CRC Construction Innovation
BUILDING OUR FUTURE

E-tendering – Security and Legal Issues: Research Report

Report No. 2002-067-A

The research described in this report was carried out by: Ed Dawson, Sharon Christensen, Bill Duncan, Ernest Foo, Rong Du, Juan Gonzalez Nieto and Peter Black.

Project Leader	Martin Betts (QUT)
Team Members	Debbie Smith, Paul Smith, Adrian Burgess (QUT BEE) Brian Fitzgerald, Bill Duncan, Sharon Christensen (QUT LAW) Ed Dawson, Colin Boyd, Ernest Foo (QUT IT/Security) Kerry London (UN)
Researchers	Peter Black (QUT LAW) Rong Du (QUT IT/Security) Juan Gonzalez Nieto (QUT IT/Security)
Project Affiliates	Ross Smith (QDPW) Ross Guppy, Paul Rollings (QDMR) Neil Abel, Sandra Cranston (BCC)
Research Program No:	A
Program Name:	Business and Industry Development
Research Project No.:	2002-067-A
Project Name:	E-business – Security and Legal Issues
Date:	31 January 2005

Distribution List

Cooperative Research Centre for Construction Innovation
Debbie Smith, Paul Smith, Adrian Burgess (QUT BEE)
Brian Fitzgerald, Bill Duncan, Sharon Christensen (QUT LAW)
Ed Dawson, Colin Boyd, Ernest Foo (QUT IT/Security)
Kerry London (UN)
Ross Smith (QDPW)
Ross Guppy, Paul Rollings (QDMR)
Neil Abel, Sandra Cranston (BCC)
Anne Fitzgerald, Neal Hooper, Tim Beale (Crown Law)

Disclaimer

The Client makes use of this Research 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 Research report or other information provided by Construction Innovation nor for any errors or omissions that may be contained in this research 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 Research 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

List of Tables

PREFACE

The Cooperative Research Centre (CRC) for Construction Innovation research project 2002-067-A, *E-business – Security and Legal 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 Crown Law.

In support of this project's research aims and objectives and as a deliverable for the project, this report is not intended as a comprehensive statement of best practice. Rather it should be read as an overall 'snapshot' of the current legal and security issues concerning electronic tendering (e-tendering).

EXECUTIVE SUMMARY

The Queensland Department of Public Works (QDPW) and the Queensland Department of Main Roads (QDMR) have identified a need for industry e-contracting guidelines in the short to medium term. Each of these organisations conducts tenders and contracts for over $600 million annually. This report considers the security and legal issues relating to the shift from a paper based tendering system to an electronic tendering system.

The research objectives derived from the industry partners include:

- a review of current standards and e-tendering systems;
- a summary of legal requirements impacting upon e-tendering;
- an analysis of the threats and requirements for any e-tendering system;
- the identification of outstanding issues;
- an evaluation of possible e-tendering architectures;
- recommendations for e-tendering systems.

The law governing tendering raises several legal issues, even when the tender process is paper-based. Thorough terms of tender in the tender advertisement are necessary to define the legal rights and responsibilities of the principal and the tenderer and ensure the tender process is both fair and undisputed. Additional legal issues for electronic tendering include:

- The need for prequalification or registration to counter the potential for fraud given the ease with which documents and identity can be manipulated in an electronic environment;
- The need for additional terms of tender to facilitate the process in an electronic environment related to access to tender documents, incorporation of electronic addendum, exercise of discretion where tenders are non-conforming, definition of non-conforming tender in an electronic environment, consent to the use of electronic communication, time of receipt of tender submission, time of formation of ultimate contract, ability to revoke tender submitted electronically and authority of corporate agents to submit tenders;
- How the integrity of the tender box can be maintained in an electronic environment;
- Determination of the time at which electronic communications are received by both tenderer and principal;
- How the security and confidentiality of the process and content can be assured electronically;
- How electronic documents should be archived and remain acceptable as evidence in the event of a legal dispute.

The move to an electronic medium raises the need to address not only legal issues but also the security threats that arise when moving to an open networked environment. These requirements include:

- Secure communication to provide integrity, confidentiality, authentication and non-repudiation of messages.
- Access Control to simulate a tender box by restricting access to submitted tender documents until after the tender close time.
- Secure time functionality to ensure that all parties are synchronised.
- Recordkeeping to ensure that audit logs are kept securely for evidentiary purposes.

There are well-known standardised cryptographic algorithms and protocols that can be used to communicate securely. The choice of concrete mechanism depends greatly on the levels of authentication required for each type of e-tendering communication, which should be determined from a formal risk analysis. Legal considerations as to the evidential value of electronic communications and contracts require the provision of cryptographic non-repudiation using electronic signatures.

Technical mechanisms must be put in place to enforce that tenders are not opened before the agreed opening time. This can be achieved cryptographically by distributing the capability of opening (decrypting) tenders among multiple parties, so as to require their joint cooperation. Alternatively, one could rely on operating access control and logging mechanisms, which for common operating systems may not be reasonable given the lack of assurance that they exhibit. Trusted operating systems provide better reliability and should be considered for the implementation of key e-tendering functionality, such as the e-tender box.

Information that is considered likely to be used as evidence should be extracted and stored in records in a way that does not affect its evidential integrity. Mechanisms are needed to authenticate the origin of records, and the time and date of recorded events. Cryptographic techniques, such as digital time stamping, and the use of trusted operating systems and other security certified software play an important role.

This project has also identified several areas in both the legal and computer security fields that need future work:

- E-tendering architectures need to be investigated further, as do the security mechanisms applied in the e-tendering architectures.
- The legal consequences of using trusted third parties in the tendering process needs to be assessed.
- Research in the area of secure authenticated time systems is required.
- Trusted systems need to be developed to provide a suitably reliable access control system for tender box servers.
- Solutions for the long term storage of secure documents need to be developed.
- A policy for using e-tendering systems for principal administrators, project managers and tenderers needs to be developed.
- A simple demonstrator system can be developed to display security techniques and to demonstrate the overall validity of the e-tendering system.
- Detailed analysis of and consideration of possible reforms to the *Electronic Transactions Act* 2001 (Qld);
- Terms of tender need to be drafted to facilitate any of the e-tendering architectures.

1. INTRODUCTION

1.1 Background

The rapid pace of technological advancement over the last three decades has transformed the construction industry. Today businesses and governments are largely reliant on information and communication technology (ICT) to communicate and enter into contracts. One aspect of this transformation has been the adoption of electronic tendering systems (or e-tendering).

E-tendering is increasingly being adopted throughout Australia and the world. E-tendering, in its simplest form, is described as the electronic publishing, communicating, accessing, receiving and submitting of all tender related information and documentation via the internet, thereby replacing the traditional paper-based tender processes, and achieving a more efficient and effective business process for all parties involved (NT Government; NSW Department of Commerce).

However, as the technology that facilitates e-tendering is relatively new and ever changing and as what little law governs e-tendering is untested and ambiguous, a need for further research into e-tendering was identified by the Queensland Department of Public Works (QDPW) and the Queensland Department of Main Roads (QDMR). This report is the culmination of that research and in addition to evaluating the legal, security and risk issues relating to e-tendering, aims to promote knowledge and awareness about ICT in the construction industry.

1.2 Definitions

While this report has been written in simple English and attempts have been made to avoid technical terms, there are occasions where technical terms are necessary to explain the legal or security issue. For ease of reference, these terms include:

acceptance	The act of assenting to, agreeing; receiving or taking something offered.
access control	Restricting access to resources to privileged entities
addendum	Additional material released by the principal relevant to the tender; any amendments to the tender advertisement and documents. Also known as a Notice to Tenderers.
authentication	Corroboration of the identity of an entity
bilateral contract	A contract formed by the exchange of mutual or reciprocal promises. The offer is made in the form of a promise to be accepted by a counter-promise.
confidentiality	Keeping information secret from all but those who are authorised to see it
cookie	A message given to a Web browser by a Web server. The browser stores the message in a text file. The message is then sent back to the server each time the browser requests a page from the server.

integrity	Ensuring information has not been altered by unauthorised or unknown means
invitation to treat	A request to another to make an offer to engage in negotiations with a contract in mind. Contrasted with an offer which indicates an intention to be bound without further discussion or negotiation, on acceptance of the terms set out.
message authenticity	Corroboration of the source of information; also known as data origin authentication
offer	The expression to another of a willingness to be legally bound by the stated terms.
principal	The party inviting the tender.
repudiation	Denial of previous commitments or actions
tender	An offer from a tenderer to the principal to do work, supply goods, or make a purchase, in accordance with conditions set out in the invitation to tender, at either a uniform rate or inclusive price.
tender document	A document contains a tender project specification, also known as tender specification
tender specification	A document contains a tender project specification, also known as tender document.
tender revocation	A formal notification that a tenderer revokes an offer/tender before it is being accepted, sometimes revocation may happen after a tender is accepted.
tender notice	Advertisement of a tender project.
tender negotiation	Also known as request for information, occurs after tender assessment but before tender acceptance
tenderer	The party submitting the tender.
tenderer submission	Tenderer submission is a tender that is submitted by a tenderer.
unilateral contract	A contract in which an offer is made in the form of a promise to be accepted by the performing of an act. Performance of the act called for with the intention of accepting the offer constitutes both the acceptance of the offer and the furnishing of consideration by the offeree. Typical examples are offers of reward for the giving of certain information or offers of reward to the return of lost property.

2. THE GOVERNMENT E-TENDERING PROCESS

2.1 Tendering Process

Government purchasing is important as considerable sums of public moneys are spent every year. For example, the Queensland Government spends around $6 billion a year on goods and services, with an additional $4.5 billion on capital assets/works (Queensland Government State Purchasing Policy). Quality of service and value for money is maintained by contracting out the provision of certain goods, services and capital assets/works.

In its simplest form, the tendering process involves the principal advertising or issuing a request for tenders (known as an invitation to treat), the various tenderers then make offers, one of which is then accepted by the principal, forming a contract between the tenderer and the principal. Often a tendering system will also involve a system of prequalification or registration so that the principal knows and can easily verify the tenderers.

2.2 The shift to an electronic environment

Traditionally the tender process was a paper based system. However, several factors have lead to the increasing use of electronic tendering, including:

- increasing use of technology within the construction industry;
- the reality that the considerable exchange of information between various parties during a tendering process means an electronic system is more efficient and minimises paper and waste.

Thus, there is a recognised need for a legally compliant and secure e-tendering system. E-tendering, in its simplest form, is described as the electronic publishing, communicating, accessing, receiving and submitting of all tender related information and documentation via the internet, thereby replacing the traditional paper-based tender processes, and achieving a more efficient and effective business process for all parties involved (NT Government; NSW Department of Commerce).

From each of the e-tendering systems reviewed a set of common features and processes can be conceptualised. These common features are mapped against the Australian Standard Code for Tendering in the table below.

Tendering System Component	**Source of Obligation under Australian Standard Code of Tendering for:**		**E-tendering Basic System Function**
	Principal	**Tenderer**	
Pre-qualification & registration			Pre-Qualification Registration
			Issue User Name and Password
Public invitation	Pre-tender	Call for tender	Tender Advertisement
			Tenderer Views Tender Advertisement and Notice
Tender submission	Tendering	Evaluation of tender documents & Formulation of	Tenderer Registration to Tender for a Project

		tenders	Download Tender Document
			Addenda Distributed by Principal
	Receipt of tenders	Submission of tenders	Tenderer Submits Tender
Close of Tender	Closing of tender		Close Tender
			Principal Opens Tender
Tender Evaluation	Evaluation of tenders		Tender Evaluation Process
	Negotiation and selection		Request for Information
Award of Tender			Award Tender/Acceptance of Tender
			Sign the Formal Agreement
Archiving			Retention of Document

Table 1. Correlation between e-tendering system components and Australian Standard Code of Tendering procedures

2.3 Summary

Given the considerable public moneys spent in government purchasing an accountable, secure and legally compliant tendering system is essential. Presently the system is largely paper-based and regulated by the common law and several policies and protocols: *Australian Standard Code of Tendering*' (AS 4120-1994), Queensland Code of Practice for the Building and Construction Industry and Department Purchasing Policies, such as the policy in effect at the QDMR.

This report will outline the legal and security risks associated in adopting an e-tendering system throughout the tender process. These steps (as identified) are:

- Prequalification and registration;
- Public invitation;
- Tender submission;
- Close of tender;
- Tender evaluation;
- Award of tender;
- Archiving.

3. LEGAL REQUIREMENTS AND LEGISLATION

A review of legal resources, including judicial decisions, statutory requirements and journal articles revealed very little in the area of electronic tendering. The majority of legal material is concentrated on the principles of tendering in a paper based system. However, a growing amount of literature and statutory material exists in relation to electronic transactions generally and this part of the report after outlining the current issues for paper based tendering highlights the legal issues and requirements emerging from the literature.

3.1 The law governing tendering

Tendering is the main means by which governments and other public sector organisations award contracts for goods and services. It is seen as the fairest means of awarding government contracts and the method most likely to secure a favourable outcome for the government in its spending of public moneys. Unlike countries, such as the United States, Australia does not have a national system which mandates that contracts be awarded by a publicly advertised tendering process and regulates each stage of the government tendering procedure. Instead, the process in Australia is regulated largely by the common law through the general principles of contract law, supplemented by statutory provisions.

Under the principles of contract law, tendering is initiated by a government advertisement or notice setting out the requirements and conditions to apply to the tender and requesting tenders to be submitted by a stipulated time and date. This initial stage is usually considered an invitation to treat as the government is simply inviting recipients to make an offer. When the government accepts one of the offers and thereby awards the contract to that tenderer, only then will a bilateral contract have been formed. Until the award is made there is no contract so a tenderer may withdraw an offer, the government can consider other offers, including non-complying and late tenders, and will not be bound by any promises made about the tendering process. This position has been judicially criticised in cases such as *Blackpool and Fylde Aero Club v Blackpool Borough Council* [1990] 1 WLR 1195 for departing from parties' legitimate expectations and gives rise to the possibility that the pre-award period could incur legal liability.

There are some exceptions to the contract being formed at acceptance, such as when the contract is contingent on a formal document being executed after acceptance, or where the department requests notification of expressions of interest in the tendering process. Such notifications are not offers but part of a negotiation stage which may lead to short listing from which the invitation to treat may flow.

This first part of this section will outline the common law principles that are present in each of the key steps in the tendering process (identified previously in section 3): pre-qualification and registration, public invitation, tender submission, close of tender, tender evaluation, award of tender, and archiving. The remaining part of this section will consider the shift to an electronic environment and the additional legal issues that arise as a result of that new environment.

3.1.1 Pre-qualification and registration

There is no legal requirement that the principal adopt a pre-qualification or registration system as part of the tender process. The Australian Standard Code of Tendering refers to pre-qualification only in section 6.1.3, where it states: 'In determining who shall be invited to tender, the Principal shall, where appropriate, apply pre-qualification criteria and take into account compliance with any applicable Code of Practice.' However, for practical and commercial reasons, both QDPW and QDMR generally require pre-qualification, while the BCC and *AusTender* require registration only where the tender is to be submitted electronically.

The main legal issue that arises at this stage in the tendering process is one of identification; that is, ensuring that the person who submits the pre-qualification documents is authorised by law to do so. This is only a minor issue as there is very little cost to the principal if a person or company fraudulently pre-qualifies or registers as presumably that fraud would be discovered during the tender evaluation and negotiation stage before the award of the tender and the final contract is signed. The literature reviewed did not suggest this was a significant issue in paper based tendering processes.

3.1.2 Public invitation

The terms of the tender advertisement are important. The ability of a principal to accept a non conforming tender depends to a large extent on the terms of the tender. While there is no doubt that the main contract is formed only once the tender is awarded, the law has only recently recognised the existence of a second collateral contract created upon submission of the tender which governs the pre-award period. In the United Kingdom the approach in *Blackpool and Fylde Aero Club v Blackpool Borough Council* [1990] 1 WLR 1195 suggests that the pre-award process involves a unilateral contract with obligations only on the principal, whereas in Canada, *Ontario v Ron Engineering & Construction Eastern* Ltd [1981] 1 SCR 111 held that the tendering process gave rise to a bilateral contract with obligations on both parties. Regardless of whether it is unilateral or bilateral contract, the two contract analysis appears to have been endorsed by the Federal Court of Australia in *Hughes Aircraft Systems International v Airservices Australia* (1997) 146 ALR 1. In this case the court held that upon submission of the tender the principal was obliged to comply with the tender advertisement and the terms of the tender process. A failure to do so would entitle the tenderer to damages.

Accordingly, a public invitation to tender must be carefully drafted. Whether the government body lays down selection criteria that is clearly articulated by reference to objective criteria and weighted, or reserves for itself a large amount of discretion, this should be readily apparent in the request to tender document.

3.1.3 Tender submission

Just as the principal is obliged to comply with the tender process stated in the terms of the tender, the tenderer is also required to comply with the process and requirements laid out in the invitation to tender. Failure to comply with the terms of the tender may result in a non-conforming tender. Generally the terms of a tender will provide discretion to the principal to either accept or reject non-conforming tenders. Whether the tender is non-conforming will usually depend upon the terms of the tender. The most common situation in which tenders have been held to be non-conforming is where the tender is submitted late.

3.1.4 Close of tender

If the principal wishes to have a discretion to consider late tenders, it is important for this discretion to be explicitly provided for in the terms of the tender advertisement and documents. For example, in the Canadian decision of *Smith Bros & Wilson (BC) Ltd v British Columbia Hydro & Power Authority* (1997) 30 BCLR (3d) 334, the British Columbia Hydro and Power Authority considered a tender that was submitted only one minute late and awarded the contract to that tenderer. However, as the terms of the tender did not give the Authority any discretion to consider a late tender, it was held that that tender should not have been considered and the plaintiff was awarded damages.

3.1.5 Tender evaluation

Several sources of law potentially impose legal obligations on the principal during the tender evaluation step: contract law, misleading or negligent conduct, equity, restitution, and administrative law.

(a) Contract law: implied terms of fairness

In *Hughes Aircraft Systems International v Airservices Australia*, where the pre-award phase was held to form a contract between the government body and the tenderer, Justice Finn found that in addition to the express terms in the Request for Tender, there was an implied term of law that the government authority would conduct its tender evaluation fairly. However in determining the scope of the fairness obligation in the process of evaluating tenders, the court held that apparent bias, as opposed to actual unfair dealing, would not be a breach of the duty to act fairly. It must be shown that there were actual consequences that flowed from a failure to act fairly, not the mere appearance of bias in the tender evaluation process. The distinction can be seen in the *Hughes case* where one member of the Board evaluating the tenders was associated with the company which was actually awarded the contract. Although this member did not disclose his interest until late in the deliberation process, the court found that this affiliation had not influenced the awarding of the contract to that company. Whilst there may have been the apprehension of bias, there was no measurable consequence which amounted to unfair dealing.

Where a breach of an express or implied term occurs in the pre-award contract phase, a tenderer may sue for damages. If successful, the assessment of damages will usually be the amount of the loss suffered by the tenderer in preparing the tender bid. It is not necessary for the tenderer to establish that but for the breach it would have been awarded the contract.

(b) Misleading or negligent conduct

Any conduct during the pre-award period which is misleading or deceptive may be in breach of section 52 of the *Trade Practices Act* 1974 (Cth) or section 38 of the *Fair Trading Act* 1989 (Qld). An example of misleading conduct arose in *Hughes' case.* The invitation to tender stated certain conditions and procedures would apply. These procedures were not followed during the evaluation of tenders. There is also the general law of negligence under which a government body could be held to be responsible for any loss suffered by a tenderer as a result of the negligent misstatement of information or non-disclosure of important information or negligent conduct, such as losing a tender.

(c) Equity: estoppel

Since the High Court's decision in *Waltons Stores (Interstate) Ltd v Maher* (1988) 164 CLR 38 estoppel has become an important aspect of contract law in Australia and thus has relevance for the tendering process. The principle is that where a party has relied, to its detriment, on an assumption, representation, assurance or conduct made by the other party, and the circumstances are such that it would be unconscionable to allow the latter to resile from that assumption, representation, assurance or conduct, then the court will provide relief to the party suffering from the detriment. An example would be where there was a departure from the stated tendering process. Where it can be shown that a tenderer has relied on the initial representation to their detriment and that it would be unconscionable to resile from that, the tenderer may use estoppel as a remedy. For example, estoppel was relied on successfully in *Metropolitan Transit Authority v Waverley Transit Pty Ltd* [1991] 1 VR 181 due to an expectation that Waverly's contract would be renewed if a course of action were taken and money expended. Waverly's reliance, to their financial detriment, on this assumption, provided the basis for an estoppel and an order was made that the contract be awarded to Waverly.

(d) Restitution

The general premise is that the cost of preparing a tender is undertaken by a tenderer and it is known that they will bear all costs should their tender be unsuccessful. It is a risk knowingly assumed by the tenderer. If, however, negotiations result in more work being undertaken at the request of the government body and this is done on the express understanding or implied assurance that the party will then be awarded the tender, it is possible for the tenderer to recoup those costs if the contract does not eventuate (*Sabemo Pty Ltd v North Sydney Municipal Council* [1977] 2 NSWLR 880). Other examples are where a project is abandoned, or where a contract is found to be void.

(e) Administrative law

Judicial review legislation, the *Administrative Decisions (Judicial Review) Act* 1977 (Cth) and *Judicial Review Act* 1991 (Qld), enables dissatisfied tenderers to have the decision reviewed by the courts for non-compliance with the tendering policy or procedure. The action is to be undertaken within 28 days of the decision.

3.1.6 Award of tender

A contract is formed when the principal communicates acceptance to the tenderer. However, it is practice that a formal agreement between the two parties is signed once the tender has been awarded. In a paper based system this does not raise a significant legal issue.

3.1.7 Archiving

The *Public Record Act* 2002 (Qld) requires that the State Archivist keep all public records, which would include documents relevant to the evaluation and award of tenders. Section 10 of the *Limitation of Actions Act* 1974 (Qld) means that these documents would need to be kept for at least 6 years, which is when the limitation of actions expires. In some cases the documents would be kept for considerably longer. This requirement is easily met in a paper based system.

3.2 The shift to an electronic environment

One of the challenges in developing any e-tendering system is in converting the functionality of the traditional paper based system to an electronic environment while maintaining legal compliance. While an e-tendering system is more efficient and cost-effective, the shift to an electronic environment presents several legal hurdles, in part because the law that governs electronic transactions is under-developed and lags behind the technology. However, as the tendering process is governed by contract law, the various gaps in the law could be remedied by explicit and detailed conditions of tender. After providing an introductory overview to the *Electronic Transactions* Act 2001 (Qld) (the ETQA), this section will briefly address some of these issues in the order they arise in the tendering process.

It is necessary to consider the ETQA as it will have an impact upon any e-tendering system adopted in Queensland. The ETQA is Queensland's version of the Commonwealth's *Electronic Transactions Act 1999* and is based on uniform legislation developed by the Commonwealth and State Attorneys-General. This uniform legislation is derived from the United Nations Commission on International Trade Law's Model Law on Electronic Commerce. The Model Law sought to give national legislators a set of internationally acceptable rules that would promote the use of electronic communications.

The objectives of the ETQA are to provide a regulatory framework that:

- recognises the importance of the information economy
- facilitates the use of electronic transactions; and

- promotes business and community confidence in the use of electronic transactions;
- 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 and technology neutral. Functional equivalence means that equal treatment should be given to both paper based transactions and electronic transactions. Technology neutral means that equal treatment is to be given to different kinds of technology, which could include communication via fax, email, Electronic Data Interchange, or some other form of data exchange.

These two principles are encapsulated in section 8 of the ETQA which states the general rule that 'A transaction is not invalid under a State law merely because it took place wholly or partly by 1 or more electronic communications.' This general rule though is subject to displacement if there is another, more specific provision in Chapter 2 of the ETQA.

Chapter 2 of the ETQA provides that the following requirements can be met electronically:

- give information in writing (sections 11 and 12);
- provide a signature (section 14);
- produce a document (sections 16 and 17);
- record information (section 19);
- keep a document (sections 20 and 21).

Notwithstanding these provisions, in the context of e-tendering the ETQA presents several unresolved issues pertaining to:

- receipt of electronic communications;
- formation of contracts electronically;
- authority to enter into contracts electronically;
- evidence of electronic communications and contracts.

These issues are further complicated by the fact that there has been no judicial consideration of the ETQA or any of its equivalents. The only judicial decision in Queensland on contracts formed by email, *Ford v La Forrest* [2001] QSC 261, was decided before the ETQA was enacted. Nonetheless, in *Ford v La Forrest*, Justice Atkinson held that even without the authority of the ETQA, a valid contract can be entered into by means of electronic communications.

Given this background the remainder of this section will analyse the legal hurdles at each step of an e-tendering system.

3.2.1 Pre-qualification and registration

Given the ease with which documents and identity can be manipulated in an electronic environment, it is necessary to employ an e-tendering system that minimises the potential for a person to submit a tender without the appropriate authority or for a person to forge a tender adopting another person's identity. Accordingly, some form of prequalification or registration may be necessary to prevent this from occurring. The ETQA attempts to address the issue of unauthorised electronic communication through s 26 of the Act, which 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 essence this would allow a person to deny the authenticity of an electronic communication sent without their authority. Despite the fact this type of situation may be rare or be discovered prior to entry into a contract, the fact authorised tenders can be submitted may in some situations generate additional costs for the principal and legal problems if tenders are accepted. A system of prequalification including security mechanisms to identifying the party using the system would miminise the potential risk.

A further advantage of prequalification in an electronic environment is that addendums can be easily communicated to potential tenderers.

3.2.2 Public invitation

The terms of the tender contained within the advertisement are particularly important in an electronic environment. Additional conditions of tender necessary within an electronic environment include:

- Limiting access to tender documentation to pre-qualified individuals via secure electronic means.
- Appropriate terms allowing the incorporation of addenda to documentation through electronic distribution.
- Appropriate terms that allow the principal to exercise discretions for tenders that do not conform.
- A clear definition of what will constitute a non-conforming tender in an electronic environment.
- Consent of the tenderer to the use of electronic communication in the contracting process.

3.2.3 Tender submission

Tender Integrity

The common law does prescribe a method for submission of tenders or the opening of tenders, this is usually governed by the terms of the tender or by internal policy. In the traditional paper based tender system, the integrity of a government tender is maintained by placing the tender in a tender box which can only be opened by two people with two different keys. If a similar policy is to be maintained in an electronic environment, similar security would need to be provided. The main function of this type of security is to protect the principal from allegations of collusion, fraud or other impropriety by tenderers.

Non-conforming tenders

The other main issue concerning tender submission is the determination of what tenders are non-conforming. It is standard practice that conditions of tender provide a definition of what constitutes a non-conforming tender and also provide a discretion to the principal to accept non-conforming tenders. The use of an electronic medium for the submission of tenders creates addition situations in which tenders may be considered as non-conforming (eg. if certain fields of the tender form are not completed, the tender documents contain a virus or macro, the tender documents are corrupted). To avoid claims by tenderers the terms of tender will need to clearly specify a meaning for ‘non conforming tenders’ and provide a broad discretion to deal with those types of tenders.

Similarly to paper based tenders the issue of late tenders is also relevant. If a tender is received late (as discussed below) the conditions of tender would need to specify first whether late tenders will be accepted and secondly, if they are accepted in what circumstances will this occur and what discretion does the principal have to reject the tender. The e-tendering system will need to be designed to accord with these legal requirements.

3.2.4 Close of tender

The time at which a tender will legally be received by the principal is of particular importance to the question of non-conforming tenders. In an electronic environment additional factors may impact on the ability of a tenderer to submit their tender on time. For example, the principal’s server may be unreachable at the time for submission of the tender. Is the tender late in this situation? If the tender is submitted late due to the conduct of the principal or their agents, what is the position of the tenderer?

At common law, an offer is generally effective upon receipt (although the terms of the tender may alter this). Accordingly, in a paper based tendering system, the tender is generally effectively received once it has been placed in the tender box. In an e-tendering system, there may be some uncertainty as to when an offer is received.

Section 24(2) of the ETQA states that unless otherwise agreed, an electronic communication is received when it comes to the attention of the addressee. If however, the address has designated a particular information system the electronic communication will be received when it enters that system (s 24(2)). Schedule 2 defines both ‘electronic communication’ and ‘information system.’

An ‘electronic communication’ is defined to mean:

- a communication of information in the form of data, text or images by guided or unguided electromagnetic energy; or
- 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.

An ‘information system’ is defined as ‘a system for generating, sending, receiving, storing or otherwise processing electronic communications.’

A tender submitted electronically is an electronic communication within the meaning of the ETQA and therefore will be received either when it comes to the attention of the addressee or when it enters a designated information system. The operation of s 24 raises the following questions:

- What is an information system?
- When does a communication enter an information system?
- How is an information system designated?
- When will a tender submission come to the attention of the addressee?

As the ETQA does not definitively answer these questions, the prudent course is for the conditions of tender to designate the information system (ie. the electronic tender box) and the time at which it will be deemed to enter that tender box (possibilies include upon receipt of an email confirming the tender had been received or at the time noted on the e-tender website).

3.2.5 Tender evaluation

Given the industry practice of extensive negotiation and clarification between the principal and the tenderers before the award of the contract, it is necessary for the conditions of tender to enable this communication to take place. It is also desirable that this communication be facilitated electronically.

3.2.6 Award of tender

There are several issues that arise in relation to the award of a tender:

1. When is a contract formed electronically?
2. When can an offer (tender submission) be withdrawn?
3. If the person submitting the tender lack authority will that affect the contract?

Formation of contract

Although the e-tendering systems currently in use do not advise the successful tenderer electronically, this issue should be considered for future use.

At common law an acceptance is generally effective at the time it is communicated to the offeror. The main exception to this rule applies where the post is used as the method of communication between the parties. This is referred to as the postal exception rule. If the rule applies an acceptance will be effective at the time it is posted.

There have been no judicial pronouncements on the application of the postal acceptance rule to e-mail correspondence . The cases tend to distinguish the post from instantaneous forms of communication such as telexes and faxes where the sender will know if the communication has not been received. The majority of e-mail will be sent via a commercial ISP through the Internet and to the recipient's ISP. While this may appear to be more equivalent to an electronic version of the post than a facsimile, the better view is that acceptance by email should be effective at the time it is received. (Christensen 2001)

Sections 23-25 of the ETQA provide for the time and place of receipt of an "electronic communication". Section 24 provides

> **Time of receipt**
>
> **24.(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.

In the context of e-tendering s 24(1) will be relevant. It would be prudent for the terms of tender to expressly provide for time at which a contract is formed. This can be achieved either by designating an information system or by expressly providing for a contract to be created at the time the communication is sent or received.

If an information system is designated for the purposes of s 24(1) one unresolved issue is exactly what is an information system. Information system is defined to mean “a system for generating, sending, receiving, storing or otherwise processing electronic communications”. The definition means that an information system may vary depending upon the individual situation:

(i) An individual with a home computer: in that case the computer would be the information system
(ii) A large company with a networked system: in that case the information system may be the network or the individual computers on each person’s desk
(iii) A large institution with their own server: in that case the information system may be not only the network but also the server maintained by the institution, or just the network for the particular area or the individual computers.

For this reason the terms of tender should provide more specifically for the time of formation of the contract rather than relying on s 24 of the ETQA.

Revocation of an offer

The time at which an offer can be revoked is linked to the question of formation of the contract. At common law an offer (in this case the submitted tender) can be revoked at any time prior to acceptance of the offer. The revocation is effective at the time the revocation is received. These principles are not altered by the ETQA. The provisions of s 24 of the ETQA are relevant to the question of when is an electronic communication received. Due to the uncertainty about the operation and interpretation of s 24 the terms of tender should deal specifically with the right of a tenderer to revoke their offer.

Authority of officers of the Tenderer

Chapter 2B of the *Corporations Act 2001* (Cth) gives individuals the power to ‘make, vary, ratify or discharge a contract’ on behalf of a company. The ETQA implicitly allows individuals to do so in an electronic environment. Given the relative ease with which identity and documents can be manipulated in an electronic environment, a pertinent issue is whether a company can challenge a contract for lack of authority of an officer or agent.

Section 26 of the ETQA provides that ‘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.’

The ETQA does not provide any technical requirements for security, integrity or authentication. The meaning given to ‘sent by the originator’ should therefore be defined in the conditions of tender. The conditions of tender should also set forth any measures to ensure to security, integrity or authentication, such as Public Key Infrastructure or the use of unique usernames and passwords generated at registration or prequalification.

3.2.7 Archiving

The *Public Records Act 2002 (Qld)*, requires public authorities to keep and maintain public records. This will apply to both paper based and electronically formed contracts following the tender process. The Public Records Act does not prescribe the method for keeping and maintaining these records, except for the fact electronic records should remain accessible: section 14(1).

Related to the maintenance of records is the question of how those records should be kept and maintained in the event of a legal dispute. Issues arising include:

- How can the contents of an e-document be proven?
- How can the integrity of an e-document be proven?
- How should the principal archive/store e-documents?

- How should e-documents be produced in court?

The *Evidence Act 1977* (Qld) allows electronic documents to be admitted in court. ‘Document’ is defined in section 3 of the Act as including ‘any disc, tape, sound track or other device in which sounds or other data (not being visual images) are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced therefrom.’ However, the court has a wide discretion not only in relation to the admissibility of evidence, but also to the weight that it will attach to certain pieces of evidence. Therefore, a reliable electronic recording system is needed to ensure the security, integrity and authenticity of documents.

Part 2, Division 4 of the ETQA provides some assistance in determining what measures would be required. Section 19 of the ETQA provides that a requirement to record information in writing is satisfied by recording information in an electronic form if the following two circumstances are met:

- at the time the information was recorded, it was reasonable to expect the information would be readily accessible so as to be useable for subsequent reference; and
- if a regulation requires the information to be recorded on a particular kind of data storage device, the requirement has been met.

Section 20 of the ETQA provides that a person may keep a written document in an electronic format if:

- having regard to all the relevant circumstances when the electronic form of the document was generated, the method of generating the electronic form of the document provided a reliable way of maintaining the integrity of the information contained in the document; and
- when the electronic form of the document was generated, it was reasonable to expect the information contained in the electronic form of the document would be readily accessible so as to be useable for subsequent reference; and
- when a regulation requires the electronic form of the document to be kept on a particular kind of data storage device, the requirement has been met for the period.

Section 21 of the ETQA allows a person to keep information contained in an electronic communication in an electronic form if:

- at the commencement of the keeping of the information, it was reasonable to expect the information would be readily accessible so as to be useable for subsequent reference; and
- the method of keeping the information in electronic form provided a reliable way of maintaining the integrity of the information contained in the electronic communication; and
- during the period, the keeper also keeps, in electronic form, such additional information as is enough to enable the identification of the origin of the electronic communication, the destination of the electronic communication, when the electronic communication was sent, when the electronic communication was received; and
- at the commencement of the keeping of the additional information it was reasonable to expect the additional information would be readily accessible so as to be useable for subsequent reference; and
- if a regulation requires the information to be kept on a particular kind of data storage device, that requirement has been met.

The main criteria within each of these sections is:

(a) the information must remain accessible;
(b) the method used for storing information must be reliable for maintaining integrity in the document

The obligations of a public authority under the Public Records Act can only be met if these criteria in the ETQA are satisfied. The following two Queensland Government Information Standards may assist in determining what is sufficient to meet these criteria:

1. Information Standard 40 (IS40)– Recordkeeping (Qld Government 2001); and
2. Information Standard 41 (IS41) - Managing Technology Dependant Records (Qld Government 2001b).

IS40 provides policies and principles for recordkeeping for State and Local Government in Queensland, and is intended to assist public authorities in complying with the Public Records Act 2002. IS40 has an accompanying Best Practice Guide to Recordkeeping (Qld Government 2002) that provides guidance for implementing IS40. IS41 identifies principles for managing technology-dependent records, including electronic records, and provides pointers to best practice standards, tools and manuals for their implementation.

Despite these standards, the technical solution for complying with the criteria in the Public Records Act is not settled and requires further research.

3.3 Summary

The law governing tendering raises several legal issues, even when the tender process is paper-based. Particular terms of tender in the tender advertisement are necessary to define the legal rights and responsibilities of the principal and the tenderer and ensure the tender process is both fair and undisputed.

Shifting the tender process away from a paper based environment to an electronic environment presents additional legal hurdles, even with the existence of the ETQA. These include:

- The need for prequalification or registration to counter the potential for fraud given the ease with which documents and identity can be manipulated in an electronic environment;
- The need for additional terms of tender to facilitate the process in an electronic environment, related to access to tender documents, incorporation of electronic addendum, exercise of discretion where tenders are non-conforming, definition of non-conforming tender in an electronic environment, consent to the use of electronic communication, time of receipt of tender submission, time of formation of ultimate contract, ability to revoke tender submitted electronically and authority of corporate agents to submit tenders;
- How the integrity of the tender box can be maintained in an electronic environment;
- Determination of the time at which electronic communications are received by both tenderer and principal;
- How the security and confidentiality of the process and content can be assured electronically;
- How electronic documents should be archived to comply with requirements of the *Public Records Act* 2002 and ETQA and remain acceptable as evidence in the event of a legal dispute.

4. SECURITY THREATS AND REQUIREMENTS

Detailed security requirements can only be the result of a risk assessment of a specific e-tendering system. A risk assessment involves evaluating the consequences, both legal and business, and likelihood of threats occurring. Security requirements are then developed from the results of the risk assessment. The previous section identified several security requirements, such as the need for identity verification, which result from legal considerations. This section provides a broader view of potential risks to e-tendering systems. It identifies generic threats and provides security requirements to act as guidelines which should apply to most e-tendering systems.

4.1 E-Tendering Threats

An e-tendering system is a collection of users, electronic media, digital data and actions that can be performed, enabling those users to interact. Actions change the e-tendering system state. E-tendering system security policies define a subset of actions that transform e-tendering system from one secure state to another. Threats and possible security violations define the subset of actions that transform the e-tendering system from secure to insecure states.

Identifying system threats is a complicated issue. It involves an overall understanding of the traditional business, legal requirements, technology (for example software applications), security standards for developing and maintaining a system, and fundamental computer security concepts. This section identifies major threats that are present at each key step in the tendering process: pre-qualification and registration, public invitation, tender submission, close of tender, tender evaluation, award of tender and archiving. The discussion assumes a simple e-tendering system design with limited security.

4.1.1 Pre-qualification & registration

The pre-qualification and registration stage of the e-tendering process requires potential tenderers to submit a registration form to the principal for qualification assessment. The principal will assess each registration and issue pre-qualification status for each qualified potential tenderer to access the e-tendering system. This status is usually based on the ability of the potential tenderer.

This stage of the electronic tendering process is ideal for the distribution of user identities and credentials for access control. This process will also raise security issues and possible threats.

The following threats apply to the pre-qualification and registration process:

Integrity violation: Malicious parties can change, alter, or delete the registration form submitted by the potential tenderer.

Confidentiality violation: The registration forms submitted by a potential tenderer may contain company sensitive information. A malicious party may gain access to this material.

Masquerade/impersonate: A malicious party may provide invalid information, including a false name, in the registration form in an attempt to receive a user identity and credentials on the e-tendering system. A malicious party may attempt to impersonate a valid potential tenderer in order to prevent them from gaining user identity and credentials on the e-tendering system.

Non-verifiable evidence: A potential tenderer may deny the validity of information specified in the registration form at a later time.

4.1.2 Public invitation

In this stage of the e-tendering process, the principal creates a public invitation to tender for a particular project. Tender specification documents or tender advertisement are developed and advertised. On restricted systems, only pre-qualified tenderers are allowed to view the tender advertisement and the principal is notified when the tenderer views the advertisement document. These systems may require the pre-qualified tenderer to register for the project.

During this stage tenderers may also query the principal and request explanation or clarification of the tender specification. In response to these queries or for any other valid reason, the principal may choose to send out an addendum to the tender specification.

Integrity violation: A malicious party may alter the tender specification document or advertising information. Thus tenderers may submit offers for the wrong project or fail to complete all requirements.

Confidentiality violation: On closed systems, where only pre-qualified tenderers are allowed to view the tender advertisement or addendums. Malicious parties may be able to view sensitive material in the tender advertisement or addendum.

Masquerade/impersonate: A malicious party may impersonate the principal and issue a false tender advertisement, causing tenderers to waste time and money developing tender submission documents.

A malicious party could also generate fake addendums pretending to be the principal and thus causing tenderers to produce invalid tender submissions.

Non-verifiable evidence: Tenderers may be able to deny that they received responses to explanation requests or addendums from the principal and falsely claim that they were not given an equal opportunity to respond to the tender. Pre-qualified tenderers in a closed tender may dispute that they ever received notice of the tender advertisement and claim they were not given the chance to participate in the tender.

4.1.3 Tender submission

During this stage the tenderers prepare and submit tender offer documents to the electronic tender box. The principal should not be able to view the tender offer documents before the close of tender. Tenderers have the opportunity to withdraw any submitted tender documents before the close of tender.

Integrity violation: A malicious party can change, alter, or delete a submitted tender document prepared by the tenderer.

Confidentiality violation: A malicious party can access sensitive information contained in the tender offer documents. The malicious party could then prepare their own tender document undercutting other tender prices.

Time Integrity violation: A malicious party may alter the time on the tender box server causing the submitted tenders to be released ahead of the close of tender time.

Masquerade/impersonate: A malicious party can submit a false tender under the name of a legitimate tenderer. The legitimate tenderer may not be able to deny ownership of this false tender document.

Denial of service: The service maybe down due to a denial of service attack or technical failure. Tenderers would not be able to submit their documents before the tender close time.

Repudiation: Both tenderer and principal can deny content or time of submitted tender document causing a dispute between principal and tenderers.

4.1.4 Close of Tender

This stage covers the close of the tender box at a time specified by the principal. Documents submitted by tenderers are then released to the principal for evaluation. After the submission deadline, the principal can reject any late or non conforming tenders.

Integrity violation: A malicious party may be able to alter, change or delete a tender submission document after the close of tender time when the tender box is opened but before the evaluation of the tender by the principal.

Confidentiality violation: An unauthorised party may be able to access the tender documents after the close of tender time. This is still a threat as tender documents may contain sensitive information which the tenderer does not wish to be released to parties who are not the principal.

Time integrity violation: A malicious party may change the time on the principal or tenderers' computer system, thus causing tender documents to be submitted late or so that their tender is submitted on time?

Masquerade/impersonate: A malicious party or unauthorised person working for the principal may access the tender box at close of tender instead of authorised agents of the principal.

Repudiation: A tenderer or other malicious party may falsely claim that the principal opened the tender box before the close of tender time. The principal may not be able to prove or deny this claim.

Denial of service: A denial of service attack or technical failure may prevent the principal from opening the tender box at the appropriate time.

4.1.5 Tender Evaluation

At this stage, the major activities involved are assessing submitted tender documents. The principal has the full control of the assessment. The principal can check each tenderer's qualifications and evaluate tender offer documents for compliance. In some cases the principal may request clarification of the tender document or conduct negotiations with the tenderer most likely to be selected.

Integrity violation: A malicious party may gain access to the document during evaluation and alter the submitted tender document to favour a particular tenderer.

Non-verifiable evidence: The preferred tenderer may falsely claim that they did not receive any clarification or negotiation messages from the principal. The principal may not be able to deny this claim. Alternatively the principal may falsely claim that a tenderer did not agree to conduct post tender negotiations. The tenderer may not be able to deny this claim.

4.1.6 Award of Tender

After tender evaluation, the principal can award the tender to the most suitable tenderer. The principal notifies the winning tenderer with a formal acceptance message. The other tenderers are notified that they are unsuccessful. The principal has the option of releasing information regarding the successful tender to the unsuccessful tenderers. The principal and winning tenderer also have the option of signing a formal contract.

Integrity violation: A malicious party may alter the award of tender message so that an incorrect tenderer is notified that they have won the tender.

Confidentiality violation: Sensitive information regarding the winning tender may be released. The list of unsuccessful tenderers may be released.

Masquerade/impersonate: A malicious party may impersonate the principal to send fake tender award to an unsuccessful tenderer or to notify the successful tenderer that they did not win the tender.

Non-verifiable evidence: If no integrity and confidentiality service in place, people can not tell which award message is genuine.

Repudiation: Both principal and tenderer can deny that they have sent or received the award of tender notification. In cases where a contract document must be signed, the principal or tenderer may deny that they have signed the document.

4.1.7 Archiving

This tendering stage covers the retention of documents to form long term verifiable contractual evidence.

Integrity violation: A malicious party can change, alter, or delete stored documents and logs. This will become an issue if a dispute occurs.

Confidentiality violation: Sensitive information may be stored in archived documents. A malicious party may gain access to these documents after a period of time.

4.2 Security Requirements for E-Tendering

The purpose of the threat identification is to define the system requirements. The normal system development requires that the developer identify threats and then define the system security requirements (Bishop 2003).

The threats identified in section 4.1 can be classified into the following categories:

- Integrity violations,
- Confidentiality violations,
- Masquerading or impersonation,
- Repudiation,
- Time integrity violations,
- Non-verifiable evidence, and
- Denial of service.

This section will study each type of threat and determine security requirements to address each threat.

4.2.1 Integrity Violations

The integrity security requirement is essential to ensuring the correct execution of the e-tendering process as integrity violations can occur throughout most steps of the e-tendering process.

To address integrity violations the integrity of transmitted messages must be protected. Also the integrity of documents must be ensured while stored temporarily in the tender box, during evaluation and after the tender has closed. The integrity of different types of documents must also be maintained. Tender submission documents are obvious targets. But system logs and acknowledgement messages must also have their integrity maintained.

4.2.2 Confidentiality Violations

Like the integrity security requirement, confidentiality is essential to ensuring the correct execution of the e-tendering process. Confidentiality of messages is important when advertising closed tenders, submitting tender documents and conducting any post tender close negotiations. Confidentiality of tender documents, particularly tenderer submitted documents may also need to be maintained after the tender process has completed.

4.2.3 Masquerading or impersonation

This threat has lead to two security requirements. The most obvious is the authentication of messages transmitted during the e-tendering process. False messages should be easily identified and rejected by all e-tendering parties. The other is the authentication of user identities when accessing e-tendering computer systems. This is particularly the case when accessing the tender box application. Only authorised personnel should be gaining access to submitted tender documents.

4.2.4 Repudiation

The non-repudiation of messages and documents is another security requirement of e-tendering systems. Originators of messages and authors of documents should not be able to deny their part in the e-tendering process. The non-repudiation property is closely linked to authentication.

4.2.5 Time Integrity Violations

Secure time is an important requirement in e-tendering. All tenderers and the principal should be operating with the same time thus all system clocks should be synchronised. This is particularly important given that the close of tender time is very important to the tender process. The authentication of the server that e-tendering parties synchronise with is also essential to prevent the wrong time from being set. Secure timestamping is also an important quality when recording and logging e-tendering events.

4.2.6 Non-Verifiable Evidence

The secure record keeping requirement addresses the threat of non-verifiable evidence. This requirement is linked with the integrity, confidentiality, authentication and non-repudiation security requirements. If records are kept with these properties in mind the threat of non-verifiable evidence is greatly reduced.

4.2.7 Denial of Service

The availability of systems is a concern at all steps of the e-tendering process. But it is particularly important during the tender submission stage before the close of tender time. It is essential that the tender box be available for this time.

4.3 Summary

The threats to the electronic tendering process can be classed into the following categories.

- Integrity violations;
- Confidentiality violations;
- Masquerading or impersonation;

- Time integrity violations;
- Non-verifiable evidence;
- Repudiation; and
- Denial of service.

These threats have lead to the following generic security requirements. Note that for a detailed list of security requirements, a risk assessment of each specific e-tendering system needs to be conducted:

- Integrity, confidentiality, authentication and non-repudiation in e-tendering communications.
- Integrity, confidentiality in the storage of records. Records can include system logs as well as documents associated with the tendering process.
- Authentication of users for access to authorised systems. This is particularly the case for the tender box system.
- Integrity and authentication of time systems to ensure that all parties can synchronise to the correct time.
- Non-repudiation of messages and documents generated by both tenderers and the principal.
- System availability particularly during the tender submission stage before the close of tender time.

5. ADDRESSING E-TENDERING ISSUES

Sections 3 and 4 of this report identified various legal and security issues that need to be considered when designing an e-tendering system. This section addresses these issues and threats by considering what security and legal solutions could be adopted to ensure an efficient and effective e-tendering system. These solutions are considered under these key areas:

1. Secure communications;
2. Access control;
3. Secure time;
4. Recordkeeping;
5. System availability;
6. File formats.

When considering each of these areas in this section the pertinent security or legal issue will be identified.

5.1 Secure Communications

An effective e-tendering system needs to ensure that any communication that passes through the system is secure. In addition to the fact that from an ICT perspective secure communications is the most obvious concern for e-tendering over open networks, such as the Internet, from a legal perspective the Australian Standard Code of Tendering AS4120-1994 (SA 1994) requires that all information passed between tenderers and the principal be treated as confidential (see section **Error! Reference source not found.** of this report). Secure communications are particularly essential during prequalification or registration, submission of tender and the award of the tender.

The main risks are that confidential information transmitted over open computer networks may be exposed to or altered by malicious parties. There is also the risk of malicious parties generating false messages, impersonating other parties or denying that messages have been sent. The following sections discuss confidentiality, integrity, message authentication and non-repudiation in e-tendering communications, as well as standard secure communications mechanisms, including the Secure Sockets Layer, the most common mechanism for enabling confidentiality and integrity on open networks. Public key cryptography and infrastructures are also discussed as these mechanisms commonly provide message authentication and non-repudiation.

5.1.1 Confidentiality

Confidentiality in computer systems and networks prevents the unauthorised disclosure of sensitive information. In the e-tendering process, communication can be kept confidential more efficiently than using a paper-based system.

In computer systems and networks confidentiality is provided through the use of cryptographic encryption mechanisms which use cryptographic keys. A cryptographic key is usually a large number used as input to the cryptographic encryption mathematical function. The strength of an encryption algorithm is usually determined by the size of the key in bits. The larger the key the more secure the encryption.

Encryption mechanisms can be split into two major types: symmetric key encryption and asymmetric key encryption. Symmetric key encryption requires the same key to be used to encrypt and decrypt a message. This key is kept secret from everyone except the recipient of the message and of course the creator of the message. Asymmetric key encryption requires a public key, which is known to everyone, to encrypt a message and a private key, which is only known to the authorised recipient of the message, to decrypt the message. Both the private key and public key are mathematically related. Asymmetric key encryption is also known as Public Key encryption systems.

In the e-tendering process, most communication will need to employ both symmetric key encryption and public key encryption systems. Public Key encryption will be used to distribute symmetric keys which will in turn be used to encrypt transmitted messages. The combination of public key and symmetric key encryption is quite common. Public key encryption overcomes the need for a shared key, but symmetric key encryption is much more efficient. The issues and problems with public key systems will be discussed in section5.1.5.

5.1.2 Integrity

Integrity can mean different things depending on the context in which it is used. Integrity of information in computer systems is a property that ensures that the protected data cannot be manipulated or modified from its original source. From a legal perspective, it is necessary to maintain integrity in the e-tendering process so that the documents are reliable and the tender box has not been compromised in contravention of the obligation of confidentiality. Therefore it is important to ensure that communications between the principal and tenderers are not altered by a dishonest or fraudulent party.

It is trivial to change the values of bytes on a computer system or as it is transmitted on a network. Indeed as data is transmitted over a network, it may be accidentally changed by physical conditions. The integrity property is maintained by allowing the recipient of the message the ability to detect if the message has been changed or not. Usually the integrity property is provided through the use of a digest or checksum which is created using a one-way hash function. This mathematical function cannot be reversed but it does produce a unique compressed solution. The message data is input into the hash function and the result is stored securely elsewhere. To verify the integrity of the original document another hash is created. The result is compared with the original stored hash result. If the values are the same the document has not been altered.

5.1.3 Non-repudiation

In computer systems non-repudiation is the proof or evidence that a particular action has taken place. It protects against denial by a party of the action. Non-repudiation can be an extension of the authentication process. In the context of secure communications, non-repudiation ensures that the originator of a message cannot deny having sent it.

In the e-tendering process, non-repudiation is required to ensure that the principal cannot deny that it has advertised the tender specification documents or awarded the winning tender. Non-repudiation can also be used to ensure that each authorised pre-qualified tenderer cannot deny their submitted tender offer document. Non-repudiation is usually implemented through the use of a digitally signed message.

Non-repudiation is particularly necessary given section 26 of the ETQA (as discussed in section 3.2.1) which states that 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. A digital signature to identify the party using the system would miminise the potential risk that that party would deny the authenticity of an electronic communication on the basis that it was sent without their authority.

5.1.4 Secure Communication Standards

There are many standard cryptographic algorithms and protocols that can be employed to implement secure data communications. Although no specific cryptographic mechanisms for secure communications have been endorsed by the Queensland Government, the Queensland Government's Information Standard 18 – Information Security (QG 2002), which sets up the mandatory general information security principles for Queensland Government departments, refers to Australian Government Information Technology Security Manual

(ACSI 33) (DSD 2003). ACSI 33 specifies a set of cryptographic algorithms and protocols to be used for the protection of communications involving Australian Government departments and agencies. The public key algorithms identified are:

- Diffie-Hellman key agreement protocol (Diffie 1976).
- Digital Signature Algorithm (DSA) (NIST 2000).
- Rivest-Shamir-Adleman (RSA) encryption (RSA 2002).

The symmetric encryption algorithms identified are:

- Advanced Encryption Standard (AES) (NIST 2001).
- Triple DES (AS 2000).

The recommended hashing algorithm is the Secure Hashing Algorithm (SHA-1) (AS 2000b).

All of the above algorithms are well known and widely used cryptographic primitives. However, it is necessary to have more than a good set of cryptographic primitives. Cryptographic protocols that specify how the primitives are to be applied to communications data, as well as how cryptographic keys are derived, are also needed. ISO/IEC 11770:1-3 (ISO 2004) specifies key establishment techniques based on symmetric keys and asymmetric keys, and a new standard ISO/IEC 11770:4 using passwords is expected to be released soon.

With respect to secure communication protocols, ACSI 33 identifies the Secure Sockets Layer (SSL) (Frier 1996). Most people who say that they are using secure Internet communications are referring to the use of SSL. Unfortunately the capabilities of this mechanism are not always well known. SSL is a set of protocols which provide end to end encrypted communication between clients and servers. SSL also provides authentication of servers and optionally authentication of clients.

SSL was originally developed by Netscape Communications. After the third version of the protocol was developed, it was standardised by the IETF. Newer versions of the SSL protocol are officially known as the Transport Layer Security (TLS) protocols (IETF1999) although they are still often referred to as SSL.

The SSL protocol has two main stages. In the first stage, SSL uses public key cryptography and digital signatures to validate the server and ensure that the server is who it claims to be. Because there is no recognised public key infrastructure in place, the web browser will often require the user to verify the digital certificate manually. SSL does not authenticate the user. The client machine can be authenticated optionally using the protocol, but this is almost never used.

After the server has been authenticated, a symmetric key is selected for the session and symmetric key encryption is used to exchange encrypted information. For each transaction, a different encryption key is used.

It is recommended that SSL be used for all secure communications required by the e-tendering process. But it should be noted that SSL only provides confidentiality and integrity from end to end on the network only. Once the message has been received by the host machine or the file uploaded to the server, it is no longer encrypted. SSL automatically decrypts the received file. So for the information to remain confidential once it is received, the sender must have additionally encrypted the message.

5.1.5 Public Key Cryptography and Infrastructure

Public key cryptography enables the use of digital signatures. In an e-tendering system, the digital signature mechanism can provide authentication and non-repudiation.

Public key cryptography employs two mathematically related cryptographic keys for each user. One is a private key which is kept secret by the user. The other key is a public key which is distributed to all. To encrypt data the recipient's public key is used. Only the recipient's private key can decrypt the message.

Public key cryptography can be used for authentication and non-repudiation by having the sender of the message encrypt the message using their private key. The original message along with the encrypted version of the message is sent to the recipient. The encrypted version of the message is often referred to as the digital signature of the sender for that particular message. The recipient uses the sender's public key to decrypt the digital signature. If the original message matches the decrypted digital signature, then we can assume that the sender has "signed" the message as only the sender can have created the encrypted message with their private key and only the sender's public key can re-create the original message. Note that because public key encryption algorithms can be relatively inefficient, usually only a digest of the original message is encrypted to create the digital signature. A digest of the original message is used to verify the decrypted digital signature.

There are several management issues with public key cryptography that must be addressed as identified in ISO/IEC 11770:1 (ISO 1999):

- key distribution;
- key generation and storage;
- key recovery;
- key revocation.

Key Distribution

The main difficulty with using public key cryptography is the distribution of public keys to the user community. On the surface having a particular user broadcast their public key to the community at large seems to be the easiest solution. But anyone can forge this message. A malicious user could pretend to be user A and broadcast their public key as user A's public key. To solve this problem, a public key infrastructure is required. A public key infrastructure ensures that all distributed public keys actually belong to the correct users. The way public key infrastructures achieve this is by employing a certificate authority. Certificate Authorities (CA) are trusted third parties who distribute digital certificates which contain a user's public key. The CA vouches for the validity of the public key by digitally signing the certificate. All users in the community must trust the digital signature of the CA. Digital certificates can also contain other data. The contents of a certificate are often defined by an IETF standard X.509.

In PGP (Pretty Good Privacy), users act as their own issuing authority and CA. The community of users accept the certificates on the basis that the user is who they say they are without further verification. It is recommended that e-tendering models do not use this simple level of public key infrastructure.

Key Generation and Storage

Another issue with public key cryptography is the generation and storage of a user's public and private key pairs. Sometimes multiple key pairs are required as a user can use different key pairs for authentication, encryption and non-repudiation. This increases the security of the system.

There are two main methods for generating keys. The first is to have the user application generate the key pair, storing the private key locally and sending the public key securely to the CA for distribution. The alternative method is to have the key pair generated by the CA or other issuing authority, with the private key being securely transmitted to the user. The advantage of the second method is that the issuing authority can keep a copy of the private key if the user loses their copy of the private key. The disadvantage of this method is that it exposes the risk that the private key could be used by the CA or issuing authority. In e-tendering systems, the pre-qualification process is ideal for the generation and distribution of private keys and public key certificates.

Private keys should be stored securely. One disadvantage of keeping a public key on a local hard drive is that if the user is away from their desk other people may be able to access their private key. Most public key cryptography applications use a password to ensure that only the correct user can access their private key. Depending on the mobility of users, the private key may be stored on a portable device such as a USB memory drive or a Smartcard device. The advantage of the smartcard is that it is also physically tamper-resistant.

Key Recovery

If public key cryptography is used for encryption, it may be necessary for entities other than the owner of the private key to be able to recover the key if it is lost. Indeed this may be a policy for government organisations which wish to be able to access all encrypted material. The process of recovering the private key is known as key recovery or key escrow.

Key recovery is only necessary when using public key encryption. It is assumed that most long term encryption mechanisms will use symmetric keys and symmetric key encryption techniques. This is not the case for authentication or non-repudiation which are the main properties employed by e-tendering. The use of key recovery mechanisms may even risk the evidentiary value of the non-repudiation property provided by digital signatures as it is possible that more than one person can create the digital signature.

Key Revocation

Private and public keys have a fixed lifetime. The longer a key is used the greater the probability that they will be compromised. A public key infrastructure must have a mechanism for notifying the community if a public key certificate and matching private key is no longer valid. This process is known as key revocation.

To enable key revocation, a system of revocation lists is used. These certificate revocation lists contain a list of certificates that are no longer valid. Users must continually check the certificate revocation list to ensure that the public key they are using is valid. The maintenance of multiple certificate revocation lists can become non-trivial with large hierarchical public key infrastructures. Since e-tendering systems are expected to have a relatively small user community with a single CA, the updating of certificate revocation lists should not pose a problem.

It is recommended that even public key cryptography with the implementation of a public key infrastructure be used for e-tendering. The assurance of digital signature authentication and non-repudiation outweighs the issues of public key pair generation and storage and certificate revocation. Since e-tendering systems are unlikely to have large user communities these issues can be addressed with little difficulty. It is also recommended that user private keys be stored securely on smartcard devices.

5.2 Access Control

In electronic tendering systems it is important to control access to computer resources to prevent threats such as collusion and internal malfeasance. This is of particular concern when tenders have been submitted to the electronic tender box but the tender has not yet closed. A good access control system combined with cryptographic tools will ensure that only authorised personnel are able to view or edit tender documents. Even system administrators can be prevented from accessing tender documents if not authorised. The access control system on a server can be used to implement a secure tender box by restricting access to submitted tender documents until the close of tender. The access control system is also responsible for maintaining the privacy of submitted documents, ensuring that the identities of the tenderers who have submitted documents are kept confidential. The e-tendering system should carefully specify access control rules that determine which users can access which resources. Information Standard IS18 (QG 2002) enunciates general principles regarding access control rules; more concrete advice is given in ACSI 33 (DSD 2004). It is generally recommended to limit user access on a need-to-know basis, assigning the least amount of privileges required.

Effective access control requires:

- a means of verifying the identities of users requesting access to system resources (user authentication),
- a comprehensive authorisation policy, and
- robust software implementation of the access control logic (software reliability) so that controls cannot be bypassed.

The latter is especially important when protecting against insiders. Trusted operating systems, discussed in Sect. 7.4.2, provide high assurance on the enforcement of access control policies, allowing access control policies that restrict the capabilities of even system administrators.

5.2.1 User Authentication

User authentication is the ability to verify a user's identity. Authentication is often associated with access control systems where the user logs into the computer system. The user announces their identity by providing a username and then authenticates by providing the password. User authentication relies on one or more of the following:

- something the user knows, such as a password,
- something the user has in their possession, such as a credit card or smart card token,
- something the user physically is, such as a fingerprint or DNA.

It is generally recommended to combine several of the above methods for user authentication.

In the e-tendering process user authentication is important to ensure authorised access to tender specification and offer documents on a local machine. Authentication is also important when communicating with other entities. Tenderers must be sure they are communicating with a valid principal and the Principal must be sure they are communicating with pre-qualified Tenderers instead of masquerading entities.

There are many mechanisms that provide authentication. These mechanisms include user passwords, biometrics, challenge response systems, and the use of digital certificates in conjunction with a public key cryptosystem. ISO/IEC 9798:2-5 specifies user authentication mechanisms based on symmetric encryption, digital signatures, hash functions, and zero-knowledge techniques. ACSI 33 (DSD 2004) provides guidelines for password-based user authentication. The mechanism chosen will depend on the level of authentication required. This will be different for different organizations and applications. A formal risk assessment should be performed to determine the level of authentication required for e-tendering applications following best practice[1]. For small tenders a simple user password may be sufficient for authentication. But it is recommended that the use of digital signatures be used for authentication in the e-tendering process as digital signatures also provide non-repudiation of messages.

5.3 Secure Time

The security of an e-tendering system relies crucially on the recording of the date and time at which events occur within the system, as well as on the compliance to agreed timelines. This is particularly important at the close of tender as late tenders may be deemed to be

[1] *The Australian Government Information Management Office is currently working in the specification of an Australian Authentication Framework, which provides guidance on deciding appropriate authentication methods based on a risk management approach. An exposure draft has been published (AGIMO 2004).*

nonconforming (see section 3.1.4). Furthermore, section 24 of the ETQA provides that an electronic communication is received when it enters a designated information system (see section 3.2.4). Therefore, secure time stamp mechanisms that provide evidence as to when a communication is received by the information system is necessary. Section 4.2.5 further discusses the requirement for secure time stamping mechanisms.

A time stamping mechanism associates a date and time to a system event (e.g. the receipt of an electronic document, the opening of the e-tender box). General requirements for time stamps are that they be:

- specified in an unequivocal format, such as Coordinated Universal Time (UTC)[2]; and
- readily available, e.g. stored with the received document.

In this section we investigate existing technical means that can be employed to:

- provide assurance as to the authenticity and integrity of date and time stamps, and
- enforce agreed closing/opening times of e-tender boxes.

We explore different options to tackle the above two goals and discuss their relative strengths and shortcomings. As usual, deciding on any particular mechanism should be based on security risk analysis.

5.3.1 Time integrity

For evidentiary purposes, it is required that electronic communications between actions in the e-tendering system be time stamped and recorded. Similarly, key events within the systems must be logged in records that include the date and time at which the event took place. The evidentiary value of recorded temporal information depends on the technical assurance that derives from both the particular choice of time stamping mechanism and from their correct deployment and maintenance.

Local host time-stamps

The first option for time stamping an event is to generate a log record that includes a description of the event and the time of occurrence as measured by the clock of the local host computer. The reliability of such time stamps depends on the following factors:

1. The accuracy of the clock;
2. The authenticity and integrity of the record.

In order to trust that an event occurred at the time that a log record indicates, one needs assurance that the clock was accurate at the time the event occurred. This assurance can be derived from confidence that the clock was set accurately at some time prior to the event and that the clock had not been reset or tampered with in the period up to the occurrence of the event. In practice, the setting of a computer clock is performed in two ways:

1. either directly by a registered user through operating system functions; or
2. automatically by a protocol being executed in the computer that synchronises the local clock with that of one or more networked computers.

System administrators can configure hosts to restrict which users can modify the local clock. An e-tendering system that relies on local host time stamping should minimise who can change the local clock time. Time synchronisation protocols, such as the popular Network Time Protocol (NTP) (IEFT 1992), designate a particular host as the time server with which other hosts in the same network synchronise their local clocks. It is advisable to use the cryptographic authentication options that are commonly available in these protocols, allowing hosts to cryptographically authenticate the time server.

[2] *See RFC 3339 - Date and Time on the Internet: Timestamps (IETF 2000).*

However, even if the local clock was probably accurate, a log record will not be worthy of trust unless there is assurance that the event actually occurred, implying that the record was correctly generated by the system and not modified afterwards.

Third party based digital time-stamping

A digital time stamping service associates date and time information to electronic documents in a cryptographic manner. Digital time stamping services are usually provided by third parties and, in general terms, work as follows. A user that wants to get a time stamp on a document computes a digest of the document as described in Section 7.1.2. The digest is then sent to the digital time stamping service, which then digitally signs the digest together with the current date and time. The digital time stamp, consisting of the digest, date, time and signature, is returned back to the user. The authenticity of a time stamp so linked to a document can be verified by checking the digital signature on the time stamp and verifying that the digest value in the time stamp coincides with the recomputed digest of the document.

Digital time stamps are commonly used on digitally signed documents. In the e-tendering context, digital time stamps could be used for example to provide receipts to tenderers when they submit a tender document. Having received a tender, the e-tendering application signs the received document using the principal’s private key. It then computes a digest on the signature and sends it to the digital time stamp service, which returns the corresponding time stamp. The e-tendering application relays the time stamp together with the signature to the tenderer. The tenderer is now in possession of very strong evidence that binds the principal to having received the tender.

There already exist standards for digital time stamping (IETF 2001, IETF 2001b) as well as commercial digital time stamping service providers (e.g.: www.digistamp.com, www.e-timestamp.com.au). Digital time stamps provide a high level of assurance with respect to the authenticity and integrity of time stamped documents. However they incur high overhead costs of running or contracting the service. They also presuppose the existence of a public key infrastructure. In the above example of a time stamped tender receipt, the principal signs the tender. To verify time stamped receipts, the tenderer needs the authentic public keys of the principal and the digital time stamp service. If the sender were to provide similar time stamped receipts for documents sent by the principal, tenderers would also need to be registered within the PKI.

Hash Chains

Sometimes the resolution of a legal dispute depends on discerning the order in which events occurred, not necessarily on exactly determining when the events occurred. For example, in the case of e-tendering, it may be necessary to demonstrate the exact order in which a sequence of communications occurred between the principal and a tenderer during the contract negotiation phase. Hash chaining is a cryptographic technique that, in conjunction with digital signatures, can be applied to electronic communications to provide strong evidence about the order in which a series of electronic document exchanges occur. This application of hash chaining was proposed by Du et al. (Du 2004).

5.3.2 Closing/Opening Time of E-tender Box

The closing time for e-tender submission and the opening time of the e-tender box are critical from both a legal and security point of view. No tender submissions should be allowed after the stipulated closing time. In order to mitigate the threat of insider collusions, submitted tenders should not be opened before the established opening time, which must be set to be after submission closing time. There may be situations when deadlines need to be extended in response to extraordinary circumstances, such as when due to technical failure of the e-tendering system tenderers have been unable to submit tenders for a prolonged period. The e-tendering system should ensure that the functionality for extending submission deadlines is only available to authorised parties.

Submission closing time

Two main security issues arise with regard to submission closing time:

- **Late tenders.** The size of the electronic documents that form a tender submission may be of the order of megabytes (MB), the transmission of which could not reasonably be considered instantaneous, especially when employing open networks such as the Internet. Transmitting a document of 1 MB size using a typical dial-up Internet connection of 56 Kbps (kilobits per second) will not take less than 2.5 minutes. Race conditions are likely in e-tendering systems, where tenderers try to submit at times near the submission closing time. This may result in tender documents being in the process of transmission at exactly the closing time. A decision has to be made as to whether such submissions are considered late. If submissions in progress were considered valid, then a maximum period for completion of transmission must be stated.

- **Time synchronisation.** In the case where there are multiple tender boxes, either electronic or physical, a secure way of synchronising the times of these boxes should be in place. Synchronisation of electronic boxes can be achieved using time synchronisation protocols, such as NTP (IETF 1992), which afford high accuracy and cryptographic authentication.

E-tender box opening time

There are a variety of technical mechanisms that can be considered in order to protect the confidentiality of submitted tenders until the pre-accorded opening time. The three relevant mechanisms are:

1. **Ordinary access control mechanisms.** The first option is to rely on the access control policies enforced by the operating system that stores the documents. Such a mechanism would typically allow the e-tendering application to limit access to tender submissions to specific users (e.g. users with the role of evaluator for a given tender). Unfortunately, common operating system access control policies cannot express date and time access conditions; so there is no direct operating system mechanism to disallow access to a set of files prior to a given date and time. To discourage early access the system may rely on audit trails that record document access, including the date and time of access, and the identity of the user. An actual security risk analysis of an e-tendering application is likely to deem inappropriate the reliance on ordinary operating system access control mechanisms and audit trails to protect the e-tender box, for several reasons, including[3]:
   - In practice, it is usually not difficult for an attacker to subvert operating system access control mechanisms to stored data, provided the attacker has physical access to the system.
   - It does not prevent authorised users from accessing tenders before submission closing time; it merely aims to detect and record such access.

2. **Encryption-based access control mechanisms.** Since inside attackers pose the main threat to the security of the e-tender box, the use of encryption appears to be a more suitable mechanism for protecting submitted tenders. As tenders are received, the e-tendering application encrypts them. Even if an insider manages to get access to the submitted tender files, no information will be revealed, except possibly the number of submitted tenders and any other metadata that might have been stored in clear-text form. There are many ways in which encryption can be implemented to protect tenders. Two high-level options are the following:

[3] *This may not be the case when a trusted operating system is employed, see section 5.4.2.*

- **Application-mediated tender opening.** The e-tendering application encrypts and decrypts the tenders, and enforces itself the access control policy. Received tenders are automatically encrypted by the e-tendering application. The corresponding decryption key is only known by the application itself[4]. The e-tender application enforces the access control policy to the submitted tenders: decryption of submitted tenders is only performed after the specified opening date and time, and only to authenticated users. Two ways in which an attacker may try to subvert the access control mechanism in this scenario are: tampering with the source of time, and extracting the decryption key from the application (e.g. reading the key from memory). Protection of the integrity of time sources is discussed in section 5.3.1. Cryptographic tamper-resistant hardware can be used to protect the secrecy of decryption keys so that they are never stored in the computer's main memory, from which it would not be very difficult for a technically sophisticated attacker to extract.

- **Tender opening using public-key cryptography.** Public-key encryption can be used as an alternative approach that does not require the e-tendering application itself to protect the secrecy of decryption keys. The access control policy for a particular tender would identify a public key under which the submitted documents are encrypted by the e-tendering application. Only the parties in possession of the corresponding private key can decrypt the documents. There are well-known cryptographic techniques that allow the distribution of the decryption capability among a group of users, so that decryption requires the cooperation of multiple parties. For example, two system users, the project manager and another designated party, say the e-tendering system administrator, may each have half a share of the private key. In order to open the e-tender box, the system administrator applies their share of the private key to contents of the box, ie. the submitted documents, resulting in a partially decrypted[5] version of the documents. The project manager can then retrieved these partially decrypted documents and complete the decryption by applying their share of the private key. Assurance that the e-tender box is not opened early comes from the trust assumption that at least one of the parties involved in the decryption acts honestly.

5.3.3 Time of receipt of electronic communications

This section considers the issue of determining the time of receipt of an electronically transmitted document from a technical point of view. As discussed in section 3.2.4, establishing the time of receipt of an electronic communication has important legal repercussions. A definition of time-of-receipt for communications that occur as part an e-tendering process must take into account the technical idiosyncrasies of the data communication protocols used. It is envisioned that most e-tendering applications will only use two types of data communications protocols: store-and-forward (e.g. email) and point-to-point connection-oriented (e.g. HTTP).

Email

Email is the typical example of store-and-forward communications. The most common way of sending and receiving email in the Internet involves two different types of software: email servers and email clients. Users compose the email messages using email client software. An email message consists of envelope information (destination address, priority, etc) and the proper message, which itself may include multiple files (attachments). Roughly, the transmission of an email from originator to recipient proceeds as follows. The email client

[4] *As discussed in Sect. <Key Recovery>, however, a key recovery mechanism should be in place to mitigate the danger of becoming locked out from the clear-text data.*

[5] *Note that "partially decrypted" does not mean that partial information about the clear-text data is revealed.*

establishes a connection with an email server and transmits the email. The server stores the email locally. If the client has several messages that need to be delivered these are also sent to the server, which also stores them. The connection between the client and the server is then terminated. The email server processes the queue of stored messages that need delivery in turn. For each email, it reads the recipient email address from the envelope information and finds out the Internet address of the email server that services the addressee. It then establishes a connection with the addressee's email server and negotiates the transmission of the message. If the addressee is not known by the contacted email server, a notice to that effect is sent to the sender's email server and the transmission of the email is aborted. Otherwise the contacted email server accepts the email and stores it in the addressee's mailbox. Sometimes the sender's email server will not be able to immediately establish a connection with the addressee's email server. The sender's email server does not give up and will retry periodically. If after a configured amount of time the connection is not successful the sender's email server will stop further attempts and will send a delivery error message to the sender.

How the addressee reads emails from the mailbox depends on the protocol employed between the addressee's email client software and the email server. There are two main protocols: the Post Office Protocol (POP) and the Internet Message Access Control Protocol (IMAP). With POP, the addressee, through their email client program, logs into the mail server, using a username and password, and downloads all emails stored in their mailbox. Once messages are downloaded, the email server deletes them from the user's mailbox. With IMAP, users manage the email messages directly on the server. Messages are not downloaded and deleted immediately as with POP.

Important points to make with regard to email communications are:

- Email transmission times from originator to addressee's mailbox at the email server vary from fractions of a second to days. Note that the addressee still needs to log into the server to read the email.
- There is no guarantee that email messages will arrive to their destination.
- Internet email does not provide reliable return receipts to communicate to the originator of an email message that the addressee has received it.
- A notice of delivery failure is returned to the originator when the system cannot relay the message to the addressee, informing as to the cause. However, it may take a long time (up to days) before the originator receives the transmission-failure notice.

Point-to-point connection-oriented communications

This corresponds to the most popular method of downloading and uploading data in the Internet, i.e. the Hypertext Transfer Protocol (HTTP) running over the Transport Control Protocol (TCP). Communication here is connection-oriented, meaning that the two end-points interact directly to establish and maintain a communication session. Data is sent in the form of discrete packets of standardised maximum size (64 kilobytes). End-points acknowledge the receipt of packets, allowing the detection and retransmission of lost packets. When the sender does not receive an acknowledgement for a particular packet after a certain amount of time (typically of the order of seconds), it automatically retransmits the packet. When a packet times out repeatedly, the sender concludes that there is a problem and terminates the connection. After all packets are received and acknowledged by the receiver, both sender and receiver exchange special control messages and terminate the connection.

The important points to make with regard to point-to-point connection-oriented communications are:

- Successful establishment of a connection between the two end-points occurs very quickly (order of fractions of a second to a few seconds). The actual transmission time of the data varies depending on its size.
- When transmission fails both end-points are aware of the failure, shortly afterwards (typically within a few seconds).

- The Internet protocols used for downloading and uploading files from and to web servers do not provide any reliable mechanism that could allow a party to prove having sent or received a file, nor the time when it may have happened.

5.4 Recordkeeping

E-tendering systems generate and process electronic documents that are part of business activities and hence need to be preserved as records within a record keeping system in order to comply with relevant legislation and standards, as discussed in section 3.2.7.

A key requirement for recordkeeping is the preservation of the evidentiary integrity of records, both documents and contextual data; this poses a major technical challenge in an electronic environment. Standards Australia HB 171 – Guidelines for the Management of IT Evidence (SA 2003) provides advice on how to maximise the evidentiary weight of electronic records. HB-171 identifies five objectives that must be taken into account in the design of an e-tendering system:

1. ensuring that evidentially significant electronic records are identified, are available and are useable;
2. identifying the author of electronic records;
3. establishing the time and date of creation or alteration;
4. establishing the authenticity of electronic records; and
5. establishing the reliability of computer programs.

The technical aspects of objectives 2, 3, and for 4 have already been discussed in sections 5.1.3 and 5.3, respectively. In the next subsection objectives 1 and 5 are considered.

5.4.1 Identification of evidential information

A detailed assessment of the electronic information within an e-tendering system that has evidentiary value needs to be performed. Such assessment should employ a risk management approach, taking into account the likelihood of a record being used for evidentiary purposes together with the severity of the consequence of the record not being accepted as evidence[6].

A cursory assessment shows that the following e-tendering documents are important evidential material:

- Tenderer document submissions;
- Tender specification and addendums produced by the principal;
- Tender revocation notices submitted by tenderers;
- Negotiation communications post tender close time;
- Request for explanation communications pre-tender close time;
- Award of tender announcement;
- Any receipt of message acknowledgments.

5.4.2 Software reliability

When determining the evidentiary weight of a record, it may be necessary to demonstrate that the software that generated the record was operating correctly. Assuring high levels of reliability of complex information systems is a difficult and expensive engineering task. It requires methodological design and deployment, as well as detailed evaluation. A number of strategies can be taken to enhance the demonstrable reliability of the software in relation to the evidential value of records:

[6] *See Appendix E of HB-171.*

1. Identify and isolate the functionality within the e-tendering system on which the evidential value of the record relies upon. This reduces the complexity of the software, thus making the provision and assessment of assurance more manageable.

2. Use certified products. There exist several security evaluation standards that are used by independent entities to assess the conformance of products to a set of standard security requirements. The two more common evaluation standards are the Information Technology Security Evaluation Criteria (ITSEC) (CEC 1991) and the Common Criteria (CC) (ISO 1999). Both standards define different levels of security testing, resulting in the levels of assurance. In Australia, the Defence Signals Directorate[7] is the only accredited body for issuing certification according to the ITSEC and CC standards.

3. Use trusted operating systems. Trusted operating systems, such as Sun Trusted Solaris of Sun Microsystems Inc., are certified according to ITSEC and CC standards, and provide strong assurance on the operating system access control mechanisms. This allows the protection of programs and data against unauthorised modification. Trusted operating systems can enforce strict security policies that restrict the capabilities of even system administrators.

5.5 System Availability

Availability ensures that computer systems and data are accessible to authorised parties. Availability of the computer system to hold the tender offer documents is essential.

The parameters that affect the availability property are many and varied. There is no specific mechanism or policy which provides this property. The topic of providing availability and preventing denial of service attacks is still the subject of much research.

In the e-tendering process, the availability of the tender box is essential. The reliability of the electronic tender box should exceed that of the physical tender box. One of the major concerns which principals and tenderers have of moving to the e-tendering process is the issue of the electronic tender box not being available at the close of the tender. This section raises two possible issues which may prevent the availability of the e-tendering system. These issues are denial of service attacks and malicious code.

5.5.1 Denial of Service

The electronic tender box may be unavailable for several reasons. There may be an error in network configuration or the tender box server may have hardware problems. These issues, although serious, are different from denial of service attacks. Denial of service attacks are attacks by malicious parties with the aim of preventing legitimate parties from accessing a computing service. Denial of service attacks exploit flaws in server operating systems and in the Transport Control Protocol/Internet Protocol (TCP/IP) communications protocol. The TCP/IP communications protocol is pervasive in all large networks particularly the Internet, so denial of service attacks are relatively easy to conduct and thus are the most common attacks. Needham (Needham 1993) class denial of service attacks into three different types:

1. Attacks on the server. An attacker attempts to prevent the server from accepting normal connections from legitimate users. In the e-tendering process this attack is likely to occur on the tender box server which accepts tender offers from tenderers. The malicious attacker aims to prevent legitimate tenderers from submitting their offers before the close of the tender.

[7] *See http://www.dsd.gov.au/infosec/evaluation_services/aisep_pages/aisep.html*

2. Attacks on the network. An attacker attempts to flood a network, thus preventing communication between servers and clients. This type of attack can affect any part of the e-tendering process. The obvious target is submission of tender offers from tenderers, but other time critical communication can be targeted such as tender inquires and addendums.

3. Attacks on the client. An attacker attempts to interrupt or disrupt a service to a specific client or person. In the case of the e-tendering process, a malicious party will target a specific principal or tenderer.

One of the most common denial of service attacks is the SYN flood attack or simply the SYN attack (CERT 1996). This attack targets the server and exploits a flaw in the connection process, called the Three-Way Handshake. The three-way handshake must exchange three messages between the client and the server before the connection process is completed. An attack is conducted by only sending the first message. The server is stuck waiting for the remaining messages which never arrive.

Another common attack which floods the network is called the Smurf attack (CERT 1998). In this attack, the attacker sends a large amount of ICMP echo messages to the broadcast address of the network and forges a victim's IP address as the source address. The ICMP echo protocol requires a reply message be sent by all recipients of the message. Since the ICMP echo message is sent to the broadcast address all hosts on the network will receive an ICMP echo message. All hosts will send a reply message to the victim's machine. If there are a large amount of computers on the network a large amount of network traffic can be generated and thus the network can be flooded.

The affect of both the SYN flood attack and the Smurf attack can be increased when they are employed as part of a Distributed Denial of Service attack (CERT 1999). This type of attack involves an attacker compromising multiple machines to attack a specific target. A distributed denial of service attack is considerably more effective and more complicated than traditional denial of service attacks as it consists of several simultaneous attacks from several computers.

Denial of service attacks are difficult to prevent because they exploit the communications protocol or the operating system. Thus counter measures require the replacement of the communications protocol or alteration of the operating system. Some countermeasure techniques involve the use of SYN cookies or SYN caches which attempt to provide authentication of clients (Lemon 2002). But these techniques are only effective if attackers require privacy. Other techniques like client puzzles and puzzle auctions (Juels 1999, Wang 2003) require the client to solve puzzles before being connected. These counter measures attempt to slow flooding. The flaw behind these techniques is that both attackers and legitimate users are penalised.

In summary, denial of service attacks are difficult to defend against using current technology. The most common method of defence is to over engineer the server so that it can cope with heavy load. However, in the event that a denial of service attack does occur, it is essential that the terms of tender state whether the principal will accept late tenders due to a denial of service attack.

5.5.2 Malicious Code

Malicious code is any software which purposefully attempts to subvert the anticipated execution of a computer system. The most common form of malicious code are computer viruses that pass on malicious code to other uninfected programs. But there are many other forms of malicious code including logic bombs, trapdoors, Trojan programs, and worms.

Malicious code can be delivered to computer systems using several different methods. The first computer viruses were spread by users copying executable malicious code in the form of applications. Recently, computer viruses have been spread by opening files containing macro viruses (Highland 1989) or by opening email attachments or web downloads with malicious code. Internet worms (Eisenburg 1989) are particularly dangerous as this form of malicious code can spread copies of itself through the Internet without human intervention. Most viruses and malicious code exploit a security weakness in a computer system or network.

Computer systems involved in the e-tendering process will be exposed to the threat of malicious code as tender documents are required to be uploaded and downloaded. E-tendering computer systems are also expected to be connected to the Internet.

The most common countermeasure employed against malicious code is the use of Anti-Virus scanners. Anti-Virus scanners can be executed on user workstations and on network firewalls. These applications scan for files containing a set of virus signature patterns. Files that match the pattern are flagged for deletion or recovery. For anti-virus scanners to be an effective counter measure the database of signature patterns must be updated regularly and the actual anti-virus scan must be executed regularly. In terms of the e-tendering process, anti-virus scanners are less effective. To enhance the security of the e-tendering process many files are encrypted. As well as providing confidentiality to the document, the encryption of the file also hides the virus signature pattern. The solution to this problem is to ensure that all files received by the e-tendering process are scanned after they are decrypted and before they are opened or executed.

Other countermeasures for malicious code include the education of users in proper security techniques. Another countermeasure is the use of firewalls and access control mechanisms to prevent access by remote systems and limit possible actions conducted by malicious code.

As recommended by the Defence Signals Directorate (DSD 2004), all entities in the e-tendering process should employ protective countermeasures against malicious code. In addition, the terms of tender should provide that a document with a malicious code is considered a non-conforming tender.

5.6 File Formats

One of the aspects of the e-tendering process is the fact that it may require the interoperability between several different computer systems. Not all file formats are the same. Some file formats are proprietary but they are very commonly used. Some of these file formats include Word Documents, PDF documents and CAD documents. The disadvantage of these formats is that a proprietary application is usually required to view the file format. Other formats such as the rich text format (rtf) are not proprietary but are easily edited by any number of applications. Proprietary formats are also easily edited by proprietary software.

There are several options available to administrators of e-tendering with respect to file formats. The first is to use a set of accepted file formats for the advertisement and distribution of tender specification documents. This way tenderers and principals will be required to purchase proprietary software to view the documents. But the advantage of this approach is that it will limit the range of file formats. The other option is for principals to specify a particular non-proprietary file format. This can be done by defining or using a previously defined XML standard such as the United Nations XML standard for e-tendering. XML files can be generated from web page input forms or from specifically developed applications or by simply using a text editor.

To prevent the easy manipulation of file contents by malicious parties the integrity of files should be maintained through cryptographic means. A hash or checksum of the file should be made to ensure the integrity of the file. A digitally signed document will also ensure that non-repudiation is maintained. The terms of tender should also specify what file formats are acceptable and that any file submitted in a different format will be a non-conforming tender.

5.7 Summary

Security and legal requirements for e-tendering give rise to a number of important technical issues relating to secure communications, access control techniques, and recordkeeping.

There are well-known standardised cryptographic algorithms and protocols that can be used to communicate securely. The choice of concrete mechanism depends greatly on the levels of authentication required for each type of e-tendering communication, which should be determined from a formal risk analysis. Legal considerations as to the evidential value of electronic communications and contracts would appear to require the provision of cryptographic non-repudiation using electronic signatures.

Technical mechanisms must be put in place to enforce that tenders are not opened before the agreed opening time. This can be achieved cryptographically by distributing the capability of opening (decrypting) tenders among multiple parties, so as to require their joint cooperation. Alternatively, one could rely on operating access control and logging mechanisms, which for common operating systems may not be reasonable given the lack of assurance that they exhibit. Trusted operating systems provide better reliability and should be considered for the implementation of key e-tendering functionality, such as in this case the e-tender box.

Assuring the evidential value of records collected as part of the e-tendering processes presents interesting technical challenges. Information that is considered likely to be used as evidence should be extracted and stored in records in a way that does not affect its evidential integrity. Mechanisms are needed to authenticate the origin of records, and the time and date of recorded events. Cryptographic techniques, such as digital time stamping, and the use of trusted operating systems and other security certified software play an important role.

The terms of tender also need to mirror these technical mechanisms and detail the legal responsibility if these mechanisms were to fail.

6. RECOMMENDATIONS AND CONCLUSION

As e-tendering is a relatively recent concept, governments and businesses are unlikely to immediately abandon the paper tendering system and adopt an e-tendering system where the entire tendering process is conducted electronically, including contract formation. Rather, governments and business are more likely to develop an e-tendering system in phases. The development of any e-tendering system will generally occur in three phases:

1. **Principal to tenderer communication:** This stage of development allows the principal to post the tender advertisement and documents on a website and the tenderers download the tender documents. However, the documents are still submitted in paper. There is no two-way communication occurring in an electronic environment.

2. **Tender submission and two-way communication:** This stage of development is where the tender documents are downloaded from a website and also submitted electronically. There is two-way communication between the principal and tenderer and the distribution of any addendums and negotiation take place electronically. However, the tender is not awarded electronically.

3. **Electronic tendering contract formation:** This stage of development is the same as stage 2 except the tender is awarded and the contract formed electronically.

This section of the report will outline the security and legal requirements at each of these stages. Each stage builds upon the previous stage, so that as each stage is implemented, it is assumed that the security and legal requirements necessary at the previous stage have been satisfied. The recommendations contained in this section address the e-tendering issues considered in section 5.

However, before putting forward any recommendations as to potentially suitable security mechanisms, it is important to note that this research project represents an initial study of the security needs for e-tendering. This report focuses on the security and legal issues peculiar to e-tendering. Prior to the implementation of any effective e-tendering system for a particular business, several major tasks must be undertaken:

- Risk assessment: A formal risk assessment process is needed to elucidate concrete levels of protection. The risk assessment should be organisation-specific and follow appropriate risk assessment methods; in the case of Queensland Government departments best practice guidance is given in (QG 2001).

- Functional security requirement analysis: Based on the results from the risk assessment task, specific mechanisms must be decided upon. The functional security requirement analysis should include the standards, laws and regulations discussed in this report.

- Security assurance requirements analysis: The level of assurance on the correctness of security mechanisms must be determined taking into account the legal and security requirements from the previous two tasks. Assurance may be gained from the evaluation and accreditation of implemented system security functions, following standard methods as indicated in section 5.4.2.

General information systems security principles, in particular those specified by Information Standard IS18, should be implemented in the e-tendering system. There are many aspects of information systems security that have not been covered in this report, but that are crucial, such as security policy development, operational security management, and physical and personnel security.

Basic security precautions must be put in place by the entities involved in the e-tendering process. In particular the following general computer security steps should be applied.

- All installed software applications and operating systems should be correctly patched against known attacks and security vulnerabilities.
- Firewalls should be installed and configured to protect networks and workstations from external attacks.
- System audit logs and other error recording mechanisms should be maintained and monitored regularly by administration staff.
- Anti-virus scanner software should monitor workstations and network traffic for data containing virus signatures. Virus signatures should be updated regularly.

Essential computer systems, such as tender box servers, secure time servers and certificate authorities, should be regularly backed up with secondary servers available to cope with extra load.

6.1 Principal to Tenderer Communication

This stage of development allows the principal to post the tender advertisement and documents on a website and the tenderers download the tender documents. However, the documents are still submitted in paper. There is no two-way communication occurring in an electronic environment.

6.1.1 Security Mechanisms

Secure Communication

The design and security evaluation of cryptographic controls is a highly specialised discipline. The history of information security is full of in-house cryptographic solutions that almost invariably turn out to be insecure. Hence, a general recommendation for secure communication is to only employ reputable standard cryptographic protocols and algorithms to provide secure e-tendering communications.

For web-based applications, the Secure Sockets Layer (SSL) is an effective mechanism to provide integrity and confidentiality to communications. SSL allows a choice of symmetric and asymmetric algorithms to be used within the protocols. Nowadays, a commonly accepted recommendation for business applications would be the use of RSA or DSA with a key length of at least 2048 bits as asymmetric algorithms, and AES or triple DES for symmetric encryption. SSL can protect the confidentiality of tender data being downloaded. In open tenders this is not necessary, but in closed or restricted tenders SSL can be used to protect information while in transit.

SSL provides a secure communication channel between hosts but not users. It allows client hosts to verify the identity of the server host. Authentication of the server host is easily configured and hence, this option should be enabled for electronic tendering. Although SSL can provide message authentication, it does not provide non-repudiation of communicated data. When non-repudiation is needed, this has to be provided by signing the data before it is passed on to SSL for transmission.

Authentication and Non-Repudiation

For closed or restricted tenders, only correctly identified pre-qualified tenderers should be able to view the tender specification or advertisement. The use of a unique username and password to identify pre-qualified tenderers may be sufficient for authentication for this simple e-tendering system. Thus only authenticated tenderers will be allowed to download the tender specification.

A dispute may occur between the tenderer and the principal if the tenderer submits a non-conforming tender submission. The tenderer may claim that it had correctly followed downloaded instructions. The principal should not be able to deny the correct distribution of tender advertisements and addendums.

If an organisation wishes address this possibility, it is recommended that tender advertisements and addendums be digitally signed by the principal. This will provide assurance to tenderers that malicious parties have not tampered with tender specifications. Digital signatures infer the use of a public key infrastructure to distribute the public key of the principal. Notice that only the principal's public key needs to be included in the public key infrastructure which will be considerably simpler to set up than a full authentication framework that also includes tenderers.

6.1.2 Legal Terms and Conditions

Terms necessary to compliment security mechanisms

Legal terms necessary to compliment the stage one security mechanisms include:

1. **Access by Tenderer to documents:** Access control to tender documentation can be used as a method of ensuring authentication of the tenderers and provide a mechanism for tracking and auditing use of the system. Tender conditions related to this issue include:
   - Requiring pre-qualification or at least registration prior to access;
   - Requirement to access through a user name and password;
   - Requirements for maintaining security of access user name and password;
   - Limitation of principal's liability for misuse of username and password.

2. **Authentication of Tenders:** The need for the identity of a tenderer to be certain within an electronic environment is discussed at 3.1.1 and 3.2.1. The use of an electronic medium increases the opportunity and risk of authorised or fraudulent transactions. The conditions of tender should include provision for the identity of a tenderer to be authenticated either through pre-qualification or some other process.

Terms necessary to resolve legal uncertainties

Legal terms necessary to resolve legal uncertainties at this stage of e-tendering development relate to the **status of electronic addendums**. An e-tendering system will allow a increased opportunity to provide additional material to tenderers in the form of addendums to the tender documents. However, the risk of this material never being received or a tenderer failing to collect new information from the site are increased. The conditions of tender should address the status of addendums and the status of a tender submitted without reference to an addendum. A requirement for the tenderer to indicate the material documents and information relied upon when submitting the tender will allow a principal to check that important variations to the requirements for the tender have been included.

6.2 Tender Submission and Two-Way Communication

This stage of development is where the tender documents are downloaded from a website and also submitted electronically. There is two-way communication between the principal and tenderer and the distribution of any addendums and negotiation take place electronically. However, the tender is not awarded electronically.

6.2.1 Security Mechanisms

Secure Communication

In this more advanced e-tendering system, the integrity and confidentiality of most network communication may need to be maintained. In closed or restricted tenders all communication can be kept confidential using SSL or other cryptographic mechanisms.

Secure communications protocols such as SSL only protect data during transmission. In addition to communications security, it is advisable to encrypt sensitive tender documents, such as offers, while stored.

It is advised that HTTP file upload or similar point to point, connection oriented protocol be used rather than email or other store and forward protocols especially when information is not encrypted. This ensures that no non-trusted intermediate parties store data for extended periods of time.

Access Control and Tender Box Simulation

Security mechanisms must enforce that tenders that are submitted electronically are not opened before the opening time. Section 5.3.2 describes several approaches of which tender opening using threshold public-key decryption provides an effective solution. Its security may be considered commensurate to the current common practice of a physical tender box that requires two keys to be opened.

More generally, access control mechanisms are needed within the e-tendering system to restrict access to e-tendering data and applications. Trusted operating systems, with their enhanced assurance on access control mechanisms should be considered for the implementation of key e-tendering functionality, including the e-tender box.

Authentication and Non-Repudiation

In this more advanced e-tendering system, certain communication between the principal and the tenderer may need to be authenticated and non-repudiation for each message provided as they are part of the contract forming process. These documents are:

- Tenderer document submissions;
- Tender specification and addendums produced by the principal;
- Tender revocation notices submitted by tenderers;
- Negotiation communications post tender close time;
- Request for explanation communications pre-tender close time;
- Award of tender announcement;
- Any receipt of message acknowledgments.

Authentication and non-repudiation can be achieved using digital signatures. Digital signatures provide a high degree of assurance as to the authorship of digital data which could be used in a legal dispute. In contrast to the previous e-tendering system, a public key infrastructure is now needed which contains both the principal and the tenderers' public keys; thus increasing the complexity of the system. The issues concerning public key infrastructures are addressed in section 5.1.5.

6.2.2 Evidential Integrity of Electronic Data

Maintaining the evidential integrity of stored documents and contextual data, including audit trails is a complex task. It is particularly difficult given the lack of concrete indications as to what will ensure that electronic data be given strong evidential value in a court of law. Standards Australia HB 171 – Guidelines for the Management of IT Evidence (SA 2003) provides some guidance on maximising the evidentiary weight of electronic records.

All the documents and event logs that are generated within the e-tendering system should be evaluated to determine their potential evidentiary value, using a risk management approach.

This research has identified security mechanisms to enhance the evidentiary weight of electronic records captured within the e-tendering system, including:

- Digital time-stamping, which can be implemented as a trusted third party service, and hash chains (section 5.3.1);
- Trusted operating systems and applications (section 5.4.2);

- Authentication and non-repudiation mechanisms to determine the origin and integrity of records.

Electronic records that are stored in encrypted form should make provisions to satisfy the legal requirement for accessibility to archived documents discussed in sections 3.2.7.

6.2.3 Legal Terms and Conditions

Terms necessary to compliment security mechanisms

Legal terms necessary to compliment stage one security mechanisms include:

1. **Access by Principal to tender submissions/tender box.** Controlling access by the principal to the tender box particularly prior to the closing time of the tender is important for maintaining security and integrity of tender submissions as well as minimising opportunities for collusion and fraud. To ensure this occurs the conditions of tender should include provision for:
   - A prohibition on accessing the e-tender box prior to closing subject to any exceptional circumstances which may necessitate opening by the principal;
   - How the e- tender box will be accessed after closing (ie access control mechanism).

2. **Time of receipt of electronic communications.** The time of receipt of a tender submission, an addendum issued by the principal, a revocation by the tenderer and the time of formation of a contract are all important from a legal perspective. The technical mechanisms for enuring time stamping is reliable are discussed at 7.3. Due to uncertainty in the operation of common law principles and their interaction with the ETQA specific provisions in relation to the time of receipt of particular e-documents or communications should be included in the conditions of tender.

3. **Authority of Agents or Employees.** The authority of agents and employees particularly of corporations to submit tender documents is discussed at 3.2.6. To miminise the risk to the principal where unauthorised tenders are submitted the conditions of tender should include a deeming provision related to authority of agents and employees. In particular where the correct username and password is used to access the e-tender system the tender is deemed submitted with authority.

Terms necessary to resolve legal uncertainties

Legal terms necessary to resolve legal uncertainties in this stage of development include:

1. **Definition of non-conforming tenders.** The issue of non-conforming tenders was discussed at 3.2.3. Within an electronic environment additional opportunities for tenders to fail to conform with requirements exist such as failure to complete all fields of the tender, submission of documents containing viruses or corruption of documents. An expanded definition of the situations in which a tender will be non-conforming should be included within the tender conditions.

2. **Discretion to deal with non-conforming tenders.** The terms of tender will usually contain a discretion for the principal to accept or reject non-conforming tenders. This type of clause should be reviewed to ensure it is adequate to cover non-conforming tenders within an electronic environment.

3. **Consent to use of electronic communication.** The terms of tender should contain a consent by the tenderer to the use of electronic communication for variation, requests for information, negotiation and formation of the ultimate contract. This ensures compliance with provisions of the ETQA and alerts the tenderer to the fact all communication will be electronic.

6.3 Electronic Tendering Contract Formation

This stage of development is the same as the previous stage except that additionally the tender is awarded and the contract formed electronically.

6.3.1 Security Mechanisms

The same security issues and mechanisms such as secure communication, authentication and non-repudiation, access control and evidential integrity are relevant in this electronic tendering system. The risk profile in this electronic tendering system could be quite different. In the previous electronic tendering system, digital signatures were proposed as a technical means to ensure the non-repudiation of pre-contract communications. In this new electronic tendering system, electronic signatures will be needed to ensure the authenticity of an electronic contract. The probability that this authenticity will be brought into dispute is likely to be much higher than that of pre-contract communications. Failing to prove the authenticity of an electronically signed contract may lead to severe consequences. The risk assessment for this electronic tendering system needs to take into account these consequences. High security assurance is likely to be required for digital signature mechanisms; this may be achieved using trusted systems and secure tokens.

6.3.2 Legal Terms and Conditions

Terms necessary to compliment security mechanisms

As the same security issues and mechanisms apply to the electronic tendering contract stage of development, no additional legal terms are necessary, apart from the terms outlined in 6.1.2 and 6.3.2.

Terms necessary to resolve legal uncertainties

Legal terms necessary to resolve legal uncertainties include:

1. **Formation of electronic contract.** If e-tendering systems develop to the next stage of contract formation electronically, the conditions of tender will need to include provisions related to the time at which a contract is formed, the content of the contract, the time at which revocations of the tender submission will be accepted and ideally obligations related to the maintenance of electronic records on both parties.

2. **Right to revoke tender after submission.** The right to revoke a tender after submission should be restricted by the conditions of tender, particularly where formation of the ultimate contract occurs electronically. To ensure commercial certainty to the transaction it may be reasonable to impose a time limitation on the withdrawal of tenders particularly if the process for awarding tenders does not include informal negotiations prior to the formation of a contract. Where informal negotiations are part of the evaluation process the need for limiting the right of revocation may not exist.

6.4 Future Work

This project has identified several areas in both the legal and computer security fields which need future work:

- E-tendering architectures need to be investigated further. An in depth study of the trust relationships is required to recommend the best architecture for a given situation. Additional architectures can also be developed.

- The security mechanisms applied in the e-tendering architectures also need to be developed. Existing threshold and multiple key encryption schemes can be studied for suitability in the e-tendering environment. These types of encryption algorithms will assist in developing more secure tender box applications.

- The rights and liabilities of all persons where trusted third parties are utilised in the tendering process needs to be analysed with a view to drafting appropriate material terms and conditions in agreements between the principal and the trusted third parties and in the conditions of tender.

- Research in the area of secure time is still immature. A timed cryptographic key release protocol is required that will generate a cryptographic key at a particular time. This protocol can be used to ensure that submitted tender documents are only opened after the tender close time.

- Trusted Systems play an important role in ensuring that computer systems remain unaltered and reliable. Trusted systems, including hardware and software, need to be developed to ensure that computer record keeping and auditing are conducted correctly. Trusted systems also need to be developed to provide a suitably reliable access control system for tender box servers.

- Solutions for the long term storage of secure documents need to be developed. This is not only the case for electronic tendering but also for other legal electronic material. The issues in this area include the long term use of storage mediums and the verification of the integrity and confidentiality of archived material.

- A policy for using e-tendering systems for principal administrators, project managers and tenderers needs to be developed.

- Drafting terms of tender for an e-tendering system.

- A simple demonstrator system can be developed to display security techniques and to demonstrate the overall validity of the e-tendering system.

- A detailed analysis of and consideration of possible reforms to the ETQA.

7. REFERENCES

Australian Government Information Management Office (AGIMO) (2004), *Australian Government Electronic Authentication Framework - An Overview for Australian Businesses*, May 2004, available at http://www.agimo.gov.au/__data/assets/file/31772/AGAF_Overview_4__Business.pdf

Australian/New Zealand Standard (AS) (1999), *AS/NZS 4360:1999 – Risk Management*, 1994.

Bishop, M. (2003), Computer Security-Art and Science, Addison-Wesley, Boston, USA

Commission of the European Communities (CEC 1991), ITSEC, *Information Technology Security Evaluation Criteria Version 1.2*, June 1991

Computer Emergency Response Team (CERT) (1996), *SYN Flooding Attack*, 1996, available at http://www.cert.org/advisories/CA-1996-21.html

Computer Emergency Response Team (CERT) (1998), *Smurf Attack*, 1998, available at http://www.cert.org/advisories/CA-98-01.smurf.html.html

Computer Emergency Response Team (CERT) (1999), *Tribe Flood Attack*, 1999, available at http://www.cert.org/advisories/IN-99-07.html

Defence Signals Directorate (DSD) (2004), *Australian Government Information Technology Security Manual (ACSI 33)*, available at http://www.dsd.gov.au/library/infosec/acsi33.html

Du, R., Foo, E., Boyd, C., Fizgerald, B., (2004). *Secure Communication Protocol for Preserving E-Tendering Integrity*, Proc. of Fifth Asia-Pacific Industrial Engineering and Management Systems Conference (APIEMS'2004), Brisbane, Australia, December 12-15, 2004.

Eisenberg, T. D. Hartmanis J,, Holcomb D., Lynn M., and Santoro T. (1989), *The Computer Worm: A Report to the Provost of Cornell University on an Investigation Conducted by the Commission of Preliminary Enquiry*, Cornell University.

Frier A. et al., *The SSL 3.0 Protocol*, Netscape Communications Corp., November 1996.

Highland, H.(1989), *Random Bits and Bytes*, Computers and Security 8(6), p. 460-478.

International Standards Organisation, International Electrotechnical Commission (ISO 1999), *Standard ISO/IEC 15408: Evaluation criteria for information technology*, 1999.

International Standards Organisation, International Electrotechnical Commission (ISO 2004), *Standards ISO/IEC 18014:1-4: Information technology—Security techniques—Time stamping services*, February 2004.

International Standards Organisation, International Electrotechnical Commission (ISO 2004b), *Standards ISO/IEC 117700:1-3: Information technology—Security techniques—Key management services*, February 2004.

Juels, A., Brainard, J., (1999), *Client Puzzles: A Cryptographic Defense Against Connection Depletion Attacks*, In the 1999 Network and Distributed System Security Symposium (NDSS '99), Internet Society Press, p 151-165.

Just M. (1998), *On the Temporal Authentication of Digital Data*, Ph.D. Thesis, Carleton University, 1998, available at http://www.nlc-bnc.ca/obj/s4/f2/dsk2/ftp03/NQ37068.pdf

Lemon, J., (2002), *Resisting SYN flood D0S attacks with a SYN cache*, In the BSDCon 2002, p 89-97.

National Institute of Standards and Technology (NIST) (2000), *Federal Information Processing Standards Publication 186-2: Digital Signature Standard*, January 2000, available at http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf

National Institute of Standards and Technology (NIST) (2001), *Federal Information Processing Standards Publication 197: Advanced Encryption Standard (AES)*, November 2001, available at http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf

National Office for the Information Economy (2002), *Online Authentication - A Guide for Government Managers*, July 2002, available at http://www.agimo.gov.au/__data/assets/file/21171/OnlineGuideFinal.pdf

National Office for the Information Economy (NOIE) (2002), *Online Authentication - A Guide for Government Managers*, available at http://www.agimo.gov.au/__data/assets/file/21171/OnlineGuideFinal.pdf, July 2002

Needham, R. M., (1993), *Denial of Service*, In the 1st ACM conference on Computer and Communications Security, p 151-153.

NSW Department of Commerce (2003). *Welcome to the eTendering System Help Page*, New South Wales Department of Commerce. <https://tenders.nsw.gov.au/commerce/shared/help.cfm?p_page=termsofuse&p_pagetitle=Terms%20of%20Use>

NT Government. (2000), *An Introduction to 'Tenders Online'*, Northern Territory Government, Department of Corporate and Information Services, Contract and Procurement Services.

Queensland Government (QG) (2002), *Information Standard 18 – Information Security (IS 18)*, October 2002.

RSA Laboratories (2002), *PKCS #1 v2.1: RSA Cryptography Standard,* June 2002, available at ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf

Standards Australia (SA) (1994), *Code of tendering,* AS 4120-1994, December 1994.

Standards Australia (SA) (2000), *Electronic funds transfer - Requirements for interfaces ciphers - Data encipherment algorithm 3 (DEA 3) and related techiniques,* AS 2805.5.4-2000, April 2000.

Standards Australia (SA) (2000b), *Electronic funds transfer - Requirements for interfaces - Secure hash functions,* AS 2805.13.3-2000, April 2000.

Standards Australia (SA) (2003), *Guidelines for the Management of IT Evidence,* HB 171 – 2003.

The Internet Engineering Task Force (IETF) (1992), *Network Time Protocol (Version 3) (RFC 1305)*, March 1992, available at http://www.ietf.org/rfc/rfc1305.txt

The Internet Engineering Task Force (IETF) (1999), *The TLS Protocol Version 1.0, (RFC 2246)*, January 1999.

The Internet Engineering Task Force (IETF) (2001), *Internet X.509 Public Key Infrastructure Time Stamp Protocols (TSP) (RFC 3161)*, August 2001, available at http://www.ietf.org/rfc/rfc3161.txt

The Internet Engineering Task Force (IETF) (2001b), *Electronic Signature Formats for long term electronic signatures (RFC 3126)*, September 2001, available at http://www.ietf.org/rfc/rfc3126.txt

The Internet Engineering Task Force (IETF) (2002), *Date and Time on the Internet: Timestamps (RFC 3339)*, July 2002, available at http://www.ietf.org/rfc/rfc3339.txt

Wang, X., Reiter, M. K., (2003), *Defending Against Denial of Service Attacks with Puzzle Auctions*. In the 2003 IEEE Symposium on Security and Privacy (SP'03), p 78-92.

8. AUTHOR BIOGRAPHIES

Professor Ed Dawson

Information Security Research Centre
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 Director of the Information Security Research Centre. 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.

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.

Mr Peter Black, B.A.(Qld), LL.B.(Hons I)(Qld), LL.M.(Columbia)

School of Law
Queensland University of Technology
Ph +61 7 3864 5335, fax +61 7 3864 1161, email p2.black@qut.edu.au

Mr Black is an associate lecturer in the School Law of the Queensland University of Technology. He recently returned from Columbia University in New York, USA, where he was completed his LL.M.

Dr Ernest Foo, B.E. (Hons)(UQ), PhD(QUT).
Information Security Research Centre
Faculty of Information Technology
Queensland University of Technology
Ph +61 7 3864 9554, Fax +61 7 3864 1801, 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 Research Centre. Dr Foo has research interests in the field of electronic commerce, in particular the development of secure protocols.

Ms Rong Du, B.Sc(UNE), M.I.T(QUT),
School of Software Engineering and Data Communication
Queensland University of Technology
Ph +61 7 3864 1930, fax +61 7 3864 1801, email r.du@qut.edu.au

Ms Rong Du is currently a PHD student at Information Security Research Centre (ISRC). Her research area is in Security and Legal Compliance of Electronic Tendering.

Dr Juan González Nieto, B.Sc. (UQ), Grad.Dip.(IT) (QUT), Ph.D. (QUT).
Information Security Research Centre
Faculty of Information Technology
Queensland University of Technology
Ph +61 7 3864 9569, Fax +61 7 3864 1801, email, j.gonzaleznieto@qut.edu.au

Dr González Nieto is a Research Fellow with the Information Security Research Centre. He obtained his doctorate in the field of cryptographic protocols and has research experience in diverse areas of information security, particularly public-key cryptography and protocols.