CRC Construction Innovation
BUILDING OUR FUTURE

Security and Legal Issues in E-tendering

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

Contents

Authors and Contributors

The research described in this publication 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

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.

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 and University of Newcastle.

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).

Two versions of this report are available. The full report cited above is intended for legal, IT and compliance professionals responsible for policy matters concerning e-tendering. This condensed version is intended for procurement personnel who require a sound appreciation of the issues without the accompanying case law and related information.

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;
- Record-keeping 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.

The project also identified several areas in both the legal and computer security fields that need future work.

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). The report evaluated the legal, security and risk issues relating to e-tendering and aimed 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

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 following.

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

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 tenders	Tenderer registration to tender for a project
			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

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. After outlining the current issues for paper-based tendering, this paper highlights the legal issues and requirements emerging from that 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. 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.

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.

The report outlined the common law principles that are present in each of the key steps in the tendering process: pre-qualification and registration, public invitation, tender submission, close of tender, tender evaluation, award of tender, and archiving.

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 contract law governs the tendering process, the various gaps in the law could be remedied by explicit and detailed conditions of tender.

Shifting the tender process away from a paper-based environment to an electronic environment presents additional legal hurdles, even with the existence of the *Electronic Transactions Act 2001* (Qld) (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. The report 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.

4.2 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 can be classified into the following categories:

- Integrity violation
- Confidentiality violations
- Masquerading or impersonation
- Repudiation
- Time integrity violations
- Non-verifiable evidence
- 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 time-stamping 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.

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. These give rise to a number of important technical issues relating to secure communications, access control techniques, and record-keeping.

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. The Development of an E-tendering System

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 project identified these three stages in the development of any e-tendering system:

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.

The project considered the security and legal requirements for each stage. 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.

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.

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 to address this possibility, it is recommended that the principal digitally sign tender advertisements and addendums. 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 complement security mechanisms

Legal terms necessary to complement 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 identity of a tenderer must be certain within an electronic environment. 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 an 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. 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.

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;
- Trusted operating systems and applications;
- 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.

6.2.3 Legal terms and conditions

Terms necessary to complement security mechanisms

Legal terms necessary to complement 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. 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 should be considered. 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.** 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 complement 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 *Checklist for e-tendering development*

The following checklist provides a useful summary of the important issues involved in e-tendering development.

6.4.1 General computer security steps

- Installed software applications and operating systems correctly patched against known attacks and security vulnerabilities ☑
- Firewalls ☑
- System audit logs ☑
- Anti-virus scanner software ☑
- Secondary servers ☑

6.4.2 Stage 1: Principal to tenderer communication

Security mechanisms:

- Secure communication by employing the Secure Sockets Server ☑
- Authentication and non-repudiation by username and password ☑

Legal terms relating to:

- Access by tenderer to documents ☑
- The status of addendums ☑

6.4.3 Stage 2: Tender submission and two-way communication

Security mechanisms:

- Secure communication by using HTTP file upload or similar point to point, connection oriented protocol ☑
- Access control and tender box simulation through threshold public-key decryption ☑
- Authentication and non-repudiation using digital signatures ☑
- Maintaining evidential integrity of electronic data by using digital time-stamping and trusted operating systems and applications ☑

Legal terms relating to:

- Access by principal to tender submissions/tender box ☑
- The time of receipt of electronic communications ☑
- Authority of agents or employees ☑
- A definition of non-conforming tenders ☑
- A discretion to deal with non-conforming tenders ☑
- Consent to use electronic communication ☑

6.4.4 Stage 3: Electronic contract formation

Security mechanisms:

- High security assurance for digital signature mechanisms by using trusted systems and secure tokens ☑

Legal terms relating to:

- Formation of an electronic contract ☑
- The right to revoke a tender after submission ☑

6.5 Future work

The project 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.

This report considers the security and legal issues relating to the shift from a paper-based tendering system to an electronic tendering system. It notes that the law governing tendering raises several legal issues even when the tender process is paper-based. It identifies additional legal and security threats that arise when moving to an open networked environment. The full and condensed versions of the report are 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.

Further information

A copy of the full report can be found in Report 2002-067-A "E-tendering – Security and Legal Issues: Research Report

or by contacting:

Professor Martin Betts
Dean of Faculty of Built Environment & Engineering
Queensland University of Technology
GPO Box 2434
Brisbane Qld 4001
Australia
Phone: +61 7 3864 2415
Email: m.betts@qut.edu.au

QUT

BRISBANE CITY

Queensland Government
Department of Main Roads

Queensland Government
Department of Public Works

The UNIVERSITY of NEWCASTLE
AUSTRALIA