TOWARDS SECURE AND LEGAL E-TENDERING

SUBMITTED: June 2005
REVISED: December 2005
PUBLISHED: April 2006 at http://itcon.org/2006/07/
EDITOR: K. Ruikar

Martin Betts, Dean
Faculty of Built Environment and Engineering, Queensland University of Technology, Australia
email: m.betts@qut.edu.au

Peter Black, Associate Lecturer
School of Law, Queensland University of Technology, Australia
email: p2.black@qut.edu.au

Sharon Christensen, Professor and Deputy Director
Information Security Institute, Queensland University of Technology, Australia
email: s.christensen@qut.edu.au

Ed Dawson, Professor and Director
Information Security Institute, Queensland University of Technology, Australia
email: e.dawson@qut.edu.au

Rong Du, Ph.D. student
Information Security Institute, Queensland University of Technology, Australia
email: r.du@qut.edu.au

William Duncan, Professor
Queensland University of Technology, Australia
email: w.duncan@qut.edu.au

Ernest Foo, Lecturer
Faculty of Information Technology, Queensland University of Technology, Australia
email: e.foo@qut.edu.au

Juan González Nieto, Research Fellow
Information Security Institute, Queensland University of Technology, Australia
email: juanma@qut.edu.au

SUMMARY*: Tendering processes are considered to be a suitable mechanism for governments to fairly assign contracts for construction projects and procurement. The demand for efficiencies to be created in the process has resulted in a significant number of governments implementing e-tendering systems. E-tendering systems generally involve the submission of tender offer documents to a secure system hosted by the government (principal). An electronic environment presents obvious opportunities for collusion between principal and certain tenderers, fraud by tenderers and a minefield of legal uncertainties for fuelling protracted disputes. Critical examination of the security and legal requirements for e-tendering systems does not appear in the current literature. This paper identifies key security and legal issues to be addressed in the design of e-tendering systems, which may be included in e-procurement software, and proposes a new e-tendering architecture, using distributed trusted third parties which may be suitable for secure large scale operations such as the construction industry.*

KEYWORDS: *e-tendering, law, security, authentication, architectures.*

1. INTRODUCTION

Tendering is considered to be one of the fairest means of awarding government contracts and the method most likely to secure a favourable outcome for a government in its spending of public money. The basic principles of the tendering process have been applied to many business areas, such as purchasing goods, seeking service providers, business consulting, or the selection of main contractors for construction work. Although demand from governments and the construction industry for paperless business processes has generated many commercial e-tendering systems around the world these remain largely untested from both a legal and security compliance perspective.

The uncertainty resulting from a lack of sufficient understanding of the legal rules and principles likely to be applied to and electronic tendering systems makes security compliance for an e-tendering system paramount. Inadequate security opens significant opportunities for fraud and collusion by parties inside and outside of the process. These risks can be minimised in part through detailed and specific conditions of tender but these conditions will rely upon effective security mechanisms existing within the system.

Despite the legal hurdles present in the move to an electronic environment few studies appear to have considered the interrelationship between the law and security issues. There have been closely related studies in the field of electronic contracting. Boulmakoul and Salle (Boulmakoul and Salle, 2002) point out that electronic contract negotiation and other e-trading mechanisms must inherently provide some security properties to protect the legal elements of the process. Angelov and Grefen (Angelov and Grefen, 2002) have reviewed frameworks for Business-to-Business Electronic Contracting Support. These studies have not directly addressed security issues unique to e-tendering.

More recently, Du et al (Du et al, 2004a) have defined security services for electronic tendering with consideration for its legal nature. Du et al (Du et al, 2004b) also developed a protocol to preserve e-tendering communication integrity and to protect contractual evidence, but only limited consideration was given to e-tendering security issues.

This paper seeks to identify key security and legal issues to be addressed in the design of secure and legally compliant e-tendering systems. First, general legal and security requirements for a typical e-tendering system will be identified. Secondly, the three stages of development and implementation for an electronic tendering system will be discussed and security and legal issues discussed. Thirdly, an analysis and categorisation of e-tendering architectures will be presented with a proposal for a new type of architecture that provides legal and security compliance. These stages may also have some applicability for other forms of systems, including extranets and e-procurement software.

2. TYPICAL E-TENDERING SYSTEM

While there are a number of e-tender systems available to governments and the construction industry each of the systems generally offers similar communication tools (such as messaging to all parties), document management tools and audit trails. The functionality and process aspects of current e-tendering systems are similar and attempt, at most points, to mirror the legal requirements of a paper tendering system. The main parties in an e-tendering system are the principal and the tenderers. For the purposes of this paper, we have proposed a typical e-tendering process generally engaged in by most systems. The components of the systems will facilitate the process of prequalification or registration, public invitation, tender submission, close of tender, tender evaluation and award of tender. The Table 1 below indicates the detailed steps that would occur within those broad components.

Any e-tender system must ensure that it maintains legal compliance within a secure environment. Before considering the potential architectures for an e-tendering system, it is important to examine the legal and security issues relevant to the several components of an e-tendering process.

TABLE 1: Steps in a typical e-tendering process

Tendering System Component	E-tendering Basic System Function
Pre-qualification & registration	Pre-Qualification Registration
	Issue User Name and Password
Public invitation	Tender Advertisement
	Tenderer Views Tender Advertisement and Notice
Tender submission	Tenderer Registration to Tender for a Project
	Download Tender Document
	Addenda Distributed by Principal
	Tenderer Submits Tender
Close of Tender	Close Tender
	Principal Opens Tender
Tender Evaluation	Tender Evaluation Process
	Request for Information
Award of Tender	Award Tender/Acceptance of Tender
	Sign the Formal Agreement
Archiving	Retention of Document

3. LEGAL REQUIREMENTS

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 will be 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 largely by contract law (as supplemented by constructions protocols or standards in some jurisdictions) many of the various gaps in the law may be remedied by explicit and detailed conditions of tender.

In developing conditions of tender that may fill the various gaps in the law, reference needs to be made to any legislation governing electronic transactions in the relevant jurisdiction. As the *UNCITRAL Model Law on Electronic Commerce* has been adopted worldwide, either in whole or in part in 25 national jurisdictions, it will be used as a guide to the likely legal issues which may arise. The Model Law was designed to give national legislators a set of internationally acceptable rules that would promote the use of electronic communications. The Model Law 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.

Against this background, some of the legal issues that arise in an e-tendering system will be considered.

3.1 Authentication

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. Article 13 of the Model Law addresses the issue of unauthorised electronic communication. In essence, this Article would allow a person to deny the authenticity of an electronic communication sent without their authority. Despite the fact that 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 minimise the potential risk.

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

3.2 Time of 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?

An offer to tender 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.

Article 15(2) of the Model Law is concerned with the time of receipt of data messages:

> Unless otherwise agreed between the originator and the addressee, the time of receipt of a data message is determined as follows:
> (a) If the addressee has designated an information system for the purpose of receiving data messages, receipt occurs:
> (i) At the time when the data message enters the designated information system; or
> (ii) If the data message is sent to an information system of the addressee that is not the designated information system, at the time when the data message is retrieved by the addressee;
> (b) If the addressee has not designated an information system, receipt occurs when the data message enters an information system of the addressee.

The operation of Article 15(2) raises many questions:

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

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

3.3 Award of Tender and Formation of Contract

Although most e-tendering systems do not award the tender electronically and contract electronically, there are several issues that arise in relation to the award of a tender. First, when is a contract formed electronically? Secondly, when can an offer (tender submission) be withdrawn? Thirdly, if the person submitting the tender lacks authority, will that affect the contract? The Model Law does not directly provide for the time of formation of a contract or for the terms of that contract. It is expected that the principles of contract law will need to be modified to fill this gap or that the terms of the tender provide for the timing of formation and the relevant terms of the contract.

3.4 Archiving

Governments and construction companies need to keep and maintain records of the tender process in the event of litigation. This applies to both paper based and electronically formed contracts following the tender process. When these documents are kept and maintained electronically, legal issues arise as to how the contents and integrity of those documents can be proven in court. Article 9 of the Model Law provides:

> 1. In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:
> (a) On the sole ground that it is a data message; or

(b) If it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

2. Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.

This Article gives the court 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, reliable e-tendering systems should include an electronic recording system with features such as audit logs, trusted record keeping, restricted access to transaction software, archived data and preservation of records to add weight to the credibility of data which may have to be later presented in court as evidence.

4. SECURITY REQUIREMENTS

E-tendering security requirements are similar to other electronic commerce systems. There is a need to address the integrity, confidentiality, authentication and non-repudiation in e-tendering communications. This will include an examination of:

- E-tendering needs to provide secure access to critical systems, particularly in the case of the tender box which temporarily stores tender submissions after the tender closing time. Submitted tenders are highly confidential documents, which are always the target for business collusion.
- 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 non-conforming. There are three main areas of concern relating to secure time: Integrity of timestamps, the closing and opening of the e-tender box and the time of receipt of electronic communications.
- 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. A key requirement for secure 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.
- System availability is crucial, particularly during the tender submission stage before the close of tender time.

5. E-TENDERING STAGES OF DEVELOPMENT

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. A significant number of government e-tendering systems in operation in Australia and internationally (such as Hong Kong and Malaysia) have developed e-tendering systems up to the second stage of development.

The first phase involves only 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.

The second phase is 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.

The final phase of implementation would be electronic contract formation and contract administration. This stage of development is the same as the second stage except the tender is awarded and the contract formed electronically with on-going contract administration carried out electronically via collaboration software.

This section of the paper 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.

5.1 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.

5.1.1 Security Mechanisms

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) also known as the TLS protocol (Dierks and Allen, 1999) 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. A commonly accepted practice for business applications is 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 digitally signing the data before it is passed on to SSL for transmission.

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.

To address this possibility, tender advertisements and addendums should 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. Only the principal's public key needs to be included in the public key infrastructure which will be considerably simpler to implement than a full authentication framework that also includes tenderers.

5.1.2 Legal Terms and Conditions

The conditions of tender will need to compliment these security mechanisms and therefore, should relate to the tenderer's access to the documents. Relevant tender conditions include requiring pre-qualification or at least registration prior to access, a requirement that access to the system be through a user name and password, requirements for maintaining security of access user name and password and limiting the principal's liability for misuse of username and password.

Also, as the use of an electronic medium increases the opportunity and risk of unauthorised or fraudulent transactions, the conditions of tender should include provision for the identity of a tenderer to be authenticated either at pre-qualification or some other process.

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.

5.2 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.

5.2.1 Security Mechanisms

As in the Principal to Tenderer Communication stage, the integrity and confidentiality of most network communications must 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.

The main improvement of the Tender Submission and Two-Way Communication stage is that tenderers can upload electronic tender submission documents. HTTP file upload or similar point to point, connection oriented protocol should be used rather than email or other store and forward protocols especially when information is not encrypted. This ensures that non-trusted intermediate parties cannot store data for extended periods of time before being sent to the electronic tender box.

Security mechanisms that simulate the physical tender box must ensure that electronic tender documents cannot be opened before the designated opening time in the tender conditions. The tender box simulation security may be considered equivalent to the current common practice of using a physical tender box that requires two keys to be opened. One approach to simulate this system is to open the electronic tender box using threshold public-key decryption (Shamir, 1979). This encryption system requires multiple cryptographic keys to be used to decrypt an encrypted message.

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.

In this more advanced e-tendering system, certain communications 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 formation 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 (Diffie and Hellman, 1976, ElGamal, 1985, Rivest et al, 1978). 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 Principal to Tenderer Communication stage, a public key infrastructure is now needed which contains both the principal and the tenderers' public keys; thus increasing the complexity of the system.

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 clear indication from the courts as to what mechanisms or processes will ensure that electronic data presented in a court is given strong evidentiary weight.

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.

Several security mechanisms have been identified which should enhance the evidentiary weight of electronic records captured within an e-tendering system, including:

- Digital time-stamping (Haber and Stornetta, 1991, Adams et al, 2001) to provide timestamp integrity, which can be implemented as a trusted third party service, and hash chains;
- Trusted operating systems and applications (ITSEC, 1991, ISO15408, 1999) to provide assurance of system functionality; and
- Digital signature mechanisms to provide authentication and non-repudiation that will determine the origin and integrity of records.

5.2.2 Legal Terms and Conditions

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 a prohibition on accessing the e-tender box prior to closing subject to any exceptional circumstances which may necessitate opening by the principal and how the e- tender box will be accessed after closing (that is, the access control mechanism).

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 the law, provisions specifying the determination of the time of receipt of particular e-documents or communications should be included in the conditions of tender.

In addition to those two legal terms necessary to compliment the security mechanisms, legal terms will be necessary to resolve legal uncertainties introduced by an e-tender system where the tenderer is submitting all documentation electronically. For example, in a paper system the question of what is a non-conforming tender is relatively settled. An electronic environment provides additional situations in which a tender submitted may fail to conform to the requirements of the tender conditions. This may include failure to complete all fields of the tender, submission of documents containing viruses or corruption of documents. To address this an expanded definition of the situations in which a tender will be non-conforming should be included within the tender conditions. In addition, as the terms of tender 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.

Finally, the terms of tender should contain a clause whereby the tenderer consents to the use of electronic communication and agrees to designate an information system (email address) for receipt of electronic communications concerning variations, requests for information, negotiation and formation of the ultimate contract. This ensures compliance with provisions of the Model Law and alerts the tenderer to the fact all communication with the principal will be electronic.

5.3 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.

5.3.1 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.

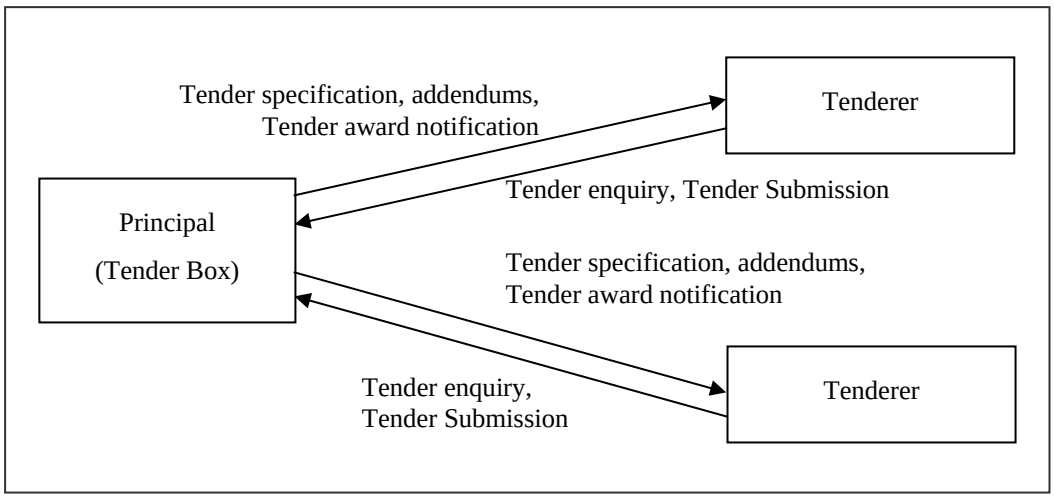

FIG. 1: The Principal Based Architecture

5.3.2 Legal Terms and Conditions

As the same security issues and mechanisms apply to the electronic tendering contract stage of development, no additional legal terms are necessary to compliment the security. However, two legal terms are necessary to resolve legal uncertainties surrounding the formation and content of electronic contracts. First, 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.

Secondly, the conditions of tender should include provisions related to:

- The time at which a contract is formed. This will avoid any disputes concerning the exact time of formation.
- The content of the contract. The terms of the ultimate contract and particularly limitations or exclusions should be clear between the parties.
- The maintenance of electronic records by both parties. This provision should include requirements for maintaining versions of documents and technical requirements for archiving.
- Tracking of access to any collaboration software used by the parties during the contract administration phase and especially the consent of the tenderer to the principal tracking their usage of the system.

6. IMPLEMENTATION ARCHITECTURES

This section introduces and classifies e-tendering system architecture. These architectures have been the result of interviews, system demonstrations and discussions with four government bodies and two international level private companies. This paper describes three possible system architectures for e-tendering:

- Principal based;
- Trusted third party (TTP) based; and
- Distributed TTP architecture (DTTP).

The principal and TTP based architectures have been implemented by many organisations. The DTTP architecture is a new proposal. Each of the e-tendering architectures has the ability to address the issues raised in the Legal and Security Requirements section. It is assumed that trusted operating systems apply suitable mechanisms for access control to simulate the electronic tender box and that suitable measures have been taken to ensure system availability, and record keeping. Secure communication, including authentication and non-repudiation is assumed to be achieved using public key cryptography and a public key infrastructure. Secure time

is provided through a time-stamping secure time server. It is the interaction of participating parties, certificate authorities and time servers that provides the unique advantages and disadvantages in each system.

6.1 Principal Based Architecture

The principal based architecture is mostly used by government e-tendering organisations. The principal based architecture is displayed in Fig. 1. This architecture only requires two types of parties: the principal and the tenderer.

The principal is the main administrator of the tendering process and communicates directly with the tenderers. The principal is responsible for ensuring the authentication of the tenderers. Tenderers usually verify the identity of the principal and all correspondence coming from the principal, including tender specification documents and addenda, using a certificate distributed by the principal. Tenderers submit tender documents directly to the principal. The principal maintains the tender box application and must store all submitted tender documents securely, and ensure that no tender documents are submitted after, or viewed before the designated tender close time. The principal is also responsible for the secure storage and archiving of documents after the tender has been awarded.

This architecture places a great deal of trust in the principal. Tenderers place their trust in the access control system employed by the principal to ensure that collusion or internal malfeasance by the principal's users is difficult. The principal must also develop a scheme for verifying the identity and authenticating documents from the tenderers. To achieve this, it is likely that the principal would run a certificate authority, issue certificates and conduct a cryptographic key generation process with tenderers when they complete the pre-qualification process. The principal is responsible for providing a standard time for the e-tendering process.

In summary the principal based architecture depends on the principal to enforce and maintain the essential e-tendering requirements of non-repudiation and authentication, secure time and secure record keeping.

6.2 Trusted Third Party Based Architecture

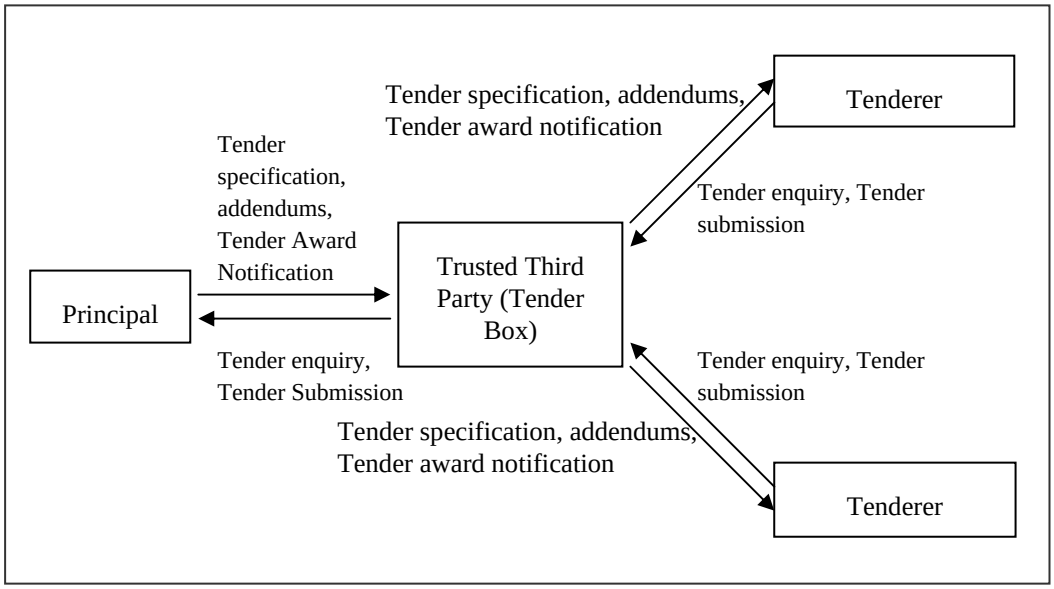

FIG. 2: The Trusted Third Party Based Architecture

The TTP based architecture, seen in Fig. 2 is commonly used by private industry or independent government bodies. Unlike the principal based architecture, the TTP architecture passes all communications between the principal and tenderers through a TTP. The TTP is the main administrator in this architecture. The TTP is responsible for ensuring the authentication of the tenderers and the principal. All tender documents including tender specification documents, addenda and negotiation messages are stored by the TTP. The system is usually implemented using the HTTP protocol with tenderers uploading offer documents to a web site. The principal also uploads tender specifications and addenda to the web site. The TTP maintains the tender box application by controlling who views or downloads the documents. Thus, the TTP will only allow the principal to view tender offers from the tenderer after the tender close time. The

TTP can also act as a messenger so no separate communication between the principal and the tenderer needs to be sent via email. All messages can be verified and authenticated or kept confidential if necessary by the TTP.

Because the TTP holds all documents during the tender process, it is also the TTP's responsibility to secure the storage and archiving of documents after the tender has been awarded.

Like the principal in the principal based architecture, the TTP is responsible for authentication of all parties in the architecture. To enable this, the TTP should act as a certificate authority issuing certificates and cryptographic keys to the principal and tenderers.

The TTP should also act as a secure time server. The principal and tenderers should synchronise their clocks with the time published by the TTP.

Thus, in the TTP based architecture the TTP entity is responsible for enforcing and maintaining the e-tendering requirements of non-repudiation, authentication, secure time and record keeping.

6.3. Distributed Trusted Third Party Architecture

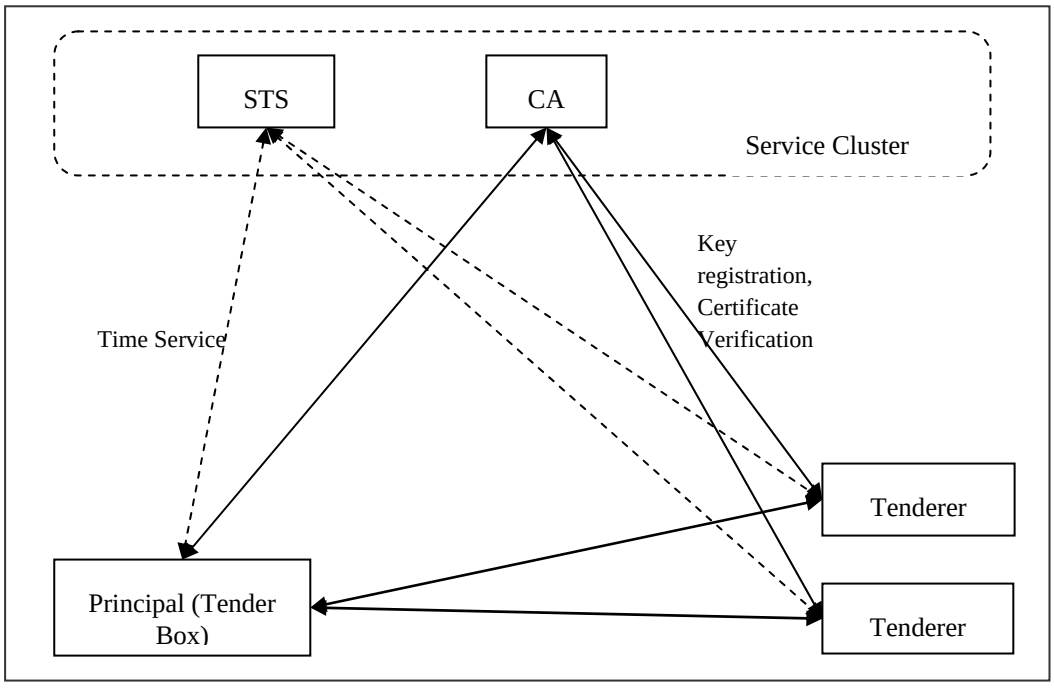

FIG. 3: The Distributed Trusted Third Party Architecture

The DTTP (Fig. 3) uses multiple TTPs to provide security services such as the secure time server (STS) and the certificate authority (CA). The STS performs two functions, time synchronisation and time controlled key release for accessing submitted tenders. The CA has the function of key registration and key verification. These are separate TTPs although both these services may be provided by the same entity. Because of the separation of these roles, this architecture lends itself to a large scale e-tendering implementation.

Unlike the TTP based architecture, the DTTP does not host the e-tender box, but only provides security services to protect e-tendering process integrity. The interaction of parties involved in the DTTP architecture can be described in the following steps.

6.1.1 Pre-qualification and Registration

This 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. The CA will distribute user identities, cryptographic keys and credentials to successful tenderers.

6.1.2 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 are digitally signed and distributed by the principal. Tenderers can use the CA to verify the principal's signature and origin of the message.

During this period, tender document clarification may be required by tenderers. The principal will send addenda and distribute to all tenderers who are participating in tendering for the project. On receiving the addenda, each tenderer will connect to a CA to verify the signature on the addenda to confirm its origin and integrity.

6.1.3 Tender Submission

During this stage the tenderers prepare and submit encrypted 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. Tender submissions should be digitally signed by the tenderer and verified with the CA. The principal must ensure that its clock is synchronised with the STS and that the correct submission time is recorded.

6.1.4 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. The principal will request a key to decrypt the offers from the STS. The STS will only release the key when the tender box is to be opened at or after the tender close time. After the submission deadline, the principal can reject any late or non conforming tenders according to the time-stamping information and tender specification.

6.1.5 Tender Evaluation

During the evaluation, the principal may need to request more information from the tenderer. These messages should be signed and the receiver should verify the message using a CA.

6.1.6 Award of Tender

The principal will accept a tender and send notification to the winning tenderer. It also involves the public announcement of the result. A formal contract can then be signed between the principal and the winning tenderer if it is required. Both the principal and the tenderers will use a CA to verify each other's signatures.

6.1.7 Archiving

Both the tenderers and the principal need to find a secure way to store their documents. The document retention will consider the file format, access, viewing software and integrity verification. In terms of e-tendering requirements, the DTTP architecture differs from the principal based architecture and TTP based architecture. Different entities are responsible for each security requirement. Non-repudiation and authentication are provided by the CA. Secure time is maintained by the STS. The principal is responsible for secure record keeping.

7. ARCHITECTURE ANALYSIS AND DISCUSSION

7.1. Trust between E-Tendering Participants

In a principal based system, tenderers must put their full trust in the principal; therefore the principal has the potential to manipulate the system. For a TTP based system, both tenderers and principals must put their full trust in the TTP, which is the service provider. For example, both principal and tenderers have to trust the third party to store their confidential documents, such as biding strategy. This is an uncomfortable situation for many companies. However, the TTP architecture may reduce the principal's capacity for collusion or internal malfeasance with the system.

A key question is how impartial can the TTP be. The principal is in a position to choose which third party's system to use, and tenderers have no choice. It is obvious that principals will have more favourable relationship with the TTP than any tenderers in the process. The trust in the DTTP architecture is shared and inter-controlled by separate TTPs. It minimises the reliance on one party thus reducing the chance of collusion and single point failure problems. Also, the documents for each tendering project are not stored on a third party system.

CA and STS are specialized security services in controlling of key registration, certificate verification and opening time of submitted tender document. These security functions address security issues discussed in section 2, improve process integrity and increase evidentiary weight of the data stored from an e-tendering process. In the DTTP

architecture, the privilege of controlling these security services has been separated from the parties who host the e-tendering business process, principal or single TTP. Tenderers could have the opportunity to choose the service provider without affecting their ability to tender for a project. The CA and STS in the DTTP architecture are more impartial than the TTP in existing systems.

The use of an impartial TTP as a certificate authority (CA) allows for a more trustworthy authentication and identification system. The implementation of public key infrastructure allows for the user of digital signatures to provide non-repudiation of documents, although this solution is available for all architectures.

An impartial STS allows parties to be sure that the time cannot be changed to suit the principal or a malicious tenderer.

7.1 Scalability

Widespread use of a TTP system for e-tendering would reduce costs significantly over a situation where every principal implemented their own system. A reduction in the number and variety of systems would create cost savings in system development and maintenance, and through standardisation, reduce monitoring and regulation costs to government.

However, as all documents are no longer stored locally (on the principal or tenderer systems), accessing these documents on the TTP system would generate additional traffic over that in the principal based tendering process.

For the DTTP architecture, this design can be easily integrated into current systems for both principal and TTP based architectures. Other security mechanisms can be added on in the future by using more TTPs. Each party can focus on its speciality. The e-tendering business process system can be standardised and developed as universal software for commercial sale. The security services can be developed and modified to suite local legal and security requirements.

8. CONCLUSION

This Article has identified a number of legal and security requirements for the implementation of an e-tendering system. The application of these requirements to three (3) security architectures is considered. The third architecture proposed is a DTTP architecture which may be suitable for large scale operations. The DTTP architecture needs to be investigated in more detail. Specific cryptographic protocols and mechanisms need to be developed to ensure security, particularly secure time issues. Legal aspects of the e-tendering process also need to be given careful consideration in the implementation of an e-tendering system. Contract terms and conditions for e-tendering need to support and compliment security mechanisms, while also resolving any legal uncertainties arising from an electronic environment.

9. REFERENCES

Adams C., Cain P., Pinkas D. and Zuccherato R. (2001). Internet x.509 public key infrastructure time stamp protocols (TSP), *RFC3161*, The Internet Engineering Task Force.

Angelov S. and Grefen P. (2002). A conceptual framework for B2B electronic contracting, *Collaborative Business Ecosystems and Virtual Enterprises - Proceedings 3rd IFIP Working Conference on Infrastructures for Virtual Enterprises*; Sesimbra, Portugal; 143-150.

Boulmakoul A. and Salle M. (2002). Integrated contract management, Proceedings of the 9th Workshop of the HP OpenView University Association Online Conference.

Dierks T. and Allen C. (1999). The TLS protocol version 1.0, RFC 2246, The Internet Engineering Task Force.

Diffie W. and Hellman M. E. (1976). New directions in cryptography, IEEE Transactions on Information Theory, IT-22, 644–654.

Du R., Foo E., Boyd C. and Fitzgerald B. (2004a). Defining security services for electronic tendering, The Australasian Information Security Workshop (AISW2004), Australian Computer Society Inc and ACM.

Du R., Foo E., Boyd C. and Fitzgerald B. (2004b). Secure communication protocol for preserving e-tendering integrity, Fifth Asia-Pacific Industrial Engineering and Management Systems Conference (APIEMS'2004), Asian Pacific Industrial Engineering and Management Society.

ElGamal T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory, 31(4), 469–472.

Haber S. and Stornetta, W. S. (1991). How to time-stamp a digital document, Journal of Cryptology, 3(2), 99–111.

ISO15408 (1999). ISO/IEC 15408 Evaluation criteria for information technology, International Standards Organisation, International Electrotechnical Commission.

ITSEC (1991). Information technology security evaluation criteria (ITSEC), Commission of the European Communities, Version 1.2, Brussells.

Rivest R., Shamir A. and Adleman L. (1978). A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, 21, 120–126.

Shamir A. (1979). How to share a secret, Communications of the ACM, 22, 612–613.