using the services of a time stamping authority.

17. EVIDENTIAL WEIGHT

17.1 Risk

While an electronic record may be admissible as evidence in the event of a dispute, a court may not give the electronic record the same evidential weight as a paper record. The court may not necessarily believe or act on the evidence (National Archives of Australia 2004). The key issues that may impact on the evidentiary weight to be attached to an electronic record will be establishing the integrity of the record (i.e. it is an accurate and unaltered copy of what it purports to be), that it is authentic (i.e. it has emanated from the source it purports to be from) and the time of

its creation or communication. Establishing the authenticity of an electronic record is considered in section 19 of this Report and establishing the time of creation or communication of a record is considered in section 18 of this Report.

The integrity of a record may be in doubt if it cannot be proven that the record has not been altered by human intervention or corrupted by computer malfunction. While issues as to the integrity of electronic records have generally not arisen in court to date, with electronic records being generally accepted on their face (ALRC 2005, p150), it may be that electronic evidence may be challenged in the future as lawyers become more familiar with the technical challenges that may be raised (Spenceley 2003).

One issue in particular that may be raised by a party objecting to evidence being relied upon is where the party relying on the evidence cannot establish the chain of custody of the original electronic record from the time it is created or identified as evidence to the time it is produced in court (Reed 2001, p90; Standards Australia 2003, p22).

Risk Example

Company A is the head contractor and Company B is a building contractor on a construction project. An employee of A provides to B's site foreman a computer disk containing a schedule of specifications relevant to the building works. The foreman takes the disk home to work on that evening. When he finishes working, he puts the computer disk in his drawer. The home computer is used by the foreman's family and the disk is unsecured.

A and B subsequently become involved in a dispute relating to the project. The schedule of specifications is relevant to the dispute and B wishes to rely on it as evidence supporting its case. The disk is admissible, the hearsay rule does not apply because the schedule is relied on not as proof that it is correct but only as proof of the information supplied by A to B.

If A denies that it gave the information to B as alleged it may object to the court placing evidentiary weight on the disk because B will be unable to prove that the information contained on the disk has not changed since it was given to the foreman. Any person with access to B's home office could have altered the data contained on the disk.

17.2 Resolution

While non-technical means of authenticating an electronic record exist (Casamassima & Caplicki 2003), for example by evidence of a person who saw the record being created or communicated (Robins 2003, p226), such means will not always be available in relation to a particular record. An organisation wishing to ensure that it can establish the integrity of an electronic record if required to do so in court would need to put in place technical means of ensuring that it can do so.

The technical means of ensuring the integrity and authenticity of an electronic record include using SSL and digital signatures. The SSL protocol uses message authentication codes (MACs) to ensure the integrity and data origin authentication of the information exchanged over the Internet. The TLS version 1.0 (Dierks & Allen 1999) is the next version of SSL version 3. The TLS version 1.1 is the next version of TLS version 1.0 (Dierks & Rescorla 2006). It is recommended that any of these

protocol versions be used for all communications in an e-contracting process, to ensure the integrity of the information communicated over the Internet.

If the electronic record is of such importance that a higher degree of evidential certainty should be attached to it, then it is recommended that the electronic record be signed using digital signature technology which assures the integrity of the message, data origin authenticity and cryptographic non-repudiation. The security of the cryptographic hash function guarantees the integrity and authenticity of the electronic record and the secrecy of the signer's private key assures the origin of the electronic record. Time stamps also guarantee the authentication of digital signatures computed in the past, as digital signatures without time stamping become invalid when the digital certificate expires. Time stamping also assures integrity well into the future.

If an online collaboration system is used, the system will usually have features such as the automatic saving of electronic records, the creation of a new version for every new document and the automatic archiving of all previous document versions. The system will generally not allow the users of the system to alter or delete any records. These functional features provide only a weak form of authenticity, integrity, and cryptographic non-repudiation. Stronger forms of authenticity, integrity, and cryptographic non-repudiation are achieved by computing digital signatures on the documents (discussed in sections 7.1 and 18 of this Report). The existence of a record at a particular point in time is more readily achieved by using digital time stamping (discussed below in section 18).

Online collaboration systems also usually employ a role-based access control policy whereby system users have their own identity, responsibilities and access permissions in accordance with their role within the project and the company for whom they work. The systems are configured in such a way that they permit users to view only documents or document types that are applicable to them, or which they have been given permission to access.

Accordingly, the desired security properties of authenticity, integrity, and non-repudiation may be satisfied when all of the parties who are involved in an e-contracting process use an online collaboration system that incorporates the functional features discussed above.

18. PROOF OF TIME

18.1 Risk

It may be difficult to prove the time an electronic record was created, sent, or received. Time may be critical if it is necessary to prove that a notice under a contract was given within the designated time period or if it is necessary to establish when a contract was formed. Time may also have a bearing on other evidentiary issues, such as assisting in establishing that a record either was or was not created by a particular person.

There is a risk that computer systems might not record time accurately. The administration of a computer system's clock is at the discretion of the system administrator. A person may intentionally speed up or slow down the system clock. It is also possible for computer system clocks to be inaccurate and there is no guarantee that different computer clocks are synchronised to each other.

Risk Example

Company A is required to give a written notice by 5 pm on a certain day. The contract provides that the time of giving the notice is the time it is received by the recipient.

A sends the relevant notice to B by email at 4.55pm on the specified day. B alleges that the notice was not received until 5.05pm and is therefore not valid. When sending the email A requested a notification of receipt of the email. The notification of receipt was received on A's computer at 4.59pm. The time of receipt was calculated according to the clock on A's computer. B has produced a copy of the email received which shows the time of receipt as 5.05pm (such time being calculated according the clock on B's computer).

It will be for the court to decide whether to rely on the time recorded by A or B's computer clock.

18.2 Resolution

It is recommended that companies synchronise their respective system clocks over a network that can be directly traceable to the Universal Time Code (UTC) before entering into communications where accurate time recording is required.

Where the time of creation or communication of an electronic record may need to be proved with a high degree of certainty it is recommended that digital time stamps be used. A digital time stamp establishes the existence of an electronic record at a particular point of time. Time stamps are created by a time stamping authority (TSA) on records to prove that the record has not been modified since it has been created. The TSA computes the hash code of the electronic record using a standard hash function such as SHA-1 and then attaches the current time, date and identification of the owner to the hash code and signs this compound data. The resulting digital signature is the time stamp. If the parties use digital signatures to timestamp an electronic record then the validity of the record can be proved even if a party's private key is compromised after the record has been signed. The time stamping authority may be either part of the business organisation using the time stamp or a separate trusted third party whose only role is to issue time stamps.

If the record may be of high evidential value in the event of a subsequent dispute between the parties, a trusted third party TSA should be used to issue and verify the time stamp. The trusted time stamping authority will enable fraud to be detected and proved to the court (Buldas et al 2000).

If both parties communicate to each other using the web interface of an online collaboration system then it is likely that the setting of the time in the collaboration system is under the control of the service provider of the system. Accordingly, when the parties communicate with each other by authenticating to the collaboration system, the times that appear on the parties' computers do not influence the time of dispatch and retrieval of the communication. It is the collaboration system time synchronised to the UTC which determines the time of dispatch and receipt of the communication.

19. AUTHENTICATION OF CONTRACTING PARTIES

19.1 Risk

Authentication is the process of verifying the identity of a user of a computer system. Authenticating the user of a computer system may be relevant in various stages of the e-contracting process, for example if it is necessary to establish the identity of the contacting party or of the person who created or communicated an electronic record.

User authentication relies on one or more of the following factors (NOIE 2002):

- **Something the user knows,** such as a password or a personal identification number (PIN). This assumes that only the owner of the account knows the password or PIN needed to access the account.
- **Something the user has,** such as a smart card or token. This assumes that only the owner of the account has the necessary smart card or token needed to unlock the account.
- **Something the user is or does,** such as fingerprints or the voice, retina or iris characteristics of the user or the user's hand written signature (biometrics).

An example of an authentication process is comparing the password entered by a user into the system with the password stored in the system for a given username and comparing the hash code of the entered password with the hash code of the password stored in the computer system.

The most secure methods of authentication involve a combination of two or more of the above factors (e.g. the use of a security token that generates a one time password). Two factor authentication systems are more expensive than one factor authentication systems and a cost-benefit analysis is necessary to determine the required level of user authentication in the context of the relevant organisation and transaction.

Security risks due to a lack of appropriate authentication mechanisms may arise at any stage of an e-contracting process: contract formation, administration or archiving. The authenticity of a record may be difficult to prove in the sense that the purported creator of the record may not be the true creator of the record. For example an email may not have been sent from the email address it appears to have been sent from or a person acting fraudulently may have used another person's email account to send the email. It may also be necessary for the recipient of the email to prove that he or she did not forge the email (McCullagh, Caelli & Little 2001, p8).

Authentication is particularly an issue in relation to emails because an email address may be obtained without proof of identity, emails may be sent from a person's computer without their permission and unencrypted email is relatively insecure (Mallesons 2003).

A purported author of an email can deny authorship of an email sent without their authority under s 15 of the ETA (Cth), s 26 of the ETQA or under the common law (*Grayden* (1988) 36 A Crim R 163; *In re Piranha, Inc* 297 B.R. 78 aff'd, 33 Fed. Appx. 19, 2003 U.S. App. Lexis 24745).

The simple mail transfer protocol (SMTP) (commonly used to transfer emails from one server to another) does not prevent a party from sending an email claiming an identity different from their true identity.

Risk Example

In the risk example referred to in section 17.1 above, instead of the schedule of specifications being provided to the foreman on a disk, it was purportedly emailed to him by Z, an employee of A. Z denies sending the email. The evidence that may be used to show that Z did send the email include evidence that the email originated from a computer which Z was logged into or from Z's email account.

A may challenge the authenticity of the email on the basis that a person with access to Z's email account may have sent the email without Z's authority or a person may have fraudulently made the email appear to have been sent from Z's email account.

Evidence that will be relevant to support the authenticity of the email would be evidence of Z's computer log-on, evidence that Z's password was personal to him and that no one but Z could log on to his personal email account and evidence from the email itself (for example, the syntax may be consistent with Z's writing style).

The court may not believe that Z sent the email if there was contrary evidence, for example, that personal passwords in Z's work area were generally known and occasionally used by others to log on to email accounts, or if A's record keeping system does not include a log of the email.

In the context of administering contracts through an online collaboration system, users need to authenticate to the system using their own username and password. This assures that only the user with that password can log onto the system with the username associated with them. This may not provide secure authentication if the user's password is active for the entire period that the user is registered with the system, as it is possible to carry out dictionary based attacks on the system to recover the password. In addition, if the password has been in use for a long period of time, there is an increased probability that a malicious third party may guess the password.

When contracts and other project documents are communicated over an insecure network such as the Internet, it is essential that the recipient of the documents knows the identity of the sender. The security property by which the receiver confirms the identity of the sender of a document is called data origin authentication. If either the sender's or the receiver's computer system does not have a provision for secure Internet protocols such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS), it is possible for a malicious third party to masquerade as a legitimate sender and send false documents to the receiver so that the receiver assumes that he or she is communicating with someone else. Accordingly, the recipient of the communication must be able to verify that the documents have come from a true source.

19.2 Resolution

It is recommended that when a contract is formed using email, the electronic communications should incorporate appropriate email authentication mechanisms to assure the origin of the email to the receiver of the email. Appropriate mechanisms include: the sender policy framework (SPFP 2007), trusted Email open standard (TEOS) (Schiavone et al 2003) and Yahoo Domain keys (Yahoo).

It is further recommended that where an electronic record is communicated over the Internet, secure Internet protocols such as SSL version 3.0 or TLS version 1.0 be used to establish secure Internet communications. SSL uses digital signatures to validate the sender's server and to ensure that the server is what it claims to be.

Digital certificates are used to help to ensure that a website belongs to the person or entity who claims to be its owner. The SSL protocol uses message authentication codes (MACs) to ensure the data origin authentication of the information exchanged over the Internet. However, SSL does not authenticate the individual user.

In addition to the data origin authentication established by the use of secure Internet Protocols, it may be necessary to authenticate the individual person who has used the computer system to send an electronic record. It is recommended that when choosing the appropriate authentication mechanism the parties assess the level of authentication required. Where a high level of authentication is required a combination of authentication mechanisms (such as a password together with a security token) should be used.

It is recommended that where online collaboration systems relying on password based authentication systems are used for the administration of contracts, password expiry mechanisms should be incorporated into the system. Examples of password expiry mechanisms are automatic password expiry and password history mechanisms that prevent users from choosing recently used passwords. Where a higher degree of authentication is required, it is recommended that Internet Protocol (IP) based authentication be used in addition to password based authentication. In an Internet Protocol based authentication system users can only access online resources though a fixed IP address or range of addresses. This prevents users from using dial-up access or home broadband services to access the company's online resources.

20. DISCLOSURE

20.1 Risk

In the event of litigation arising between the parties to a construction project, they will each be required to make discovery or disclosure to the other party of all relevant documentary evidence in their possession (White 2001, p47). In Queensland, rule 211 of the *Uniform Civil Procedure Rules 1999* (Qld) requires parties to litigation to make disclosure of each document in its possession or under its control that is directly relevant to an issue in the proceeding. For proceedings that take place in the Federal Court, a party may be required to make discovery under Order 15 of the *Federal Court Rules 1979* (Cth). If the parties are involved in arbitration fo their dispute then the disclosure process will depend on what is agreed by the parties (Rowley 2005, p264). The requirements of the disclosure and discovery processes differ in some respects and the parties' obligations may be more onerous where discovery is required. Construction projects generate a vast number of project records. In the event of litigation, these records will need to be analysed so that those records that are relevant to an issue in the dispute can be disclosed. As a result, the process of disclosing relevant documents in the event of a dispute may be unmanageable if the parties use multiple different communication and record keeping methods (White 2001, p46).

Where multiple electronic versions of records are kept on devices such as personal computers, lap tops, home computers, PDAs, removable storage devices, back up media and network systems (Naismith 2003, p188) these records may also be required to disclosed and compliance with disclosure obligations may be time consuming and expensive (White 2001, p46).

Where records have been deleted but are still retrievable from back up media, those records must also be disclosed (Naismith 2003, p188; Givens 2004, p2). Where the back up media has been destroyed in accordance with the party's usual document

retention policy then the record will be unavailable and will not be required to be disclosed (Gorry 1997, p62).

When construction projects are administered electronically, there is a risk that in the event of a dispute, the disclosure process will be costly and time consuming. Parties may have to disclose copies of electronic records which may be stored on a multitude of devices in the possession of any number of employees. Copies of deleted electronic records on back up storage media may also need to be discclosed. There may be no way of clearly identifying and locating all copies of electronic records in order to satisfy the party's disclosure obligations.

Risk Example

Z is the site engineer employed by Company A on a construction project. Z recorded the minutes of a site meeting on her PDA. On returning to her office she copied the minutes to her personal computer and then emailed a copy to Y, another employee of A, who was working on the project from his home office. Y copied the minutes to his personal computer at home. When he finished working that day Y copied the minutes to his flash drive so that he could take them to the site office the next day.

A's computer system was backed up automatically overnight and the backed up data was saved to a storage disk. A's usual procedure is that back up disks are kept for one month and are then reused (copying over the previous data).

In the event of litigation arising in which the minutes are relevant, A will need to disclose all of the copies of the minutes, the copy on Z's PDA, Z's PC, the email server, Y's home PC, Y's flash drive and the back up disk.

If the back up disk has been reused, then A will need to note the back up copy as an unavailable document (one that was once but is no longer in its possession).

20.2 Resolution

It is recommended that in order to reduce the burden of disclosure, organisations in litigation prone industries, such as the construction industry, should have a document retention and destruction policy that has established procedures to delete electronically stored documents from back up media (White 2001, p49).

In addition, where a party is involved in a project where a large number of records are created, it is recommended that the party implement procedures to ensure that multiple versions of electronic records are not made and that electronic records can be easily identified and located. One means of reducing the number of electronic copies is for the parties to use an online collaboration system for the project. If an online collaboration system is used exclusively for the creation and communication of electronic records in relation to the project, then the disclsoure process will be simplified as all relevant records will be kept by the system.

The use of an online collaboration system will simplify the disclosure process because it is difficult to delete or destroy electronic records that are being managed by the system. Every new record created has a new version number and all previous electronic versions of the record are archived automatically by the system. As a result, the electronic records existing at any stage of the project can be easily retrieved.

21. DUTY TO PRESERVE EVIDENCE

21.1 Risk

Parties have an obligation to preserve records they know are relevant to ongoing or potential litigation (Naismith 2003, p186; White 2001, p48). If a person believes that a record may be needed as evidence in a possible future legal proceeding, they cannot legally destroy the record (*R v Ensbey; ex parte A-G (Qld)* [2005] 1 Qd R 159*).* The duty to preserve evidence exists whether or not a legal action has commenced (*British American Tobacco Services Ltd v Cowell* (2002) 7 VR 524).

Parties may be in breach of their duty to preserve evidence if electronic records are not preserved where there is a likelihood of legal proceedings. However, where electronic records are destroyed for the purpose of using storage space more economically, that will not be a breach of the party's duty to preserve evidence (*British American Tobacco Services Ltd v Cowell* (2002) 7 VR 524).

Risk Example

Following on from the previous example, if A becomes aware of a potential dispute that may arise in relation to the project, it has a duty to preserve records it knows are relevant to the potential litigation. This means that it should suspend its usual policy in relation to back up disks so that files on the back up disks that are relevant to the litigation can be recovered.

21.2 Resolution

It is recommended that in order to avoid a breach of an organisation's duty to preserve evidence, the organisation should only destroy electronic records in accordance with a formal document retention and disposal policy. The policy must include procedures to be followed in the event of a dispute arising (Naismith 2003, p187). For example usual disposal practices (including in relation to back up media) should be suspended and electronic records should be backed up at the commencement of litigation.

22. STATUTORY OBLIGATIONS TO MAINTAIN RECORDS

22.1 Risk

If project records are not archived in a manner that ensures that the electronic records remain accessible and which maintains the integrity of the records, the parties may be in breach of their obligations which arise under various State and Commonwealth statutes to maintain records.

Parties are obliged to retain and archive records under various statutory provisions. Where projects are administered electronically, parties may be in breach of these statutory obligations if electronic records are not archived appropriately.

The following Commonwealth and State Acts contain requirements for organisations to retain records:

- The *Limitations of Actions Act 1974* (Qld): in most cases organisations should keep records for at least 6 years to defend or bring proceedings in relation to

breach of contract or possible tort claims. The equivalent Acts in other States and Territories are: *Limitation Act 1985* (ACT); *Limitation Act 1969* (NSW); *Limitation Act* 1981(NT); *Limitation of Actions Act 1936* (SA); *Limitation Act 1974* (Tas); *Limitation of Actions Act 1958* (Vic); *Limitation Act 2005* (WA).

- The *Income Tax Assessment Act 1997* (Cth) requires records to be kept for 5 years and 'to be readily accessible and convertible into writing in the English language'. The Australian Taxation Office has stated that it requires electronic records to be kept 'in such a way that the integrity of the content at capture, storage and reproduction stages can be demonstrated.' (Argy 2006)
- The *Corporations Act 2001* (Cth) requires companies to keep written financial records for 7 years after completion of the transactions covered by the records (s 286). Section 288 of the Act provides that if records are 'kept in electronic form, they must be convertible into hard copy. Hard copy must be made available within a reasonable time.'

The ETA (Cth) and the ETQA provide that where information, documents or communications are required under a law of the Commonwealth or the State to be retained, they can be retained electronically provided certain conditions are met (s 12 ETA (Cth), ss 19-21 ETQA). The main criteria within both of these sections are:

- The information must remain accessible; and
- The method used for storing information must be reliable for maintaining the integrity of the document; i.e. the information has remained complete and unaltered, apart from the addition of any endorsement or any immaterial change.

22.2 Resolution

It is recommended that an organisation review the legislation relevant to it and to the project to ensure that it complies with its record keeping obligations.

To ensure the accessibility and reliability requirements are met the organisations should comply with the archiving recommendations referred to in section 23 of this Report.

23. ACCESS TO RECORDS AFTER PROJECT COMPLETION

23.1 Risk

Parties may require access to project records after completion of the project in order to meet statutory disclosure requirements or in the event of a dispute. In order to ensure that project records are accessible, appropriate archiving procedures need to be followed.

As discussed in section 22 of this Report, the ETA (Cth) and the ETQA provide that where documents or communications are required to be retained they can be retained electronically (s 12 ETA (Cth), ss 20-21 ETQA). The main criteria within these sections are that the records are accessible and maintain their integrity.

The key risks that may impact on the accessibility or integrity of electronic records are first that the storage medium may break down over time, and second that as technology changes it may be impossible to access documents stored on an outdated storage device or using outdated software. For example, older back up tapes using large spooling devices are no longer readable without specialised equipment (White 2001, p46).

Risk Example

Company A administered a construction project electronically using an online collaboration system maintained by B, a third party service provider. At the completion of the project the electronic records of the project were archived by B. Three years after completion of the project, A become involved in a dispute relating to the project. A now seeks access to the records archived by B.

The records were stored by B on a poor quality tape and they have been affected by high levels of humidity in the storage facility. As a result, the records are no longer readable and A cannot access them for the purpose of resolving the dispute.

Risk Example

In the previous example, B also encrypted the records for archiving purposes. When A seeks to access the records, the private secret key which B used to encrypt them is no longer available. In that case it would be impossible to access the plain format of the archived electronic records because the encrypted records cannot be decrypted without B's private secret key.

In addition, if a digital signature is computed on the archived electronic records, then unless B follows an accurate key management plan, it will be difficult to ensure the authenticity and integrity of the electronic records when A seeks to access them.

A further problem may arise where a third party service provider is engaged to maintain the records. In that case, the contracting parties may have difficulty accessing the records after completion of the project if the third party service provider is no longer in business.

Risk Example

Referring back to the previous example, when A seeks to access the records archived by B it discovers that B has since gone out of business due to financial failure. The server on which B stored the records is no longer in existence or is unable to be located.

23.2 Resolution

It is recommended that to ensure that records are appropriately archived, the agreement with any party who is responsible for the archiving of project records should specify the technical standards to be met. Contractual provisions should also specify who is to bear the cost of archiving the data and if the data is required to be accessed, then the procedure for access and the party who is to bear the access costs.

It is also recommended that a copy of the data be provided to each of the contracting parties (for example on a removable storage device) that will be accessible in the event that the service provider is no longer able to provide access to the original records. It is recommended read/writable compact disks (CD R/W) be used to store

electronic records after the completion of the project as they are more resistant to degradation than magnetic tapes and disks.

Additionally, it is important to make sure that only authorised users can access the electronic project documents after the completion of the project. The NAA recommends not encrypting the project documents after the completion of the project (National Archives of Australia 2004). In order to ensure the accessibility of the archived electronic documents, NAA recommends that the electronic records should not be stored in encrypted format as private keys required to decrypt them when it is necessary may become unavailable over time. As well, NAA suggests storing the project documents in an appropriately secure facility together with audit logs, metadata and digital certificate information necessary to establish an evidentiary trail and to provide contextual information. There are well known electronic data storage products such as EMC Centera (EMC 2007) that provide secure access to the documents after the completion of the project. The features of these kinds of products ensure that only authorised users can access the archived electronic documents.

In order to ensure the authenticity, integrity and cryptographic non-repudiation of archived electronic records, it is recommended that electronic records are time stamped using a trusted third party TSA. The TSA maintains a proper key management plan to ensure the authenticity, integrity and cryptographic non-repudiation of the archived electronic records.

24. RECORD KEEPING OBLIGATIONS OF GOVERNMENT AGENCIES

24.1 Risk

Where an organisation is a government agency that party will also need to ensure that it complies with the relevant government's record keeping requirements. For instance, in Queensland, government entities are required to comply with the Queensland Government Recordkeeping Framework ('the Framework'). The Framework includes the *Public Records Act 2002* (Qld) and Queensland Information Standards 31, 40 and 41. The various Commonwealth, State and Territory legislation and guidelines are listed in the table below.

Legislation	**Guidelines**
Archives Act 1983 (Cth)	Designing and Implementing Recordkeeping Systems: A Strategic Approach to Managing Business Information http://www.naa.gov.au/recordkeeping/dirks/dirksman/dirks.html
State Records Act 1998 (NSW)	Government Recordkeeping Manual http://www.records.nsw.gov.au/recordkeeping/government_recordkeeping_manual_3573.asp
Information Act 2002 (NT)	NT Government Records Management Standards http://www.nt.gov.au/dcis/nta/recordkeeping/ntg.html

Public Records Act 1996 (Qld)	Queensland Government Recordkeeping Framework http://www.archives.qld.gov.au/government/framework.asp
State Records Act 1929 (SA)	Adequate Records Management Framework http://www.archives.sa.gov.au/management/index.html
Archives Act 1983 (Tas)	State records guidelines and recordkeeping advices http://www.archives.tas.gov.au/legislative/staterecords
Public Records Act 1973 (Vic)	Public Records Office Victoria, Standards and Advice http://www.prov.vic.gov.au/records/standards.asp
State Records Act 2000 (WA)	State Records Office of WA Recordkeeping Plan 2002 http://www.sro.wa.gov.au/pdfs/SRO-RKS-Introduction.pdf

The Acts generally provide that government agencies must retain government records. However in most cases, records can be destroyed through normal administrative practices. In some jurisdictions government entities can contract with accredited external organisations for the custody of State records.

In Queensland, the *Public Records Act 1996* (Qld) is relevant where one of the parties to the construction project is a government agency. Several mandatory guidelines are also in place under s 25 of the Act. Information Standard 40 (IS40) is a whole-of-government policy for recordkeeping in Queensland. Information Standard 31 (IS31) and Information Standard 41 (IS41) are more specific policy statements on the retention and disposal of public records and managing technology-dependent records.

Section 6 of the Act defines a public record as any information generated or received by an agency within its normal duties. The definition of public record includes copies of records including electronic copies. The explanatory memorandum to the Act explains the scope of public records as follows (Explanatory Notes, Public Records Bill 1996, p6):

> A public record is any form of recorded information that provides evidence of the decisions or actions of a public authority in undertaking its business activities or in the conduct of its affairs. The Bill includes all records irrespective of the form, the custodial arrangements and the technology used to generate, manage, preserve and access records.
>
> Copies of a public record and copies of part of a public record are also regarded as public records. A copy of a record means any reproduction of a record in any form. For example, a photocopy of a paper document, a transcript of a sound recording or a duplicate copy of an image are regarded as copies of a record.

Accordingly, any records created or received by a government agency relating to a construction project will be public records to which the Act applies. This may lead to conceptual difficulties where the records for the project are maintained by a party

other than the government agency. For instance, where an online collaboration system is used, when a record is 'sent' to a government agency, the original record will become a public record. This is because the collaboration system will simply allow the agency to view the original record rather than sending a copy of the record to the agency.. No copy of the record is made. As a result the agency will then have an obligation to comply with the Act in relation to that record.

Section 7(1) requires public authorities to keep full and accurate records of its activities which must comply with the relevant standards and guidelines.

Section 8 requires an agency to ensure the safe custody and preservation of records in its possession. Section 8 provides:

> (1) A public authority is responsible for ensuring the safe custody and preservation of records in its possession.
>
> (2) Without limiting subsection (1), an arrangement between a public authority and another person for the person to have custody of a record of the public authority must include arrangements for the safe keeping, proper preservation and return of the record.

While it is not clear from the wording of s 8 whether it enables agencies to contract out their record keeping obligations, the explanatory memorandum refers to outsourcing record keeping obligations. (Explanatory Notes, Public Records Bill 1996, p5) Accordingly, it appears that agencies can use third parties to maintain public records.

Section 13 provides that a person may not dispose of public records unless those records are disposed of under the authority of the Archivist or the Public Records Review Committee or other legal authority (such as an Act), justification or excuse. Under IS31, public authorities must develop and implement formal disposal schedules authorised by the State Archivist and implement disposal processes, to ensure the legal, systematic, consistent and disposal of records no longer required for business, accountability or cultural purposes.

Information Standard 40 requires government agencies to comply with legal, administrative, cultural and business recordkeeping requirements through reliable recordkeeping systems that ensure that full and accurate records of Government business is adequately documented, preserved and made accessible.

IS40 provides seven mandatory principles that agencies must comply with to ensure accountable recordkeeping and the implementation and management of reliable recordkeeping systems. The seven principles require that recordkeeping must be:

- Compliant and accountable. Agencies must comply with public records legislation and other legal and administrative requirements for managing records.
- Monitored and audited. Recordkeeping systems, procedures and practices must be periodically monitored, revised, evaluated and audited to ensure compliance with cultural, business, legislative and accountability requirements.
- Assigned and implemented. Recordkeeping activities must be formally assigned to and implemented by those involved in the conduct of Government business.

- Managed. Recordkeeping must be managed through an identifiable recordkeeping program and managed by appropriately trained staff.
- Reliable and secure. Recordkeeping systems, procedures and practices must work reliably to ensure that records are credible and authoritative. Recordkeeping systems must be secure from unauthorised access, damage and misuse.
- Systematic and comprehensive. Records must be created, maintained and managed systematically. Recordkeeping functionality must be designed and implemented into all business systems that create, store or manage records. All recordkeeping systems must have accurately documented policies and assigned responsibilities. Records need to document the complete range of business undertaken by an agency.
- Full and accurate. Full and accurate records must be made and kept for as long as they are required for business, legislative, accountability and cultural purposes.

IS31 sets out specific policy guidelines for the retention and the disposal of public records. Public records must be retained by agencies for as long as they are needed to meet business needs, the requirements of organisational activities and community expectations. Records that are deemed to be of value must be identified and retained in a useable form for an appropriate length of time. Disposal of records must be authorised and managed in accordance with environmental and security requirements. IS31 mandates two principles that must be complied with by government agencies:

- **Appraisal and retention.** Each agency is accountable for the creation, management, appraisal and retention of records. Records must be appraised and retained according to their legal, business, administrative, information and historical value and other criteria relevant to the record or related business activity.
- **Disposal authorisation and management.** The disposal of records can only be performed with the written authorisation of the State Archivist. Agencies must develop and implement formal disposal schedules authorised by the State Archivist and implement disposal processes, to ensure the legal, systematic, consistent and disposal of records that are no longer required. Agencies must ensure that records are secure and cannot be altered or deleted without appropriate authority. Privacy and confidentiality requirements must be in accordance with Queensland government policy.

Under IS41 it is clear that an electronic record that is a public record must be maintained in accordance with the Queensland Government Recordkeeping Framework. IS41 provides:

> Technology-dependent records generated or received in the course of Government business are public records and must be created, maintained and accessible for as long as they are required to meet legislative, accountability, business and cultural obligations.

Technology-dependent records must still comply with the same recordkeeping requirements of paper records. IS41 contains ten mandatory principles which highlight the increased evidentiary difficulties inherent in the use of technology-dependent records. The requirements include:

- **Full and Accurate Records.** Technology-dependent records have the same stature of paper public records and must be managed in accordance with existing guidelines.
- **Evidential Integrity of Technology-Dependent Records.** The evidential integrity of technology-dependent records must be preserved across successive technological systems in accordance with cultural, legislative, business and accountability requirements.
- **Integrated Management of Records.** The management of all technology-dependent records must be integrated within each public authority's recordkeeping strategy and program.
- **Accessible and Useable Technology-Dependent Records.** Technology-dependent records must be accessible in a useable and meaningful form, irrespective of the origin, location or format of those records.
- **Representation of Technology-Dependent Records.** Technology-dependent records must be maintained in their original representation or form.
- **Responsibility.** Recordkeeping in the electronic environment is a responsibility shared by all public sector employees, officials, contractors and other personnel undertaking business activities on the behalf of public authorities.
- **Recordkeeping Functionality.** Recordkeeping functionality must be designed and implemented into all business information systems in which records are made and maintained.
- **Scope.** Electronic recordkeeping must be incorporated into all government business activities conducted in the electronic environment, including electronic service delivery activities.
- **Structure.** The structure of electronic records must be documented.
- **Augmentation.** Electronic records must be able to be augmented or amended without disturbing the evidential integrity of each record.

The Queensland State Archives *Digitisation Disposal Policy, 2006* (Queensland Government, 2006), sets out the conditions under which the Queensland State Archivist will authorise the early disposal of original paper records. The agency will need to seek approval from the State Archivist to dispose of original paper records after digitisation. Authorisation is given by the State Archivist though amendment to the agency's Retention and Disposal Schedule. Authorisation is given at an agency level, specific authorisation is not required for each paper record to be destroyed after digitisation.

Where one of the contracting parties is a government agency there is a risk that it may be in breach of its statutory obligation to retain public records. If a third party service provider is responsible for the maintenance of the project database, the agency must make arrangements for the safe keeping, proper preservation and return of the records.

When a construction project is administered electronically using a collaboration system, there is a risk that if one of the parties is a government agency, all records which are 'sent' to the agency using the system will become public records. This is because the system does not send the agency a copy, but instead makes the original electronic record available for the government agency to view.

Where public records are digitised, then if the government agency destroys the original paper records there is a risk that the agency may be in breach its statutory obligation to retain records.

Risk Example

Company A has entered into a joint venture agreement with a Queensland State government agency, Agency B. A wishes to use an online collaboration system provided by a third party service provider, Company C, to electronically administer the project. If the online collaboration system is used, all of the records relating to the project will be stored electronically on a server owned by C. It is envisaged that no paper records will be created in relation to the administration of the project.

B has an obligation under the *Public Records Act 1996* (Qld) to ensure the safe custody and preservation of records in its possession. It appears the agency can contract out this obligation to the third party C. However, the agency will have to make arrangements with C for the safe keeping, proper preservation and return of the record.

C will have to comply with the *Public Records Act 1996* (Qld) and the Queensland Government Recordkeeping Framework in relation to the records relating to the project and any records that have been created or sent to the agency will have to be returned to the agency at the completion of the project. In addition to the technical record keeping requirements, this means that any record that has been 'sent' to the agency cannot be deleted except in accordance with formal disposal schedules authorised by the State Archivist.

24.2 Resolution

Where one of the parties to the project is a Queensland government agency the organisation responsible for maintaining the electronic records relating to the project must comply with the Queensland Government Recordkeeping Framework including the agency's own Retention and Disposal Schedule. As the government agency will remain responsible under the *Public Records Act 1996* (Qld) for the retention of the records, it may be reluctant to delegate responsibility for the electronic administration of the project to a third party service provider. It is recommended that government agencies assess whether an e-contracting system used to administer a project complies with all aspects of the agency's recordkeeping obligations.

It is recommended that where a government agency archives records relating to a project electronically, in order to ensure the accessibility of the archived electronic records, the records should not be stored in encrypted format as private keys required to decrypt them may become unavailable over time (National Archives of Australia 2004). The plain (unencrypted) electronic records should be stored in an appropriately secure facility together with audit logs, metadata and digital certificate information necessary to establish an evidentiary trail and to provide contextual information.

It is further recommended that where a government agency wishes to digitise paper records, it must only dispose of the original paper records in accordance with an authorisation of the State Archivist.

PART C: RECOMMENDED E-CONTRACTING SYSTEM

25. RECOMMENDED SECURITY FEATURES OF AN E-CONTRACTING SYSTEM

As discussed in section 2.4 of this Report it is essential that online collaboration systems used for e-contracting in the construction industry achieve the information security goals of confidentiality, integrity, authenticity and cryptographic non-repudiation, in a strong sense during different stages of the contracting life cycle. However, it appears that the online collaboration systems that are currently available may not achieve all of these information security goals. It is also unclear what cryptographic protocols these systems employ during the various stages of an e-contracting process.

Accordingly, it is recommended that a number of security and functional features must be present in an online collaboration system if the system is to be used by construction industry participants for e-contracting purposes. The recommendations outlined below ensure that the security goals of an e-contracting system are achieved in a strong sense, as opposed to the weaker forms of security provided by most of the systems that are currently available. The following security and functional features are recommended:

- Construction companies that need to carry out their construction project tasks must register to the collaboration system by subscribing to the ASP for a certain period of time by paying a subscription fee.
- All messages are transmitted over a communication channel secured by the TLS version 1 or TLS version 1.1 protocols or a similar secure protocol.
- Authorised employees are given permissions to access the collaboration system using a 2-form authentication mechanism, such as a username and a security token which generates a one-time password.
- A role-based access control policy is implemented throughout the system. This ensures that depending on the roles of the personnel, access rights to several documents will be assigned.
- Authorised personnel can access the collaboration system using their credentials at any time.
- The collaboration system is provided with a range of Internet Protocol (IP) addresses that perform location verification of the system enforcing the LBAC security policy. Only the company's system administrator is allowed to assign a range of IP addresses for collaboration systems used by the authorised personnel in the company.
- A strong form of cryptographic non-repudiation is ensured by computing digital signatures for every new electronic record formed using the system.
- Timestamping of the digital signatures of the project documents after the completion of the project provides true cryptographic non-repudiation and later demonstrates that the digital signatures were valid at the time of timestamping.
- Whichever company is intended to carry out the e-contracting using the collaboration system must register to the system by paying the subscription fee for a period of time.

PART D: CONCLUSION

26. RECOMMENDATIONS AND CONCLUSIONS

The use of ICT in the construction industry can lead to considerable efficiencies in the administration of projects and is extensively used as a means of managing and recording construction projects. The use of collaboration systems is an effective means to facilitate communications between diverse parties to construction contracts who are often geographically distant and who assume different roles at various stages of the project. However, the use of ICT in the construction industry leads to uncertainties which may have serious practical consequences for contracting parties if they remain unresolved. These uncertainties may also contribute to a reduced willingness by business to take advantage of modern communication technologies.

This Report has identified the legal and security risks that may arise when construction contracts are formed, administered and recorded within an electronic environment and has recommended steps that parties may take to resolve or minimise these risks. A high level summary of the risks and recommendations is set out in the table on the following pages.

Summary of Risks and Recommendations in this Report

Identified Risks	Recommendations
It may be difficult to establish the precise point in time that an electronic construction contract has been formed.	The only way to avoid the legal uncertainties surrounding the time of electronic contract formation is to incorporate clear provisions in the contract that state how acceptance is to be communicated and when acceptance of the offer will be deemed to be effective.
	Appropriate technical mechanisms (as discussed further below) should be adopted for secure time recording.
It may be difficult to establish the place where an electronic construction contract has been formed.	A construction contract should include clear provisions where the parties submit to the jurisdiction of the courts of a particular place and agree to the applicable law to govern the contract. The place of contract formation will then have minimal legal relevance.
The authority of an individual to enter into a construction contract on behalf of another person or entity may be uncertain.	Regardless of whether a construction contract is formed by paper or electronic communications, the parties must still carry out their usual due diligence investigations to ensure that the individuals who are entering into the contract on behalf of another person or organisation, possess the actual or apparent authority to enter into the contract.
Electronic communications may not satisfy statutory requirements for guarantees to be in writing and signed.	As a consequence of the legal uncertainties surrounding the validity of electronic signatures, to avoid the risk that a guarantee may be unenforceable all guarantees should continue to be entered into in paper form and be physically signed using handwritten signatures.
Depending on the terms of a construction contract, it may be uncertain whether electronic communications are effective to amend the contract and the validity of electronic notices may be unclear.	Contracting parties must expressly address electronic communications in their contract documents. The provisions must be clear as to which communications under the contract may and may not take place in electronic form.
	If the contracting parties do not wish to be bound by electronic communications, then the contract should clearly exclude electronic communications as a valid form of notice delivery.
	If the contracting parties do wish to utilise electronic communications, they should consider whether they wish to contractually avail themselves of effective electronic communications for some, but not all contractual notices. The communications that are to remain paper based should be clearly excluded by appropriate provisions.
	The electronic communication method to be used should be identified and the relevant electronic addresses and details of authorised recipients should be stated.
	If electronic communications are to be used, the parties should expressly consent to the use of electronic communications, but only to the extent specified in the contract.
	The contract should include a timing provision to govern when electronic communications will be deemed to have been received by the parties. The nature of the provision will depend on the electronic communication method being used and the commercial

Identified Risks	Recommendations
	acceptability of the proposed provision to both contract parties.
	The contract should deem those notices and communications that the contract allows to be delivered by electronic means, to be in writing and signed. In relation to electronic signatures, the contract should identify the precise signature method to be used, the parties should consent to the use of that method and acknowledge that they consider the method to be both reliable and appropriate.
	If an online collaboration system is used for electronic communications, the parties should include a contractual provision setting out alternative communication protocols to be followed in the event that the system becomes unavailable.
A construction project may be disrupted if the collaboration system used for administration of the project is unavailable for any length of time.	The contract with the service provider of the collaboration system should include provisions regarding disruptions to the system.
	Users of the collaboration system should consider taking out business interruption insurance that covers them in the event the collaboration system is unavailable.
If parties to a construction project use incompatible technology there may be difficulty ensuring consistency between the electronic records available to each party.	Users of collaboration systems should use the same version of the system and, if necessary, the same operating system to run the system.
	Where ICT is used to carry out e-contracting the parties should follow the best practice standards recommended by ITIL.
The rights and obligations of the service provider of ICT used to administer a construction project may be uncertain.	The service provider should enter into a contract with all of the proposed users of the ICT which make clear the rights and obligations of the service provider.
The electronic administration of a construction project may lead to disputes between the parties, for example the ease of copying and transmitting electronic records may lead to increased breaches of confidence or intellectual property disputes.	The contract between the project participants should contain specific provisions relating to the electronic administration of the project.
The intellectual property in project drawings may be more easily infringed in an electronic environment due to the ease with which copies of the drawings can be made and shared.	Designers should take practical steps to protect their copyright in drawings including incorporation of a copyright statement, the designer's name and logo and a watermark on all drawings.
If project drawings are amended extensively by online collaboration, the ownership of the copyright in the drawings may no longer rest with the original designer.	The contract between the parties should specifically deal with the ownership of copyright in the project drawings and should specify that these copyright provisions continue to apply regardless of the extent of any collaboration between the parties in the development of the drawings.
The confidentiality of electronic project records may be compromised during their	The contract between the project participants and the contract with the ICT service provider should include a specific duty of

Identified Risks	Recommendations
retention or communication.	confidentiality.
	The SSL protocol (or newer versions of it) should be used whenever electronic records are communicated from one computer to another.
	Where the parties use a collaboration system to administer the project, the system should use role-based access controls, and authentication mechanisms (such as passwords and IP controls) to ensure that only authorised persons can access the project database.
Electronic records may be inadmissible as evidence in the event of a dispute if they are considered to be hearsay (i.e. they contain a statement by a human and are relied upon as evidence of the truth of such statement).	Electronic records that may be of importance in the event of a dispute relating to the construction project should be created and maintained as part of the business record of the contracting party. Electronic records created by an administration system used for the administration of the project will be likely to be admissible as business records.
	The agreement between the contracting parties should include a provision deeming electronic records maintained by the agreed administration system to be admissible as evidence and prima facie accurate.
A digitised copy of a paper record may be inadmissible if the party relying on it cannot satisfy the court that it is an accurate copy of the electronic record.	Parties must implement procedures to ensure that they can demonstrate the authenticity, integrity and reliability of a digitised copy of a paper record. These procedures include ensuring the accuracy of the scanner, recording details of the person responsible for scanning the record and time stamping of the digitised record.
A paper copy of an electronic record may be inadmissible if the party seeking to rely on it as evidence cannot satisfy the court that the paper record is an accurate copy of the electronic record, for example because it does not contain all of the meta-data associated with the electronic record.	When an electronic record is printed, parties should not delete the electronic record but should retain it in case it is needed as evidence in the event of a dispute.
An electronic record may be considered by a court to be unreliable as evidence if the parties cannot prove the integrity of the record (i.e. that it has not be altered by human intervention or corrupted by computer malfunction).	All electronic communications in relation to a construction project should utilise the SSL protocol (or newer versions of it) to ensure the integrity of the communication.
	If an electronic record is likely to be of evidential importance then the electronic record should be signed using digital signature technology.
	Where the electronic record is of very high evidential importance the record should also be time stamped so that the integrity of the record can be assured even if the digital signature becomes invalid.
	Where a collaboration system is used for the administration of a project the logging and auditing features of the system will assist in

Identified Risks	Recommendations
	establishing the integrity of electronic records maintained by the system.
The parties may be unable to prove the time an electronic record was created communicated. Establishing time may be of importance in relation to the time a contract was formed or the time a notice was sent under a contract. Time may also be of assistance in establishing or challenging the integrity or authenticity of an electronic record.	Parties involved in e-contracting should synchronise their computer system clocks to the Universal Time Code.
	Where the time of creation or communication of an electronic record is highly important, the record should be signed with a digital time stamp and if necessary a trusted third party time stamping authority should be used to issue and verify the time stamp.
	Where a collaboration system is used, the time of creation or communication of an electronic record will be established by the system and synchronisation of system computer clocks is not necessary.
An electronic record may be considered by a court to be unreliable as evidence if the parties cannot prove the record was created or communicated by the person who is alleged to have created or communicated it. • A party who receives an electronic communication must be able to verify that the communication has come from the source from which it is purported to have been sent. • Password based authentication mechanisms may not be reliable because they may be subject to dictionary based attacks, or they may be disclosed by human carelessness.	Where electronic communications which take place using email are of high evidential importance they should incorporate email authentication mechanisms (such as the sender policy framework, trusted email open standard and Yahoo domain keys) to assure the origin of the email.
	Where an electronic record is communicated over the Internet, secure Internet protocols such as SSL or TLS should be used to ensure data origin authentication.
	An authentication mechanism appropriate for the degree of certainty in authentication required for the particular communication should be used. Where a high level of authentication is required a combination of authentication mechanisms (such as a password together with a security token) should be used.
	Where an online collaboration system relying on password based authentication is used, password expiry mechanisms should be incorporated into the system. Where a high degree of authentication is required, Internet Protocol based authentication systems should also be used.
The disclosure process in the event of a dispute may be costly and time consuming if there is a multitude of electronic copies of records held on a range of electronic devices. There may be no way of clearly identifying and locating all copies of electronic records in order to satisfy the party's disclosure obligations in a timely and cost effective manner.	Parties in the construction industry should have a document retention and destruction policy to ensure that electronic records can be easily identified and located. The use of an online collaboration system will meet this requirement because it automatically logs all iterations of electronic records created using the system.
	Where a collaboration system is used then the parties should not use other electronic systems for the creation or communication or electronic records as doing so will complicate the disclosure process.
	The document retention and destruction policy should include established procedures to delete electronically stored records from

Identified Risks	Recommendations
	back up media.
If a party to a construction project destroys project records after it becomes aware of potential litigation in relation to the project it may be in breach of its duty to preserve evidence.	An organisation should only destroy electronic records in accordance with a formal document retention and disposal policy which should include procedures to be followed in the event of a dispute arising.
If project records are not archived in a manner that ensures that they remain accessible and that maintains the integrity of the records, the parties may be in breach of their statutory obligations to maintain records.	Organisations should review any legislation relevant to the organisation and to the project to ensure that it complies with its statutory record keeping obligations. In particular, to ensure the accessibility and reliability requirements of electronic record keeping are satisfied, organisations should comply with the specific archiving recommendations referred to below.
Where project records are archived electronically, there is a risk that they may not remain accessible or their integrity may not be assured if the storage media on which they are kept breaks down over time or if technology changes mean that it is no longer possible to access the records.	The agreement with any party who is responsible for the archiving of project records should specify the technical standards to be met by the service provider in archiving the data. Contractual provisions should also specify who is to bear the cost of archiving the data and, if the data is required to be accessed, the access procedure and the party who is to bear the access costs.
	Ideally, archived records should not be stored in encrypted format unless they are time stamped by a trusted third party time stamping authority.
Where a third party is responsible for the archiving of electronic project records, parties may not be able to obtain access to the records if the third party service provider is no longer in business.	A copy of the project data should be provided to each of the contracting parties on CD R/W disks.
Where one of the contracting parties is a government agency the agency must comply with its statutory obligation to retain public records. If a third party service provider is responsible for the maintenance of the project database, the agency must make arrangements for the safe keeping, proper preservation and return of the records.	A government agency using an e-contracting system to administer a construction project should assess whether or not the administration system used complies with the agency's record-keeping obligations under the Queensland Government Recordkeeping Framework.
	Where a third party service provider maintains the project database, the project records must be returned to the government agency. The Queensland Government Recordkeeping Framework does not make a distinction between the original electronic records and a copy of the electronic records.
	Archived records should not be stored in encrypted format but should be stored in a secure facility together with audit logs, metadata and digital certificate information.
When a collaboration system is used to administer a construction project, there is a	It is uncertain what steps a government agency must take in order to comply with the Queensland Government Recordkeeping Framework when a collaboration system is used. It is

Identified Risks	Recommendations
risk that if one of the parties is a government agency, all records which are 'sent' to the agency using the system will become public records.	recommended that clarification be sought from the State Archivist prior to a government agency agreeing to the use of a collaboration system for the administration of a construction project.
When public records are digitised, the government agency must comply with its statutory record keeping obligations in relation to the original paper records.	Where a government agency digitises paper records, it must only dispose of the original paper records in accordance with an authorisation of the State Archivist.

REFERENCES

Argy, P., 2006, 'Electronic Evidence, Document Retention and Privacy', available at http://www.mallesons.com/search-hithighlight.cfm?hitURL=/publications/2006/Mar/8367966w.htm&keyword=electronic%20evidence (accessed 3 May 2006).

Australian Law Reform Commission (ALRC), 2005, *ALRC Discussion Paper 69 – Review of the Uniform Evidence Acts*, available at http://www.austlii.edu.au/au/other/alrc/publications/dp/69/ (accessed 1 March 2006).

Beale, H. & Griffiths, L., 2002, 'Electronic Commerce: Formal Requirements in Commercial Transactions', *Lloyd's Maritime and Commercial Law Quarterly*, 2002, part 4, p. 467.

Berning, P.W. & Diveley-Coyne, S., 2000, 'E-Commerce and the Construction Industry: The Revolution Is Here', available at http://www.constructionweblinks.com/Resources/Industry_Reports__Newsletters/Oct_2_2000/e-commerce.htm (accessed on15 December 2005).

Briggs I. & Brumpton, S., 2001, 'Embrace E-Construction With Care!', *Australian Construction Law Bulletin*, vol.13, no.4, p. 25.

Casamassima, T.J. & Caplicki, E.V., 2003, 'Electronic Evidence at Trial: The Admissibility of Project Records, E-Mail and Internet Websites', *The Construction Lawyer*, vol.23, no.3, p. 13.

Chan, S., and Leung, N., 2004, 'Prototype web-based construction project management system', *Journal of Construction Engineering and Management*, p. 935.

Christensen, S., 2001, 'Formation of Contracts by Email – Is it Just the Same as the Post', *Queensland University of Technology Law & Justice Journal*, vol.1, no. 1, p. 22.

Christensen, S., Duncan, W. & Low, R., 2003, 'The Statute of Frauds in the Digital Age – Maintaining the Integrity of Signatures', *E Law – Murdoch University Electronic Journal of Law* vol.10, no. 4, available at http://www.murdoch.edu.au/elaw/issues/v10n4/christensen104.html (accessed 5 December 2005).

Christensen, S., Duncan, W. and Low, R., 2002. 'Moving Queensland Property Transactions to the Digital Age: Can Writing and Signature Requirements be Fulfilled Electronically?', available at http://www.law.qut.edu.au/files/digital.pdf (accessed 6 December 2005).

Davidson, A., 2004, 'Signatures on Electronic Documents', *Proctor*, vol.24, no.7, p. 29.

De Zilva, A., 2003, 'Electronic Transactions Legislation: An Australian Perspective', *The International Lawyer*, vol.37, no.4, p.1009.

Department of Public Works and Services New South Wales, 2000, *Risk Management in Electronic Procurement*, available at http://www.cpsc.nsw.gov.au/e-procurement/docs/Risk-Chapter2.pdf (accessed 29 April 2007).

Dierks, T. & C. Allen, 1999. 'The TLS Protocol Version 1.0. Network Working Group, Request for Comments (RFC 2246)', *Standards Track*, available at http://www.ietf.org/rfc/rfc2246.txt (accessed 18 April 2007).

Dierks, T. & Rescorla, E., 2006. 'The Transport Layer Security (TLS) Protocol Version 1.1. Network Working Group, Request for Comments (RFC 4346)', *Standards Track*, available at http://www.ietf.org/rfc/rfc2246.txt (accessed 18 April 2007).

EMC, 2007, 'EMC Centera', available at http://www.emc.com/products/systems/centera.jsp (accessed 23 May 2007).

Forbes, J.R.S., 2004, *Evidence Law in Queensland* (5th ed), Thomson, Sydney.

Freier, A. O., Karlton, P. & Kocher, P. C., 1996, *The SSL Protocol - Version 3.0 Internet Draft*, Transport Layer Security Working Group, available at http://wp.netscape.com/eng/ssl3/ssl-toc.html (accessed 18 April 2007).

Garfinkel, S., Margrave, D., Schiller, J., Nordlander E., & Miller, R., 2005. 'How to Make Secure Email Easier to Use', *CHI:2005: Technology, Safety and Community*, Portland, Oregon, April 2-7, 2005, available at http://www.simson.net/ref/2004/chi2005_smime_submitted.pdf (accessed 17 April 2007).

Giles, D., 2000, 'You've Got Mail…Or Have You?', *Internet Law Bulletin*, vol.3, no.1, p. 12.

Givens, J.S., 2003/2004, 'The Admissibility of Electronic Evidence At Trial: Courtroom Admissibility Standards', Cumberland Law Review, vol.34, no1, p. 95.

Gorry, S., 1997, 'Electronic Records and the Evidence Act', *Australian Company Secretary*, vol.49, no.2, p. 60.

Halsbury, H.S.G.,1991, *Halsbury's Laws of Australia*, Butterworths, Sydney.

Hill, S.W.B., 2001, 'Email Contracts – When is the Contract Formed?', *Journal of Law and Information Science*, vol.12, no.1, p. 46.

Hill, S.W.B., 2001, 'Flogging A Dead Horse – The Postal Acceptance Rule and Email', *Journal of Contract Law*, vol.17, no.2, p. 151.

Hill, S.W.B., 2002, 'Formation of Contracts Via Email – When and Where?', *Commercial Law Quarterly*, vol.16, no.1, p. 3.

Kangas, E., 2004. 'The Case for Email Security', Published as a *Lux Scientiae Article*, available at http://luxsci.com/extranet/articles/email-security.html (accessed 1 May 2007).

Knorr, K., & Rohrig, S., 2001, 'Security Requirements of E-business Processes', *I3E*, p. 73.

Laryea, E. T., 1999, 'The Evidential Status of Electronic Data', *National Law Review,* Issue 3, p. 6.

Lawrence, A., 2000, 'Fundamental Issues For Electronic Transactions: the Value of Authentication', *Internet Law Bulletin*, vol.3, no.6, p. 85.

Mallesons, 2003, 'Email and Contractual Notices', available at http://www.mallesons.com/search-hithighlight.cfm?hitURL=/publications/Asian_Projects_and_Construction_Update/6497970W.htm&keyword=electronic%20transactions%20act (accessed 4 May 2006).

McCullagh, A., Caelli, W. & Little, P., 2001, 'Signature Stripping: A Digital Dilemma', The Journal of Information, Law and Technology, Issue No1, available at http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_1/mccullagh/ (accessed 5 June 2006).

Naismith, P.G., 2003, 'The Discovery of Electronic Evidence', *Journal of Judicial Administration*, vol.12, no.4, p. 180.

National Archives of Australia, 2004, *Digital Recordkeeping – Guidelines for Creating, Managing and Preserving Digital Records (Exposure Draft May 2004)*, available at http://www.naa.gov.au/recordkeeping/er/guidelines/DigitalRecordkeeping.pdf (accessed 19 December 2005).

National Archives of Australia,(2004). Recordkeeping and Online Security Processes: Guidelines for Managing Commonwealth Records Created or Received using Authentication and Encryption, available at http://www.naa.gov.au/recordkeeping/er/security.html (accessed 12 May 2007).

National Office for the Information Economy, 2002, *National Electronic Authentication Council Report on Liability and Other Legal Issues in the Use of PKI Digital Certificates*.

Nikolich, M., 2003, 'The Legality of E-mail Messages', *Australian Construction Law Newsletter*, vol.91, p. 27.

Nitithamyong, P., & Skibniewski, M., 2006, 'Success/Failure Factors and Performance Measures of Web-based Construction Project Management Systems: Professional's Viewpoint.' *Journal of Construction Engineering and Management*, January, p 80.

O'Shea, K. & Skeahan, K., 1997, 'Acceptance of Offers by E-Mail – How Far Should the Postal Acceptance Rule Extend?', *Queensland University of Technology Law Journal*, vol.13, p. 247.

Queensland Government, 2006, 'Information Standard 40', available at http://www.governmentict.qld.gov.au/02_infostand/standards/is40.htm (accessed 29 April 2007).

Queensland Government, 2004, 'Information Standard 31', available at http://www.governmentict.qld.gov.au/02_infostand/standards/is31.htm (accessed 30 April 2007).

Queensland Government, 2005, 'Information Standard 41', available at http://www.governmentict.qld.gov.au/02_infostand/standards/is41.htm (accessed 30 April 2007).

Queensland Government, 2006, 'Digitisation Disposal Policy', available at http://www.archives.qld.gov.au/government/ddp.asp (accessed 30 April 2007).

Reed, C., 2001, 'Legally Binding Electronic Documents: Digital Signatures and Authentication', The International Lawyer, vol.35, no.1, p. 89.

Reynolds, P., 1994, Admissibility of computer-produced documents as evidence, *Computer Law and Practice,* Volume 10, p. 118.

Robins, M.D., 2003, 'Evidence at the Electronic Frontier: Introducing Email at Trial in Commercial Litigation', vol.29, no.2, p. 219.

Rohrig, S., & Knorr, K., 2004, 'Security Analysis of Electronic Business Processes'. *Electronic Commerce Research*, vol. 4, nos. 1-2, p. 59.

Rowley, J. W., 2005, 'Agreement to arbitrate: Getting it right', *Building and Construction Law Journal*, vol. 21, iss. 4, p.260.

Schiavone, V., Brussin, D., Koenig, J., Cobb S. & Everett-Church, R., 2003, 'Trusted Email Open Standard. A Comprehensive Policy and Technology Proposal for Email Reform. *An e-privacy group white paper',* available at http://www.ftc.gov/bcp/workshops/spam/Supplements/eprivacygp.pdf (accessed 5 April 2007).

Sender Policy Framework Project (SPFP), 2007, 'Sender Policy Framework' available at www.openspf.org (accessed: 5 April 2007).

Sheridan, N. & Rigotti, M., 2001, 'Contract Formation and Electronic Signatures Under the Electronic Transactions Act', *Journal of Banking and Finance Law and Practice*, vol.12, no.1, p. 47.

Spenceley, C., 2003, 'Evidentiary Treatment of Computer-Produced Material: A Reliability Based Evaluation', *Thesis*, University of Sydney.

Standards Australia, 2003, *Guidelines for the Management of IT Evidence*, HB 171-2003, Sydney, 15 December 2005.

Thomson, J., 2003, 'Has the New State Electronic Transactions Act Solved All Our Problems?', *Brief*, vol.20, no.11, 26.

Walsh, N., 1998, *A Technical Introduction to XML*, available at http://www.xml.com/pub/a/98/10/guide0.html (accessed 10 May 2006).

White, S., 2001, 'Discovery of Electronic Documents', *Computers & Law*, vol.44, p. 46.

Wilkinson, P., 2005, *Construction Collaboration Technologies: The Extranet Revolution*, Taylor & Francis, London; New York.

Willmott, L. Christensen, S. and Butler, D. 2005, *Contract Law*, Oxford University Press, Melbourne, Australia.

Wolfson, A., 2005, '"Electronic Fingerprints": Doing Away with the Conception of Computer-Generated Records as Hearsay', *Michigan Law Review*, vol.104, no.1, p. 151.

AUTHOR BIOGRAPHIES

Professor Ed Dawson
Information Security Institute
Faculty of Information Technology
Queensland University of Technology
Ph +61 7 3864 9551, Fax +61 7 3864 1801, email e.dawson@qut.edu.au

Professor Dawson is the Research Director of the Information Security Institute. He has research experience in many aspects of cryptology. He has published over 200 research papers in various aspects of cryptology. He has extensive research experience in the applications of cryptology, especially to e-commerce.

Professor Sharon Christensen, LL.B.(Hons)(QIT), LL.M.(QUT), Solicitor, Queensland
School of Law
Queensland University of Technology
Ph +61 7 3864 5204, fax +61 7 3864 2121, email s.christensen@qut.edu.au

Professor Christensen is the Gadens Professor in Property Law at the Queensland University of Technology. She has written and lectured in Land Contracts and Contract and has research interests in contract, property law and electronic transactions. She is a specialist consultant at Gadens Lawyers, Brisbane and a Deputy Director of the Information Security Institute.

Professor William Duncan, LL.B.(Qld), LL.M.(Lond.), Solicitor, Queensland
School of Law
Queensland University of Technology
Ph +61 7 3864 2709, fax +61 7 3864 1161, email w.duncan@qut.edu.au

Professor Duncan is a Professor of Law at the Queensland University of Technology and consultant to Allens Arthur Robinson, Brisbane. He has written and lectured extensively in the subjects of property law, land contracts and allied subjects in tertiary institutions in Queensland and to the legal profession since 1973.

Ms Kathryn O'Shea LL.B.(Hons)(QUT), Solicitor, Queensland
School of Law
Queensland University of Technology
Ph +61 7 3864 5207, fax +61 7 3864 2121, email k.oshea@qut.edu.au

Ms O'Shea is an Associate Lecturer in the School of Law of the Queensland University of Technology. Prior to joining the university in 2005, she worked for an extensive period of time as a solicitor in private practice in the corporate and commercial areas. She has practised in national and international firms in both Brisbane and London. Her current research interests include electronic transactions, contract law and consumer protection.

Ms Judith McNamara LL.B (Hons)(Qld)**,** LLM(QUT), Solicitor, Queensland
School of Law
Queensland University of Technology
Ph +61 7 3864 1255, fax +61 7 3864 2121, email j2.mcnamara@qut.edu.au

Ms McNamara is an Associate Lecturer in the School of Law of the Queensland University of Technology. Prior to joining the university in 2006, she was an Associate Lecturer at the University of Southern Queensland and has worked as a solicitor in private practice. Her current research interests include electronic commerce law, intellectual property and privacy.

Dr Ernest Foo, B.E. (Hons)(UQ), PhD(QUT).
Information Security Institute
Faculty of Information Technology
Queensland University of Technology
Ph +61 7 3138 1923, Fax +61 7 3138 1214, email e.foo@qut.edu.au

Dr Foo is a Lecturer in the Faculty of Information Technology at the Queensland University of Technology. He is also an active researcher in the Information Security Institute. Dr Foo has research interests in the field of electronic commerce, in particular the development of secure protocols.

Associate Professor Audun Josang
School of Software Engineering and Data Communications
Faculty of Information Technology
Queensland University of Technology
Ph +61 7 3138 2960, Fax +61 7 3138 1214, email a.josang@qut.edu.au

Associate Professor Audun Josang joined QUT in August 2005. Prior to that, he was the research leader of the Security Unit at DSTC in Brisbane, worked in the telecommunications industry for Alcatel in Belgium and for Telenor in Norway. He was also Associate Professor at the Norwegian University of Science and Technology (NTNU). He has a Masters degree in Information Security from Royal Holloway College at the University of London, and a PhD from NTNU in Norway. Prof. Josang has more than 60 scholarly publications, and his research focuses on security and trust management.

Dr Praveen Gauravaram, B.Tech (EEE, S.V.U.C.E, India), MIT (QUT), PhD (QUT),
Information Security Institute
Faculty of Information Technology
Queensland University of Technology
Ph +61 7 3138 9380, Fax +61 7 3221 2384 email p.gauravaram@isi.qut.edu.au

Dr Gauravaram is a research associate in the Information Security Institute (ISI), QUT and has recently completed his doctoral dissertation in the area of cryptanalysis, design and applications of cryptographic hash functions. His current research interests include the analysis and, design of cryptographic primitives, applications of cryptology, side channel cryptanalysis of cryptographic algorithms and information security.