Defining Security Services for Electronic Tendering

Rong Du, Ernest Foo, Colin Boyd, Brian Fitzgerald

Information Security Research Centre (ISRC)
Faculty of Information Technology
Faculty of Law
Queensland University of Technology,
2 George Street, Brisbane, QLD 4001, Australia,
Email: r.du@qut.edu.au,e.foo@qut.edu.au,boyd@isrc.qut.edu.au,bf.fitzgerald@qut.edu.au

Abstract

A major step is required to integrate critical legal requirements into e-tendering system design. The current systems using ad-hoc security mechanisms do not meet the legal requirements for forming a complex electronic contract. This paper analyses the e-tendering process and its legal obligations. The mapping of these obligations to security policies has identified a set of essential security services (mechanisms) for e-tendering systems, with particular emphasis on the contract forming process. These essential security services provide a promising solution for a reliable e-tendering system.

Keywords: Electronic tendering, e-tendering procedure, legal obligations, security policies, security mechanisms, security services, e-commerce, e-contract

1 Introduction

Tendering is a method of entering into a sales contract. It is a long and complex business process and generates a series of contractually related legal liabilities. Substantial construction and engineering contracts are entered into through the tendering process (Thorpe & Bailey 1996). The Australian government has been contracting out multi-billion dollars worth of businesses through the years. It is inevitable that both government and contractors will utilize electronic technology in order to conduct an efficient tendering process.

Maddock Lonie & Chisholm Lawyers (1997) have stated that tendering is a practice involving a complex web of legal issues, which must be known before tendering. The unguarded use of electronic technology in electronic tendering and post-tendering project management has created contradictory effects, such as the trade off between efficiency and security. Shan (2003) in his thesis indicated that people are unsure of the legal impact of using the existing e-tendering project management system. For this reason, industry is reluctant to conduct contracting activities such as tendering process for selecting main contractors, and subcontractors using current e-tendering systems. Another factor contributing to this reluctance, is the ease with which documents can be manipulated electronically, such as copying, deleting, altering, or searching. This further threatens the issues of confidentiality, integrity and copyright.

Business has traditionally incorporated many elaborate procedures into their regular business processes to seek legal protections. E-tendering systems should also include appropriate security mechanisms for increasing the system's reliability.

Fitzgerald & Fitzgerald (2002) point out that electronic commerce solutions are undertaken in the absence of the ability to authenticate people by sight. This immediately creates problems with authenticity and integrity of electronic transactions as trust has been compromised. These threats have undermined the foundation of the admissibility of contract evidence, which consequently affects every step of an e-tendering process.

Improper use of electronic communication systems could also increase the possibility of collusion. Still the most common form of collusion is the leaking of a competing tenderer's information by the principal to its favoured tenderer in the traditional tendering process (The Independent Commissioner Against Corruption 1992, The Independent Commissioner Against Corruption 1991, Thorpe & Bailey 1996). By law, the principal is obliged to conduct a fair and transparent tendering process, which also discourages any collusion activities (*Code of tendering, Australian Standard* 1994). Multiple communication channel usage in the current e-tendering systems can cause untraceable breaches of a document's confidentiality. In this case, the unguarded use of electronic communication is, in fact, providing a basis upon which collusion activities can operate undetected.

The above discussion shows that there is an increasing demand that the legal requirements should be integrated into the e-tendering system design. Modern cryptographic research has developed security mechanisms to safe guard electronic commerce processes, such as e-auction (Peng, Boyd, Dawson & Viswanathan 2003, Viswanathan, Boyd & Dawson 2000), and time stamping (Haber & Stornetta 1991, Buldas, Laud, Lipmaa & Villemson 1998, Une 2001). This has the potential to improve not only efficiency, but also business process security and reliability over that of the traditional system.

Menezes *et al.* (1997) (Menezes, van Oorschot & Vanstone 1997) stated that achieving information security goals in an electronic world, one needs to acquire significant skills and knowledge in technical and legal areas. This also implies that legal issues are a subset of requirements in respect to information security. We, therefore, are obliged to include the legal practice into the electronic commerce protocol design.

Previous cryptographic system designs (Viswanathan et al. 2000, Peng et al. 2003) has followed the defined security properties with little consideration of the legal obligations and liabilities existing in a business process. A technically secure scheme does not necessarily meet the legal requirements. Therefore, a simple add-on cryptographic mechanisms, such as SSL or digital signatures, have never met the legal requirements for forming a complex business contract. For example, the digital signature technology does not possess long term verifiability (Buldas et al. 1998) after key revocation. No current e-tendering system has taken this issue into account, and therefore does not meet the evidence requirements.

Security requirements differ significantly from business to business, due to their particular legal issues and business flows involved. In order to overcome the problems related with ad-hoc systems, we want to make sure that legal issues are a part of security policies, and that security is part of the design of e-tendering. Therefore, defining security properties is the primary step towards a successful design.

The following sections are aimed, firstly, at mapping the e-tendering procedure, and its legal obligation, to security policies; secondly, to suggest security mechanisms which can be used to enforce the security services required.

In section 2, we introduce tendering, then discuss the legal issues involved in electronic tendering. In section 3, we establish e-tendering business flow, and integrate it with the legal issues, to draw up essential security policies and threats for each stage. In section 4, we suggest security mechanisms to protect against potential threats. In section 5, the benefits in using an electronic tendering system will be discussed.

2 Understanding E-tendering and its Legal Nature

2.1 Definition of tendering

Tendering process: an invitation to those relevant parties to make an offer to the principal, which must be capable of accepting the offer, thereby creating a legally binding contract (Atlas, Pitney, Curtis, Greenham, Hanly, Glodstein, Mansfield & Grace 1993, Thorpe & Bailey 1996).

Principal: any party inviting and receiving tenders. A principal may include a contractor or subcontractor (*Code of tendering, Australian Standard* 1994).

Tenderer: any party submitting tenders, including contractor, subcontractor and supplier (*Code of tendering, Australian Standard* 1994).

Tendering is a special way of entering a sale's contract. Its process is designed with consideration of legal contracting requirements, as well as conducting business fairly, and to protect against common collusions. This process is conducive to equity and economy.

Parties involved in tendering are the principal, who runs the tendering, and the tenderer, sometimes called contractor, who makes offers to the principal. For e-tendering systems, a trusted third party may have to be introduced.

2.2 Standard tendering process

A standard tendering process contains the following four stages for selecting main contractors (Working Group 3 1997):

Stage 1: Qualification and compilation of the tender list The principal compiles a preferred tenderers list by assessing each main contractor's technical qualifications and financial ability. The principal also publishes a brief project description to its preferred tenderers, and makes enquiries about their willingness to tender. Contractors who are interested in the project respond with their expression of interest.

Stage 2: Tender invitation and submission The principal publishes detailed contract terms for a project, and sends invitations to all the preferred tenderers in the compiled list. Contractors will submit their offers to the principal.

Stage 3: Tender assessment The principal opens the offer, and assesses each offer against its quality and price. The principal will also perform post-offer open negotiations to consolidate contractual term conditions.

Stage 4: Tender acceptance The principal makes a decision, and awards the contract to the winning tenderer. The principal prepares formal contract evidence to finalise the contracting process.

Based on the standard tendering process, there are other forms of tendering methods which contains similar or less procedures for different types of projects. In the Code of tendering (AS4120-1994) (*Code of tendering, Australian Standard* 1994), the type of tendering is referred to as the tendering method, and it contains: Selected tenders, Open tenders, Preregistered tenders, Invited tenders, and Negotiation.

These types can be considered the valid variations of the standard process and require the same security properties as the standard process. They are designed with the same ethical principles to achieve equity and economy.

Equity provides fair competition, and fair competition achieves optimised economies for the principal calling for tenders. This theory requires transparent processes which are monitored and recorded. The main function of monitoring is to collect evidence, and

to detect collusions. With the evidence, a victim of collusion can seek legal protection.

For example, from the second stage of the standard tendering process, the principal and tenderers are engaged in the contractual process, which is a compulsory procedure to form a final valid contract. Any negotiations that take place between stage two and four can form a collateral contract, and can affect the final outcome (Thorpe & Bailey 1996). Many steps in the tendering process require that they be witnessed and recorded, either for quality control or for legal evidence (Working Group 3 1997).

2.3 The Legal Nature of Tendering

This section discusses major legal areas affecting the electronic tendering process, which create obligations for each party and the design of an electronic tendering system. Obligations define how each party and the system should perform, in an e-tendering process, to either protect against or detect non-ethical behaviour.

Maddock Lonie & Chisholm Lawyers (1997) have listed some major legal areas that have an impact on the e-tendering process, these are Contract Law, Freedom of Information Act, Copyright Act, Trade Practices Act, and Electronic Transaction Act. The obligations defined in the Australian Standards (AS2124-1992, AS4120-1994) are summaries of obligations drawn from many acts that have impacted on the tendering process.

Obligations for one party give rights to the other party. The principal is obliged to run the tendering process with clear and fair procedures. If the tendering process is going to be conducted through electronic tendering system, then the system should meet the requirements of the Electronic Transaction Act. Because the Electronic Transaction Act was enacted after Australia Standards were published, obligations of conducting electronic tendering are not defined by the tendering standard (*Code of tendering, Australian Standard* 1994). Obligations in the tendering process for each party, and obligations that an electronic transaction system should comply with, will be discussed separately in the following subsections.

2.3.1 Obligations for conducting traditional tendering process

Obligations for the principal During the pre-tender stage, the basic obligation for principal is to provide clear project definition and clear tender documents. Pre-tender information (tender documents, tender enquiry, clarification, amendments) should be available to every potential tenderer (*Code of tendering, Australian Standard* 1994).

In the tender invitation and submission stage, the principal should apply conditions for all tenderers equally. All tender inquiries and answers should be made available to all potential tenderers. The principal should choose any of the valid types of tender method and allow sufficient time for the tender process to complete (*Code of tendering, Australian Standard* 1994, Working Group 3 1997).

All submitted documents for tender should be safeguarded with security and confidentiality. The principal should not open submitted tender documents before receiving all submissions or deadlines. It should not disclose any information from one tenderer's documents, to any other tenderer, at any stage of the tendering process, except when publishing the winner's price.

During the assessment period, the principal should apply conditions stated in its tender document equally to all submitted tenderer documents. In post-tender negotiation, the principal should only confirm the contract term conditions, and should not engage in any price cutting activities. All negotiations should be recorded clearly by the principal.

On accepting an offer, evidence of contract should be generated by the principal for the main contractor to sign. Procedures should follow the Australian Standard of General Conditions of Contract (AS 2124-1992), and standard forms for tendering (AS 2125-1992, AS 2127-1992), or any other forms which may be used to finalise the tendering procedure.

Obligations for tenderers Tenderers should only submit their tender within their capacity and competence. They should also evaluate and fully understand the principal's tender documents. If an error exists, the tenderer should advise the principal promptly. They should not engage in any collusion and misleading activities, and should consider confidentiality.

2.3.2 Obligations for implementing an electronic tendering system

Conducting the tendering process through the electronic system, means to perform a contract process electronically. The emplacement of Electronic Transaction regulations around the world (*UNCITRAL Model Law on Electronic Commerce (1996)* 1996, *Directive on a Community framework for electronic signatures* 2000) and Australia (*Electronic Transactions Act 1999, Australia* 2001) has hinted that the enforceability of an electronic contract relies on its evidential weight, and is assessed by the reliability of the manner in which the e-contract is formed.

These regulations have created obligations that require an electronic commerce system provide extra technical assurance, in addition to the obligations that a traditional business should possess.

Boulmakoul and Sall (2002) pointed out that electronic contract negotiation and other e-trading mechanisms must inherently provide some security properties:

- authentication of the participating parties. System should be able to confirm the identity of the contractual participants.
- confidentiality and privacy of contract documents. To ensure that only participating parties should be able to view the content of the electronic contract.
- integrity of contract document. A series of contracting documents should remain complete and unaltered once they have been generated.

- non-repudiation. Contracting parties should not be able to deny their intention to be bound by the contractual agreements.

3 Mapping business requirements to security policies

The tendering process and its legal obligations discussed above, are a particular set of statements which define what is, and what is not, allowed for a sets of actions performed in an e-tendering process. These actions generate a set of time sequenced evidence, including a large subset of contract evidence.

Legally admissible contract evidence is the primary legal protection of parties involved in a multi-million dollar contract process. This section maps the above statements to security policies that an e-tendering system should possess. Therefore, the generation of legally admissible evidence can be ensured in the later design.

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. The e-tendering system security policies define a subset of actions that transform e-tendering system from a secure state to another secure state. Threats and possible violations define the subset of actions that transform the e-tendering system from secure to insecure states. The e-tendering security mechanism is the collection of mechanisms which either prevent the change from a secure to insecure state, or detect and log when this change occurs.

Users in the e-tendering system are the principal, tenderers and trusted third parties. Electronic media are communication media and databases.

The major actions involved in e-tendering are documentation, assessment, document handling and communications. New digital data is generated during the e-tendering process by user interaction with electronic media and digital data.

For example, documentation and assessment generate tender documents, contract terms, assessment results, and documented tendering procedures. Document handling involves document accessing, copying, printing, altering and distribution. These actions can generate the document access log histories for a tendering process. Communication can be subdivided into four types: registration process, contract term condition negotiation, notification/response, submission/notice of receiving, and inquiry/clarification. Communication generates a series of time sequenced messages for a particular e-tendering process.

For electronic tendering system the threats are inherited from two areas, traditional process and the introduction of electronic technology. The security policies and threats are discussed within each tendering stage.

3.1 Qualification and compilation of the tender list stage

The goal for this stage is to generate a final tenderer list for a project from an appropriate approved list. Figure 1 shows the process and parties in this stage of tendering. The horizontal arrows represent the communication between the principal and tenderers. The vertical arrows indicate the business flow steps. The rectangular boxes represent internal activities. The oval boxes represent communication activities. There are three cycles of selection to draw a final tenderer list. The principal compiles a preliminary list from contractor's qualification (technical and financial). After the preliminary query and response, the principal compiles a draft and a reserve tenderer list. According to the final confirmation of the tenderers interest, the principal compiles the final tender list. For electronic tendering, potential tenderers should be requested to make formal registration for tender. This step is to formalise keys and communication functions for continued process.

For example, a principal wants to call a tender for a project to construct a multi-level building block, and chooses to use selected tender method on an electronic tendering system. The principal will search a register of approved prospective tenderers, whose capability has been confirmed. According to their qualification and financial ability, the principal will compile a preliminary list, then prepare a document which briefly describes the project. The principal sends a query to all tenderers in the primary list about their willingness to tender for this project, along with the project description. On receiving the query, the tenderers will send a response to the principal as to their interest in this project.

The principal then compiles a draft tender list and a reserve tender list, which only contains a small number of registrants. If there are withdrawals, the principal will choose replacements from the reserve list, and compile a final tender list. If there are no withdrawals, the principal will finalise the tender list. The principal will then inform those not invited to tender, and request tenderers in the final list to register.

Major documents generated at this stage, include submitted tenderer qualifications, project definition, tender lists compiled by principal and logged information.

From the discussion of legal obligations and business flow, we summarise a set of security polices required for this stage, and threats related to the security policies. Because the security policies are restrictions of parties actions in tendering process, these policies have been further categorised into four action subgroups in Table 1.

The security policies related to communication are as follows: Identify communication parties, record time and date of the message, ensure communication privacy and message original integrity. The common threats are masquerade, repudiation, time repudiation, eavesdropping and integrity violation. The principal needs to make sure that the project description is accurate and avoid any misleading. For the assessment, the rules should be applied to all qualified tenderers fairly without favouring the preferred tenderer. In the document handling, the principal needs to ensure that document integrity, confidentiality and authenticity are provided. All pre-tender information should be available to all potential tenderers instead of the principal's favourite tenderer.

In order to emphasise the importance of security

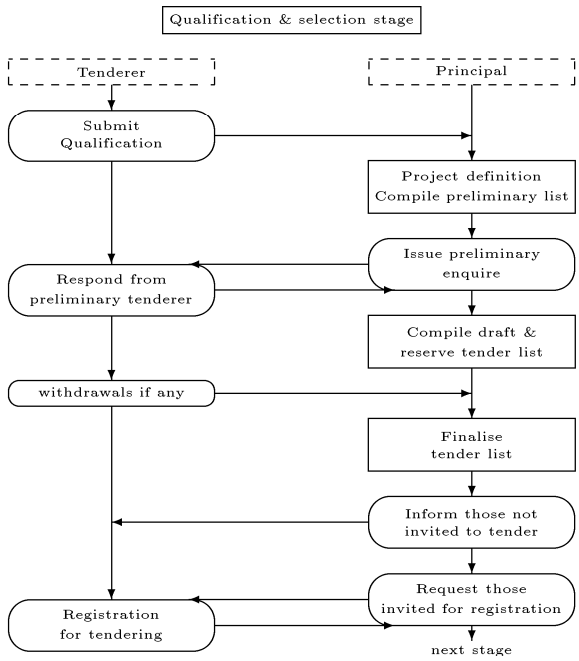

Figure 1: Qualification & selection stage

POLICY	THREAT
Communication:	
Identify communication parties	Masquerade, repudiation
Record time and date	Time repudiation
Ensure communication privacy	Eavesdropping
Ensure message original integrity	Integrity violation
Documentation:	
Project description is accurate	Misleading
Assessment:	
Assessing rules applied equally and fair	Favour preferred tenderer
Tender lists compiled with only qualified tenderers	Favour preferred tenderer
Document handling:	
Ensure same project definition distributed to all tenderers	Favour preferred tenderers
Ensure document integrity	Integrity violation
Ensure digital information authenticity	Masquerade, authorisation violation
Ensure digital information confidentiality	Confidentiality violation

Table 1: Security policy & threats of qualification & selection stage

policies we continue the above example. The principal chooses to use email as the communication method to send/receive inquiries and documents. Unfortunately, a general email system cannot identify communication parties, or ensure communication privacy and integrity. Messages are sent as plain text and sending an impersonated fake email is a trivial exercise. Company B obtains the list of companies that will be invited to tender, and knows that company A in the list is its strongest competitor. It then sends a fake email to notify the principal that company A has withdrawn from the tender process. The result is that company A is removed from the final tender list and the principal believes that company A is accountable for the email containing the withdrawal notification.

When company A discovers the reason, it decides to take the principal to court for fraudulent activity. In the court, company A denies having sent such a withdrawal email to principal. Because the original integrity and sender identity was never calculated and checked, the email can not be publicly verified for its trustworthiness, and then becomes non-admissible evidence in court.

Unreliable communication methods will directly affect admissibility of evidence. It will cause more severe problems in the latter stages of the tendering process.

3.2 Tender invitation and submission stage

This stage is the starting point of the contractual process and every step has to be evidenced and be publicly verifiable. From Figure 2, we can see that the principal should finalise its tender query documents, issue tender invitation, organize pre-tender meetings and clarify any queries made by tenderers. Tenderers should prepare their tender documents and submit within the specified time frame. After submission and deadline, the principal will reject the late tenders, and open and record the submitted tenders.

The major documents generated in this stage contain tender documents prepared by the principal, invitation, minutes of meetings, notes and reports of evaluation committee, queries of tender documents, clarification of tender documents, rejections notes, logged information and tenderer submitted documents. The principal has also added activities to handle these increasing amount of documents.

This is the stage at which the principal and tenderers are engaged in the contract process. Most of the security policies from stage one are carried to this stage to ensure the basic reliability of forming legal admissible contract evidence. The principal also needs to ensure that the digital signature scheme is reliable, the generated contract evidence is long term verifiable, and the tenderer can summit sealed tender documents. These extra policies are to protect against signature repudiation, key revocation and collusions.

We could assume that companies A, B, C and D are invited for tendering. All these companies' email addresses are stored in a list for automatic email sending process. One of the tender board members is a friend of company D, and company B is the strong business competitor to company D. The telephone is still a valid communication channel and its contents are not recorded.

This time the principal has secured its email communication, but the documentation and internal document handling still don't meet the security requirements specified in Table 2. There are still many ways that company D could drive B out of business. The tender documents prepared by the principal are the first set of contract documents in this tender process, but its original integrity is not calculated so the trustworthiness can not be verified later on. There is an amendment of the tender documents prepared by the principal after the inquiry from company C. The friend of company D could delete company B's

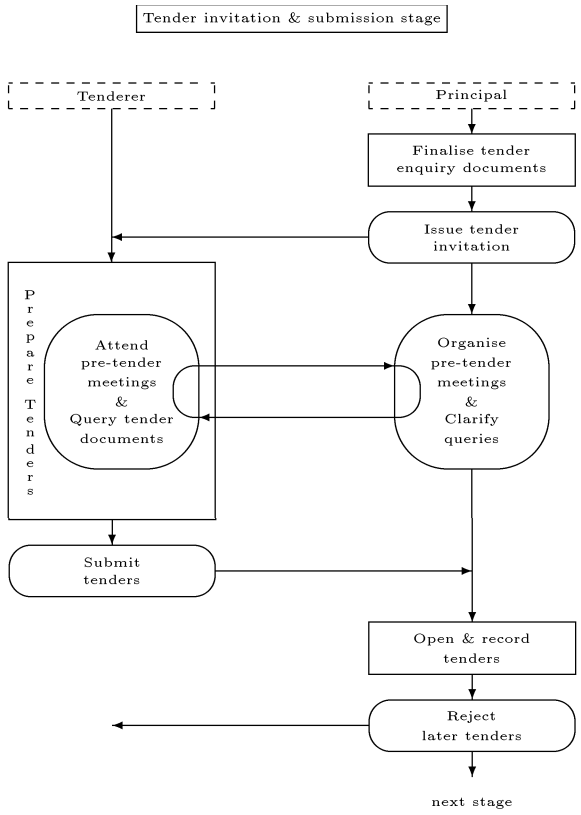

Figure 2: Tender invitation & submission stage

email address from the list without trace. When the board secretary send the emails to tenderers, company B will not receive the notice of inquiry and document amendment. The result is that company B has submitted a non-compliant tender and its tender has been automatically rejected.

Company B later is informed about the amended tender documents from company C, and sues the principal for misconduct, or unfair procedure and for recovery of tendering costs. The principal will have difficulty in providing the evidence of the reliability of its procedures that ensure its documents are properly protected against integrity, authentication, and authorisation violations.

The friend of company D could also disclose company B's price to company D without trace, because the principal did not provide a digital seal submitting service, document access is not logged and telephone communication is not recorded.

The unsecured system is not only unable to provide admissible evidence in court, but also promotes collusion activities.

3.3 Tender assessment stage

At this stage, the principal has the full control of the assessment. In most cases clarification of the contract terms requires post-tender negotiation. It may, in turn, form collateral contracts as well. The strategy is to increase the accountability and transparency with public verifiability. The major activities involved are assessing submitted tender documents, and performing post-tender negotiation.

Figure 3 shows that for assessment, the principal needs to check each tenderer's qualifications, evaluate compliant tenders and their alternative approaches.

POLICY	THREAT
Communication:	
Identify communication parties	Masquerade, repudiation
Record time and date	Time repudiation
Ensure communication privacy	Eavesdropping
Ensure message original integrity	Integrity violation
Reliable digital signing process	Repudiation, non admissible evidence
Documentation:	
Tender documents are accurate and conditions are fair	Misleading
Ensure document's original integrity	Integrity violation
Document handling:	
Ensure tender documents distributed to all tenderers	Favour preferred tenderers
Ensure tender documents are correct and trustworthy	Integrity violation
Ensure digital information authenticity	Masquerade, authorisation violation
Ensure digital information confidentiality	Confidentiality violation
Ensure tender documents, contract evidence, tender process log are long term verifiable	Key revocation
Ensure all invitations are send at the same time	Favourite tenderer get invitation earlier
Ensure all tender document enquires available to all tenderers	Favour preferred tenderers
Ensure all tender clarifications and amendments of tender documents available to all tenderers	Favour preferred tender
Publish enquire anonymously	Mistakes
Tenderer submit sealed tender documents	Collusion, disclose price, violate confidentiality

Table 2: Security policy & threats of tender invitation & submission stage

After assessment, the principal can select a preferred tender, and next preferred tender. For negotiation, the principal should negotiate with the preferred tenderer first. If the negotiation fails, it can then instigate negotiations with the next preferred tenderer. The principal also needs to perform other activities, such as rejecting non-compliant tenders, logging activities for handling digital documents. Documents generated in this stage are rejection notices, evaluation results, recorded negotiations, and other logged information.

As in the last two stages, this stage has to establish the same desired security policies (Table 3). Therefore if somebody challenges the tendering procedure, the principal is able to provide admissible evidence for public verification. For contract negotiation, depending on what has been stated in the tendering documents prepared by the principal, this stage should also be able to assist parties to distinguish different contract negotiation steps such as offer, counter offer and acceptance for each contract term negotiated. Without completing the whole contract negotiation cycle, some terms could be invalid, and liabilities can not be enforced.

The principal may state that the floor covering of a chemistry lab in the building should resist acid spills with two years warranty. The factory only offers one

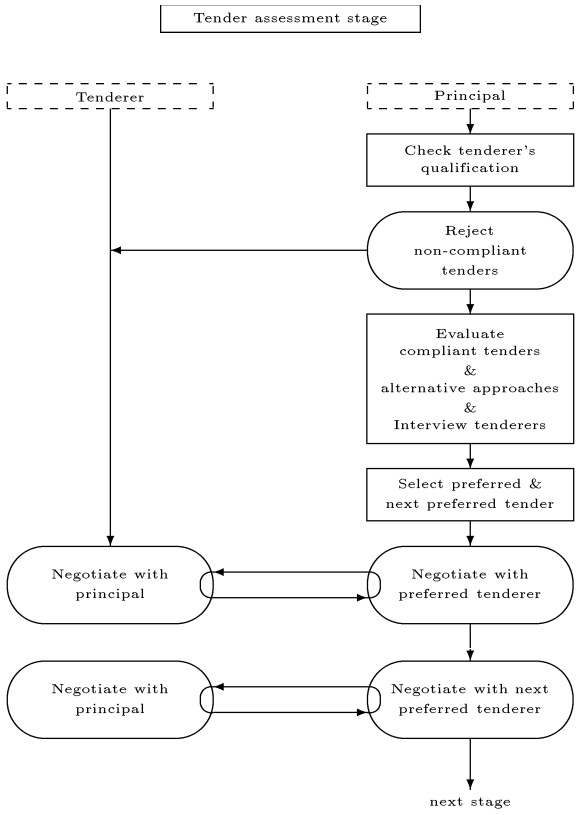

Figure 3: Tender assessment stage

year warranty with their floor covering normally used for this purpose. Therefore, company D only offers a one year warranty. The principal either unconditionally accept D's offer, or puts up counter offer insisting on two years warranty. It is now up to the company D to accept or reject the principal's counter offer. Before a decision can be made by company D, this term can not be consolidated.

3.4 Tender acceptance

This is the final stage of the tendering process, as well as a contracting process for selecting main contractors. Steps involved are, the principal sends formal acceptance to the winner and informs the unsuccessful tenderers. A successful tenderer issues an acknowledgment to the principal on receipt of the acceptance. The principal prepares a formal record of the selection of the successful tenderer, and draws formal contract evidence for both parties to sign using standard forms, if they exist. The business flow has been highlighted in Figure 4.

Documents generated in this stage include formal acceptance notice, notification and briefing of unsuccessful tenders, formal record of tender process, signed contract evidence, and logged activities.

Security policies and common threats for this stage are summarized in Table 4. From Table 4 we can see that this stage needs to possess most of basic security policy stated previously. The main requirement in this stage is to form long term verifiable contract evidence. For example, the principal chooses to use a digital signature to sign the contract evidence with PKI support, the keys of which are revoked within two years. In this example, the floor cover in chemistry lab is an unconsolidated term. The previous stage did

POLICY	THREAT
Communication:	
Identify communication parties	Masquerade, repudiation
Record time and date	Time repudiation
Ensure communication privacy	Eavesdropping
Ensure message original integrity	Integrity violation
Post-tender negotiation only to confirm term conditions	Collusion, price cutting
Contract term negotiation complete full cycle	Contract terms dispute, repudiation
Reliable digital signing process	Repudiation, non admissible evidence
Documentation:	
Formalise each agreed term and sign	Repudiation, dispute
Reliable digital signing process	Repudiation, non admissible evidence
Assessment:	
Applying weighing system equally	Favour preferred tenderer
Compile preferred tender and next preferred tender from complied tenders	Favour preferred tenderer
Document handling:	
Principal open submitted tenders after deadline or when receive all tenders	Violate open rules
Record tender open person, time and witnesses	Violate open rules
No price change is allowed	Integrity violation
Protect unauthorized information (tender designs) disclosure	Violate confidentiality, copy right infringement
Ensure digital information authenticity	Masquerade, authorisation violation
Ensure digital information confidentiality	Confidentiality violation
Ensure submitted tender documents are correct and trustworthy	Integrity violation
Ensure tender documents, contract evidence, tender process report and evidence are long term verifiable	Key revocation

Table 3: Security policy & threats of tender assessment stage

not provide alert to inform this term's condition and final contract drawn up to accept company D's offer. The floor cover in the lab failed after one year in use, and the principal seeks replacement from company D. It took one year for company D to construct the building, and two years had passed when floor cover failed. A dispute could occur, but neither negotiation evidence, nor final contract evidence could be publicly verifiable, due to key revocation or key lost. In this case, there will be no chance of having the floor cover replaced by company D.

4 Essential security mechanisms for electronic tendering

Threats are potential violations of the security properties or polices required for e-tendering. Security mechanisms are the technical tools for enforcing security policies. The previous section discussed essential security requirements for protection against threats. The essential security mechanisms are suggested in Table 5, and they can be used to protect against the major security threats of the e-tendering system.

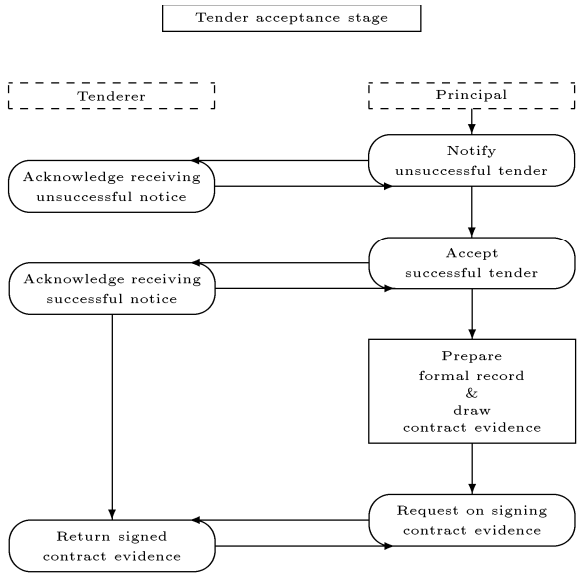

Figure 4: Tender acceptance stage

POLICY	THREAT
Communication:	
Identify communication parties	Masquerade, repudiation
Record time and date	Time repudiation
Ensure communication privacy	Eavesdropping
Ensure message original integrity	Integrity violation
Reliable digital signing process	Repudiation, non admissible evidence
Documentation:	
Prepare formal contract evidence signed by both parties	Repudiation
Prepare formal tender process report with evidence	Procedural dispute, non transparent process
Reliable digital signing process	Repudiation, non admissible evidence
Document handling:	
Ensure contract evidence origin integrity	Masquerade, integrity violation
Ensure tender documents, contract evidence, tender process report and evidence are long term verifiable	Key revocation

Table 4: Security policy & threats of tender acceptance stage

From previous tables we can see that some security requirements, and associated threats, are listed across many tendering stages, and action categories. Such threats include masquerading, eavesdropping, signature repudiation. They form basic threats to the e-tendering system, and require the system to provide more fundamental security services such as authentication, confidentiality, integrity, reliable signature scheme. For example, an eavesdropper could monitor insecure communication and gather valuable information. They could also use compromised secrets to impersonate an authorised person, in order to steal confidential information, or change document integrity.

With the emplacement of these basic security mechanisms, a system can provide more advanced security services, such as secret sharing schemes, to increase the accountability of the tender board, and time chaining contract negotiations and terms. These are also essential for a reliable e-tendering system.

THREATS	SECURITY MECHANISMS
Basic:	
Masquerade	Authentication
Eavesdropping	Confidentiality
Signature repudiation	Reliable signature scheme
Time repudiation	Time stamp
Integrity violation	Integrity
Authorisation violation	Accesses control, security audit trail
Confidentiality violation	Confidentiality, accesses control, security audit trail
Key revocation	Time stamp
Advanced:	
Procedural dispute	Time stamped chained evidence
Contract terms dispute	Time stamped chained terms
Misleading	Accountability
Favour preferred tenderer	Form tender board with shared secret schemes to increase accountability
Non transparent process	Public verifiability
Violate open rules	Sealed bidding scheme, accesses control, security audit trail

Table 5: Common Threats & Essential Security Mechanisms

For example an invalid contract term could occur in any of the following cases: signed person not properly identified, original integrity violated, original integrity not verifiable after key revocation, incorrect time sequence of evidence, or contract process not completed. The first three cases can be prevented by the basic security mechanisms of authentication, reliable signature scheme and time stamp scheme. The last two cases, however, require the introduction of more complex schemes, such as time stamped chain of contract negotiations and consolidated terms.

5 Benefits

The benefit of using an e-tendering system derives from strategically integrating the appropriate security mechanisms to provide the desired security service and efficiency.

The traditional tendering system relies on transparency to achieve equity. Because of the need for confidentiality, the transparency of the tendering process is low. The confidentiality mechanisms can increase the public verifiability of information without revealing the content. The e-tendering system can increase public verifiability to enhance its transparency, thereby achieving greater equity and economy for the principal.

At a practical level, the traditional tendering procedure is vulnerable to abuse (Thorpe & Bailey 1996, Atlas et al. 1993). One common collusion is for the tenderer to induce an insider either to give special consideration to its offer and/or to reveal a competitor's offer. The general practice to guard against this type of collusion, is to use sealed bids and to form a tendering committee or 'tender board'. Many mature cryptographic sealed bid schemes have been developed for e-auction (Peng et al. 2003). They can easily be adapted to suit the e-tendering scheme.

A signature scheme with PKI can ensure evidence origin integrity, but does not detect integrity viola-

tion after the key has been revoked. With combined schemes (checking identification, ensuring that contract process is complete, reliable signature procedure, time-stamp for long term verifiability) the original integrity of contract evidence can be protected and subsequent integrity violation can be detected.

Chained and time-stamped contract terms and its negotiations, and tendering activities will improve the system reliability, reduce disputes, and increase individual accountability. This can be designed to automatically generate legally admissible time sequenced evidence for formal report writing, and to draw up formal contract evidence.

Access control and security audit trails increase system security for accountability. E-tendering systems can also formalise the tendering process to overcome staff discipline problems, and reduce human errors.

6 Conclusions

A simple ad-hoc cryptographic block will not eliminate the possible threats existing in the e-tendering system, and will not meet legal requirements for the contracting process. The security policies have to be drawn up with the consideration of both the tendering business and its legal obligations, to ensure the designed system can generate legally admissible evidence.

The security mechanisms have to be carefully integrated into the system to provide desirable security service for the complex contract processes involved in an e-tendering system. This integration has the potential to not only improve efficiency, but also business process security and reliability over that of the traditional system.

References

Atlas, I., Pitney, A., Curtis, J., Greenham, P., Hanly, G., Glodstein, D., Mansfield, J. & Grace, T., eds (1993), *The Tendering Process*, Blec Business Law Education Centre from the training division of Longman Cheshire.

Boulmakoul, A. & Sall, M. (2002), Integrated contract management, *in* 'Proceedings of the 9th Workshop of the HP OpenView University Association Online conference'. http://www.hpovua.org /PUBLICATIONS/PROCEEDINGS /9_HPOVUAWS/Paper_4_1.pdf.

Buldas, A., Laud, P., Lipmaa, H. & Villemson, J. (1998), Time-stamping with Binary Linking Schemes, *in* H. Krawczyk, ed., 'Advances on Cryptology — CRYPTO '98', Vol. 1462 of *Lecture Notes in Computer Science*, Springer-Verlag, Santa Barbara, USA, pp. 486–501.

Code of tendering, Australian Standard (1994), Prepared by Standards Australia Committee on Construction Industry Practice, published by Standards Association of Australia, 1 the Crescent, Homebush, NSW 2140. AS 4120, 1994.

Directive on a Community framework for electronic signatures (2000), EN Official journal of the European Communities 19.1.2000 L 13/12. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999.

Electronic Transactions Act 1999, Australia (2001), Prepared by the Office of Legislative Drafting, Attorney-General's Department, Canberra. Act No. 162 of 1999.

Fitzgerald, B. & Fitzgerald, A., eds (2002), *Cyberlaw, Cases and Materials on the Internet, Digital Intellectual Property and Electronic Commerce*, Butterworths LexisNexis.

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

Maddock Lonie & Chisholm Lawyers (1997), *Solving the Tendering Puzzle, Competitive tendering in Australia*, Tender support services Pty. Ltd, The business manager, Tender support services Pty. Ltd., P.O.Box 236, Abbotsford Vic 3067, chapter The Legal Nature of Tendering.

Menezes, A., van Oorschot, P. & Vanstone, S. (1997), *Handbook of Applied Cryptography*, Chapter One page 4, CRC Press, CRC LLC, 2000 Corporate Blvd., N.W., Boca Raton, Florida 33431.

Peng, K., Boyd, C., Dawson, E. & Viswanathan, K. (2003), Five sealed-bid auction models, Springer-Verlag, Berlin. To appear in the proceedings of Australia Workshop of Information Security 2003.

Shan, L. K. (2003), Case Study of Application of E-Project Management System for Construction Industry in Hong Kong, Bsc (hons) in building engineering and management, Department of Building and Real Estate, The Hong Kong Polytechnic University.

The Independent Commissioner Against Corruption (1991), 'Report on investigation into tendering for vinyl floor products', Box 500 GPO Sydney 2001, DX 557, CNR Cleveland & George Streets Redfern NSW 2016.

The Independent Commissioner Against Corruption (1992), 'Report on investigation into the sydney water board and sludge tendering ICAC', This Report results from an investigation and hearing conducted in late 1991 and early 1992 by Miss Margaret Beazley AC, Box 500 GPO Sydney 2001, DX 557, CNR Cleveland & George Streets Redfern NSW 2016.

Thorpe, C. & Bailey, J. (1996), *Commercial contracts, A practical guide to deals, contracts, agreements and promises*, Woodhead, Cambridge England.

UNCITRAL Model Law on Electronic Commerce (1996) (1996), prepared by the United Nations Commission on International Trade Law (UNCITRAL).

Une, M. (2001), The security evaluation of time stamping schemes: The present situation and studies, *in* 'IMES Institute for Monetary and Economic Studies', number No.2001-E-18 *in* 'IMES Discussion Paper Series', Bank of Japan, C.P.O BOX 203 Tokyo 100-8630 Japan.

Viswanathan, K., Boyd, C. & Dawson, E. (2000), A three phased schema for sealed bid auction system design, *in* 'Information Security and Privacy, 5th Australasian Conference, ACISP'2000', Springer-Verlag, Berlin, pp. 412–426. Lecture Notes in Computer Science 1841.

Working Group 3 (1997), *Code of Practice for the Selection of Main Contractors*, Construction Industry Board.