Designing Secure E-Tendering Systems*

Rong Du, Ernest Foo, Juan González Nieto, and Colin Boyd

Information Security Institute (ISI)
{r.du, e.foo, j.gonzaleznieto, c.boyd}@qut.edu.au

Abstract. Security requirements for e-tendering systems have not been closely scrutinised in the literature. This paper identifies key issues to be addressed in the design of secure e-tendering systems. In particular, the issues of secure timing and record keeping are raised. This paper also classifies existing e-tendering system designs by presenting common e-tendering architectures. A new e-tendering architecture, using distributed trusted third parties is proposed which may be suitable for secure large scale operations.

1 Introduction

Tendering has been seen as 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. The demand of the electronic environment for business processes has generated many e-tendering systems around the world with untested legal and security compliance.

The main parties in an e-tendering system are the principal and the tenderers. For this paper we consider that the e-tendering process to be conducted as following. Various tenderers will be pre-qualified and registered by a principal. The principal then advertises or issues a public invitation to qualified tenderers. Qualified tenderers make offers or tender submissions to the principal before a specfied tender closing time. Some time after the tender closing time, the tender submissions are opened and non-conforming tenders are rejected. The principal then performs tender evaluation and selects the winner of the tender. The parties can then form a contract and archive documents that are related to this tender process.

An investigation of e-tendering systems is important as the process is inherently linked to legal proceedures. A legally binding contract is the product of the e-tendering process. The amount of money and resources involved in many tendered projects may tempt insiders to collude. Ensuring the security of the e-tendering process is paramount.

* This research was supported by the Construction Innovation Cooperative Research Centre project CRC2002-067-A.

S. Katsikas, J. López, G. Pernul (Eds.): TrustBus 2005, LNCS 3592, pp. 70–79, 2005.

Few papers concerning the security of e-tendering systems have been published, although international organisations have been standardizing e-tendering business processes and message formats through ebXML standards. The United Nations is developing an E-Tendering ebXML Standard. The Business Requirement Specification of E-Tendering [1]. eLEGAL [2] was another research project within the European Information Society Technologies program. eLEGAL targeted the contractual process in the construction industry; and attempted to develop some ebXML standards for legal elements.

More recently, Du et. al [3], have defined security services for electronic tendering with consideration for its legal nature. Du et. al [4] have also developed a protocol to preserve e-tendering communication integrity and to protecting contractual evidence. However, only limited e-tendering security issues have been addressed by them.

The contribution of this paper is to identify key issues to be addressed in the design of secure e-tendering systems. This paper also classifies existing e-tendering system designs by presenting common e-tendering architectures. A new e-tendering architecture is proposed.

The next section of this paper will identify e-tendering security requirements. Next e-tendering systems are studied and classified into system architectures. A short discussion then follows analysing the e-tendering architectures.

2 E-Tendering Security Requirements

Some 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.

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.

System availability is crucial, particularly during the tender submission stage before the close of tender time.

However, we believe the most important security requirements that are relevant to e-tendering are those that are dependent on legal requirements. These requirements provide mechanisms that may be called on to provide evidence in the case of litigation. Specifically, these e-tendering requirements are non-repudiation and authentication, secure time, and record keeping. These will be discussed in detail in the following subsections.

2.1 Non-repudiation and Authentication

Non-repudiation property, in a technical sense, is proof or evidence that a particular action has taken place. The algorithm for non-repudiation can also be an extension of the authentication process. It provides a defence against denial of their actions by a participating party.

Non-repudiation is critical in most electronic commerce applications. In the e-tendering process, non-repudiation is required to provide reliable evidence to prove that the principal has advertised the tender specification documents or awarded the winning tender. Non-repudiation should also be used to prove that an authorised pre-qualified tenderer has submitted a particular tender offer document.

Non-repudiation property is usually implemented through the use of a digitally signed message. Digitally signed messages are often as legally binding as traditional signatures. Public key cryptography enables the use of digital signatures. In an e-tendering system, the digital signature mechanism [5,6,7], can provide authentication and non-repudiation. E-Tendering system design should include a public key infrastructure to support a digital signature mechanism.

2.2 Secure Time

The security of an e-tendering system relies crucially on the recording of the date and time at which events occur within the system, as well as on the compliance to agreed timelines. This is particularly important at the close of tender as late tenders may be deemed to be nonconforming. There are three main areas of concern relating to secure time: Time integrity, the closing and opening of the e-tender box and the time of receipt of electronic communications.

Time Integrity. In e-tendering, it is important for litigation to estabish when key events occur. The integrity of timestamps for the e-tendering process can be provided by a time stamping mechanism [8,9], which associates a date and time to a system event. An example of this event is the receipt of an electronic document or the opening of the e-tender box. The evidentiary value of recorded temporal information depends on the technical assurance that derives from both the particular choice of time stamping mechanism and from their correct deployment and maintenance.

The first option for time stamping an event is to generate a log record that includes a description of the event and the time of occurrence as measured by the clock of the local host computer. A second option involves using a digital time stamping service that associates date and time information to electronic documents in a cryptographic manner. Digital time stamping services are usually provided by third parties. The third party digital time-stamping provides a high level of assurance with respect to the authenticity and integrity of time stamped documents. However they incur high overhead costs of running or contracting the service. They also presuppose the existence of a public key infrastructure. There already exist standards for digital time stamping [10,11] as well as commercial digital time stamping service providers [1].

Closing/Opening Time of E-Tender Box. The closing time for e-tender submission and the opening time of the e-tender box are critical from both a

[1] http://www.digistamp.co and www.e-timestamp.com.au

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

A submission closing time and a reasonable transmission time frame need to be clearly stated in tender specification. A tender submission should be initiated before the closing time and completed within this reasonable time frame. A time synchronisation mechanism needs to be in place. Sometimes there are multiple tender boxes, both electronic or physical. Synchronisation of electronic boxes can be achieved using time synchronisation protocols, such as NTP [12], which afford high accuracy and cryptographic authentication.

For the control of e-tender box opening time, there are a variety of technical mechanisms that can be considered in order to protect the confidentiality of submitted tenders until the pre-accorded opening time. There are two types relevant mechanisms, ordinary access control mechanisms and encryption-based access control mechanisms.

Ordinary access control mechanisms rely on the access control policies enforced by the operating system that stores the documents. Such a mechanism would typically allow the e-tendering application to limit access to tender submissions to specific users (e.g. users with the role of evaluator for a given tender). Unfortunately, it does not prevent authorised users from accessing tenders before submission closing time; it merely aims to detect and record such access.

Encryption-based access control mechanisms protect against the main security threat posed by inside attackers to the e-tender box. The use of encryption appears to be a more suitable mechanism for protecting submitted tenders. The tender/offer will be encrypted and stored as encrypted before opening time. Even if an insider manages to get access to the submitted tender files, no information will be revealed. The control of decryption key releasing time can be achieved by many technologies such as time vault service [13] using pairing based encryption.

Time of Receipt of Electronic Communications. From a legal point of view, in case of litigation, it is important to know when a communication was recieved by the system. A clear definition of time-of-receipt for communications that occur as part an e-tendering process is required. For email based communication clarification of time of receipt is required as there may be a delay between when the message is sent and when the receiver reads the message. When using slow communication links there needs to be clarification as to whether time of receipt should be recorded at the beginning of the file transfer or whether the time of receipt should be recorded when the file transfer is complete.

2.3 Secure Record-Keeping

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 legal requirement for recordkeeping is the preservation of the evidentiary integrity of records, both documents and contextual data; this poses a major technical challenge in an electronic environment.

To maximise the evidentiary weight of electronic records, the e-tendering system needs to ensure that evidentially significant electronic records are identified, are available and are usable; identify the author of electronic records; establish the time and date of creation or alteration; establish the authenticity of electronic records; and establish the reliability of computer programs.

A detailed assessment of the electronic information within an e-tendering system that has evidentiary value needs to be performed. Such assessment should employ a risk management approach, taking into account the likelihood of a record being used for evidentiary purposes together with the severity of the consequence of the record not being accepted as evidence. The following e-tendering documents are important evidential material: tenderer document submissions; tender specification and addenda 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; and any receipt of message acknowledgments.

When determining the evidentiary weight of a record, it may be necessary to demonstrate that the software that generated the record was operating correctly. Assuring high levels of reliability of complex information systems is a difficult and expensive engineering task. It requires methodological design and deployment, as well as detailed evaluation. A number of strategies can be taken to enhance the demonstrable reliability of the software in relation to the evidential value of records. The first strategy involves identifying and isolating the functionality within the e-tendering system on which the evidential value of the record relies upon. Another strategy involves using certified products which are assessed by an accredited body according to the existing security evaluation standards [14,15]. Finally , the use of trusted operating systems, such as Sun Trusted Solaris of Sun Microsystems Inc. [2], that provide strong assurance of the operating system's access control mechanisms.

3 E-Tendering System 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. E-tendering web sites were also studied for systems in Australia, China

[2] http://www.sun.com/software/security/blueprints/

HongKong , Japan , UK and the US . This paper describes three possible system architectures for e-tendering; principal based, trusted third party (TTP) based and distributed TTP architecture. The principal and TTP based architectures have been implemented by many organisations. The distributed TTP architecture is our new proposal.

Each of the e-tendering architectures has the ability to address the issues raised in the previous 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.

3.1 Principal Based Architecture

The principal based architecture is mostly used by government e-tendering organisations. 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.

3.2 Trusted Third Party Based Architecture

The TTP based architecture 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 th e! 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.

3.3 Distributed Trusted Third Party Architecture

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

Pre-qualification and Registration stage of the e-tendering process requires potential tenderers to submit a registration form to the principal for qualification assessment. The principal will assess each registration and issue pre-qualification status for each qualified potential tenderer to access the e-

tendering system. This status is usually based on the ability of the potential tenderer. The CA will distribute user identities, cryptographic keys and credentials to successful tenderers.

Public Invitation 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.

During **Tender Submission** 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.

Close of Tender 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.

During the **Tender 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.

In **Award of Tender** stage, 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.

For **Archiving**, both 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 distributed TTP 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.

4 Architecture Analysis and Discussion

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 of 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 are forced to go along with the decision. It is obvious that principals will have more favourable relationship with the TTP than any tenderers in the process.

The trust in the distributed TTP 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 evidential weight in e-tendering process. In the distributed TTP 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 distributed TTP 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.

The distributed TTP architecture 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 modifed to suite local legal and security requirements.

5 Conclusion

This paper identifies security requirements and classfies security archtectures for e-tendering. It also proposes a high level overview of a distributed TTP architecture for e-tendering sytems which may be suitable for large scale operations. The distributed TTP architecture needs to be investigated in more detail. Specific cryptographic protocols and mechanisms need to be developed to ensure security, particularly secure time issues. In addition, the legal aspect of the e-tendering

process needs to be addressed. Contract terms and conditions for e-tendering need to be developed that will support security mechanisms.

References

1. UN/CEFACT-tbg6: Electronic Tendering International Standardization - Business Requirement Specification. Technical Report ETP020 6.0, UN/CEFACT, http://www.etendering-tbg6.net/doc_specification_01.html (2005)
2. Carter, C., Hassan, T., Mangini, M., Valikangas, P., Ott, E.: User Requirements for Legal Support. Technical Report IST-1999-20570, Information Society Technology-European Community, http://cic.vtt.fi/projects/elegal/public.html (2001)
3. Du, R., Foo, E., Boyd, C., Fitzgerald, B.: Defining security services for electronic tendering. In: The Australasian Information Security Workshop (AISW2004). Volume 32., Australian Computer Society Inc and ACM (2004) 43–52
4. Du, R., Foo, E., Boyd, C., Fitzgerald, B.: Secure communication protocol for preserving e-tendering integrity. In: Fifth Asia-Pacific Industrial Engineering and Management Systems Conference (APIEMS'2004). Volume 14., Asian Pacific Industrial Engineering and Management Society (2004) 16.1–16.15
5. Diffie, W., Hellman, M.E.: New directions in cryptography. IEEE Transactions on Information Theory **IT-22** (1976) 644–654
6. ElGamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory **31(4)** (1985) 469–472
7. Rivest, R., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM **21** (1978) 120–126
8. Haber, S., Stornetta, W.S.: How to time-stamp a digital document. Journal of Cryptology **3(2)** (1991) 99–111
9. Buldas, A., Laud, P., Lipmaa, H., Villemson, J.: Time-stamping with Binary Linking Schemes. In Krawczyk, H., ed.: Advances on Cryptology — CRYPTO '98. Volume 1462 of Lecture Notes in Computer Science., Santa Barbara, USA, Springer-Verlag (1998) 486–501
10. The Internet Engineering Task Force: Internet x.509 public key infrastructure time stamp protocols (tsp) (rfc 3161). http://www.ietf.org/rfc/rfc3161.txt (2001)
11. The Internet Engineering Task Force: Electronic signature formats for long term electronic signatures (rfc 3126). http://www.ietf.org/rfc/rfc3126.txt (2001)
12. The Internet Engineering Task Force: Network time protocol (version 3) (rfc 1305). http://www.ietf.org/rfc/rfc1305.txt (1992)
13. Casassa, M., Harrison, K., Sadler, M.: The HP time vault service: exploiting IBE for timed release of confidential information. In: Proceedings of the twelfth international conference on World Wide Web, May 2004, Budapest, Hungary, ACM (2003) 160–169
14. Commission of the European Communities, ITSEC,: Information technology security evaluation criteria version 1.2. http://www.ssi.gouv.fr/en/confidence/methodology.html (1991)
15. International Standards Organisation, International Electrotechnical Commission: Standard iso/iec 15408: Evaluation criteria for information technology. http://www.iso-standards-international.com/iso-5725-kit70.htm (1999)