# A Secure E-Tendering system

Shahriyar Mohammadi
IT group, Faculty of industrial engineering
K.N.Toosi University of technology
Tehran, Iran
smohammadi40@yahoo.com

Hediy Jahanshahi
IT group, Faculty of industrial engineering
K.N.Toosi University of technology
Tehran, Iran
hedie63@gmail.com

*Abstract*— **Today E-tendering is increasingly being adopted through the world. An electronic environment presents obvious opportunities for collusion between principal and certain tenderers, fraud by tenderers and attempt of intruders to illegally access the system. In this paper, security requirements of an e-tendering system are described. Then the existing architecture of popular-tendering system are introduced. Then a new architecture for a highly secure E-tendering system is proposed. The new architecture uses encrypted iris pattern as biometric attribute for authentication of tenderers participating in a tender. The proposed architecture uses Shamir threshold crypto system for securing the e-tender box and imposes Bell-LaPadula security model on the access rights of parties involved in the e-tendering system.**

## I. INTRODUCTION

Today businesses and governments are largely reliant on information and communication technology to communicate and making contacts. E-tendering is increasingly being adopted through the world. E-tendering in its simplest form is described as the electronic publishing, communicating, accessing, receiving and submitting of all tender related information and documentation via the internet. Thereby replacing the traditional paper-based tender processes and achieving a more efficient and business process for parties involved. 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 [1]. Inadequate security brings opportunities for fraud and collusion by parties inside and outside of the tendering process. In this paper first, a general framework for 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 and security issues related to each stage will be discussed. Thirdly, three types of E-tendering architectures will be presented, then a new E-tendering architecture using biometrics for accurate authentication , Shamir threshold crypto system and Bell-LaPadula security Model for an effective access control to the E-tender Box will be introduced.

## II. E-TENDERING

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 the tendering process [15]. 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 [15].

### *A. 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. System availability is also crucial, particularly during the tender submission stage before the close of tender time. Lopez [17] believes that 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.

#### *1) **Non-repudiation and Authentication***

Non-repudiation property 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 defense against denial of their actions by a participating party. In an e-tendering system, the digital signature mechanism [5,6], can provide authentication and non-repudiation

#### *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.The main areas of concern relating to secure time are: Time integrity, the closing and opening of the e-tender box.

##### *a) Time Integrity*

978-1-4244-3355-1/09/$25.00©2009 IEEE


Authorized licensed use limited to: LUNGHWA UNIV OF SCIENCE AND TECHNOLOGY. Downloaded on October 4, 2009 at 07:02 from IEEE Xplore. Restrictions apply.

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.

*b) Closing/Opening Time of E-Tender Box*

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. Sometimes there are multiple tender boxes, both electronic or physical [12]. 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.

***3) Secure Record-Keeping***

E-tendering systems generate and process electronic documents that are part of business activities. A key legal requirement for record keeping 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 maximize 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. The following e-tendering documents are important evidential material: tender 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 oftener announcement; and any receipt of message acknowledgments.

## *B. E-tendering legal requirement*

Lonie & Lawyers [16] 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 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 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 [17]. As the UNCITRAL Model Law on Electronic Commerce has been adopted worldwide, either in whole or in part in many jurisdictions, it will be used as a guide to the likely legal issues which may arise [16]. The United Nations Commission on International Trade Law (UNCITRAL) is a subsidiary body of the General Assembly. It plays an important role in improving the legal framework for international trade by preparing international legislative texts for use by States in modernizing the law of international trade and non-legislative texts for use by commercial parties in negotiating transactions. [4]. Adopted by UNCITRAL on 1996 , the Model Law is to facilitate the use of modern means of communications and storage of information. It is based on the establishment of a functional equivalent in electronic media for paper-based concepts such as "writing", "signature" and "original". By providing standards by which the legal value of electronic messages can be assessed, the Model Law should play a significant role in enhancing the use of paperless communication. The Model Law also contains rules for electronic commerce in specific areas, such as carriage of goods [8].The Model Law on electronic signature adopted by UNCITRAL on 5 July 2001 [13], aims at bringing additional legal certainty to the use of electronic signatures. Building on the flexible principle contained in article 7 of the UNCITRAL Model Law on Electronic Commerce, it establishes criteria of technical reliability for the equivalence between electronic and hand-written signatures. The Model Law follows a technology-neutral approach, which avoids favoring the use of any specific technical product. The Model Law further establishes basic rules of conduct that may serve as guidelines for assessing possible responsibilities and liabilities for the signatory, the relying party and trusted third parties intervening in the signature process. Adopted by the General Assembly on 23 November 2005 [4], the United Nations Convention on the Use of Electronic Communications in International Contracts aims to enhance legal certainty and commercial predictability where electronic communications are used in international contracts.

# III. E-TENDERING STAGES OF DEVELOPMENT

Governments and business are more likely to develop an e-tendering system in phases. Base on Katsikas and Lopez , a significant number of government e-tendering systems have developed e-tendering systems up to the second stage of development [1].

## *A. One way 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 The documents are still submitted in paper. There is no two-way communication occurring in an electronic environment. For web-based applications, the Secure Sockets Layer (SSL) is an effective mechanism to provide integrity and confidentiality to communications. 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.



Authorized licensed use limited to: LUNGHWA UNIV OF SCIENCE AND TECHNOLOGY. Downloaded on October 4, 2009 at 07:02 from IEEE Xplore. Restrictions apply.

two-way communication

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. However, the tender is not awarded electronically. The main improvement of the Tender Submission and Two-Way Communication stage is that tenderers can upload electronic tender submission documents [1]. HTTP file upload or similar point to point, connection oriented protocol should be used rather than email or other store and forward protocols.

*B. Electronic Tendering Contract Formation*

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. 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.

E-TENDERING SYSTEM ARCITUCTURES

There are three possible system architectures for e-tendering:

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

*C. principal based architecture*

The principal based architecture is mostly used by government e-tendering organizations. The principal is the main administrator of the tendering process.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 addendum, 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 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. 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.

*D. Trusted Third Party Based Architecture:*

The TTP based architecture is commonly used by private industry or independent government bodies. 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 also act as a time-stamping server. The principal and tenderers should synchronies 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.

*E. Distributed Trusted Third Party Architecture:*

The DTTP 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 synchronizations and time controlled key release for accessing submitted tenders. The CA has the function of key registration and key verification. Because of the separation of these roles, this architecture lends itself to a large scale e-tendering implementation.

In this architecture, principals host the e-tender box, and DTTP only provides security services to preserve e-tendering process .

IV. PROPOSED ARCITUCTURE

In our proposed architecture DTTP is improved by using Biometric information for authentication, bell-LaPadula security model and shamir threshold crypto system for securing e-tender Box and other tendering documents. Basic DTTP architecture needs PKI to be implemented and CAs verifies the digital signature of tenderers. Hierarchal structure of verifying digital signatures by CAS slows down the speed of authentication. In the other hand in the DTTP architecturedeposit payment for participating in the e-tender is not taken into consideration. every tender , bidding or any kind of auction needs payment deposit.

*A. Biometric Authentication system*

Biometrics is defined broadly as a scientific discipline of

observing and measuring relevant attributes of living individuals to identify or authenticate [7]. The iris patterns are unique to each individual and even the iris in the left eye differs with the iris in the right eye of a person [7]. Glasses and contact lens do not interfere with the recognition of the iris. Refractive, cataract surgeries and cornea transplants do not change the iris characteristics [7]. Even a blind person with an iris in his sightless eye can be recognized with the iris recognition systems. The iris characteristics do not change with age [9]. Iris authentication necessitates the existence of standardized iris image capture and encryption software along with the web camera that is built in the recent computer systems [7]. In the proposed model iris recognition is chosen to be used for authentication. While issuing a credit debit card, the encrypted iris details of an individual will be stored



Authorized licensed use limited to: LUNGHWA UNIV OF SCIENCE AND TECHNOLOGY. Downloaded on October 4, 2009 at 07:02 from IEEE Xplore. Restrictions apply.

along with the credit debit card number and other personal details in the issuing agency's database. A software need to be present in client systems so that while the tenderer need to be authenticated at each stage , his or her iris image can be captured, encrypted and sent along with the name, credit debit card number, and, expiration date . The iris image of the tenderer is captured using a web camera built in the client system. The iris image is preprocessed, normalized, enhanced, and the key features of the iris are extracted [7]. The biometric credit debit card authentication system consists of iris image feature extraction, RSA encryption unit at the client side with a decryption unit along with database consisting of credit card details at the server side for authentication.

### B. Shamir threshold crypto system

Threshold cryptosystem was first invented by Shamir [10]. Shamir's threshold cryptosystem is based on polynomial interpolation, and the fact that a unvaried polynomial d = f(c) of degree t - 1 is uniquely defined by t points (ci,di) with distinct ci. These define t linearly independent equations in t unknowns [11]. As demonstrated by Liu [14]: "11 scientists are working on a secret project. They wish to lock up the documents in a cabinet so that the cabinet can be opened if and only if 6 or more of the scientists are present". Some of the useful properties of Shamir's (k,n )threshold scheme are:

1.Secure: Information theoretic security.

2.Minimal: The size of each piece does not exceed the size of the original data.

3.Extensible: When K is kept fixed, $D_i$pieces can be dynamically added or deleted (e.g., when allowed principal are fired or suddenly die) without affecting the other pieces.

4.Dynamic: Security can be easily enhanced without changing the secret, but by changing the polynomial occasionally (keeping the same free term) and constructing new shares to the participants.

5.Flexible: In organizations where hierarchy is important, we can supply each participant different number of pieces according to his importance inside the organization.

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 form e-tender box by the principal to its favored tenderer in the traditional tendering process [15] .In order to implement threshold cryptosystem, for securing an E-tender Box in the proposed architecture ,there is a third trusted party in the service layer and a number of principals who are allowed to open E-tender box under some conditions. The third trusted party holds some secret S and sends shares to each of the principals . These shares are computed in such a way that only certain specific subsets of the principals can reconstruct the secret S by pooling their shares. In other word, the solutions allow the third trusted party to consider any number n of principal and any threshold t, such that from any subset of size at least t of the shares the secret S can be reconstructed uniquely and efficiently, whereas sets containing less than t shares contain no information at all about secret S.

### C. Bell-LaPadula security model

The security model developed by Bell and LaPadula [3] has been widely used as a basis for designing systems with specified security properties [2]. The Bell-LaPadula model is based on a state machine in which subjects apply operations (rules) that may require access to objects. Permissible access is determined partly by a security level (classification or clearance) associated with each object and subject. These security levels are partially ordered. Each subject also has a current security level that is bounded above by its clearance. There is also an access matrix that further constrains the access mode an arbitrary subject is allowed to have to an arbitrary object. The concept of a *secure state* is defined by three properties: the *simple security (ss) property*, the *-*property*, and the *discretionary security (ds) property*.

A state satisfies the ss-property if, for each element of $B$ that has an access mode of *read* or *write* , the clearance of the subject dominates (in the partial order) the classification of the object. A triple ($s$ ,$o$ ,$x$ ) satisfies the simple security condition relative to f (SSC rel f) if $x$ is *execute* or *append* , or if $x$ is *read* or *write* and $f_s$ ($s$ ) dominates $f_o$ ($o$ ).

A state satisfies the *-property if, for each ($s$ ,$o$ ,$x$ ) in $B$, the current security level of $s$ is equal to the classification of $o$ if the access mode is *write* , dominates the classification of $o$ if the access mode is *read* , and is dominated by the classification of $o$ if the access mode is *append* .

A state satisfies the ds-property if, for each member of $B$ , the specified access mode is included in the access matrix entry for the corresponding subject-object pair. A state is *secure* if and only if it satisfies the ss-property, *-property relative to $S$ and the ds-property.

A system satisfies the property in question for any initial state that satisfies the property and if and only if *the next state* adds no new elements to $b$ that would violate the property and removes any elements that, following the state change, would violate that property.

In an E-tendering system 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 prevents the change from a secure to insecure state, or detect and log when this change occurs

### D. proposed architecture

Base on DTTP, in our model the TTP who is responsible for authenticating the tenderers and principal is a bank or a financial institution . While issuing a credit debit card, the encrypted iris details of an individual will be stored along with the credit debit card number and other personal details in the issuing bank's database. A software need to be installed in all of the client systems who intend to use the e-tendering systems. Iris image of tenderer can be captured using a web camera built in the system, encrypted and sent along with other data. So he or she will be authenticated by the credit debit card agency. Since the iris image is encrypted before sending to the e-tendering site, the private information of the tenderers is protected and only the credit debit card agency has



Authorized licensed use limited to: LUNGHWA UNIV OF SCIENCE AND TECHNOLOGY. Downloaded on October 4, 2009 at 07:02 from IEEE Xplore. Restrictions apply.

access to it. so the credit debit card issuing bank is responsible for authentication.

Shamir threshold system is used for securing the e-tender box . Enough subset of principals who are allowed to open. The tender box have to pool their shares to open it. The e-tendering system security policies define a subset of actions that transform e-tendering system from a secure state to another secure state. Based on Bell-LaPadula security model , clearance level for every party participating in the e-tender and classification level for e-tender box and other document as objects of the system can be defined. In addition to restricting subjects from having direct access to information for which they are not cleared, this concept of security is intended to prevent the unauthorized flow of information from a higher security level to a lower one. Clearance level of participates in each step of tendering process may vary. These variations are because of variation of access permission to e-tender box and the action that the participates should do in each stage (read, write,…) during the tendering process. As you may remember in Bell- LaPadula model in **-property:*

L(*s)* = L(*o)* if the access mode is *write*

L(*s)* > L(*o)* if the access mode is *read*

L(*s)* <L(*o)* if the access mode is *append*

in the first step of tendering ,After being authenticated by the issuer bank and allowed to participate in tender, security level of tenderers is the lowest level (non-classified), e-tender

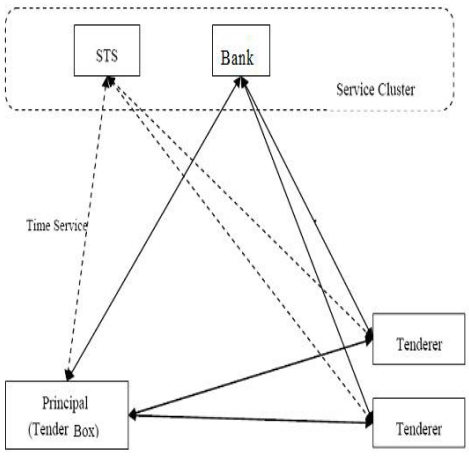


Figure 1. Proposed arcitecture of E-tendering

documents and e-tender box is confidential level ,so these tenders can submit their tender for the first time or append the tenders to the tender box.after firs submission, their security level will be confidential .so now the tenderers can write in the teneder documents. Principals have secret and top secret level so they can't write in the e-tender documents or change them illegally. But they can read this documents under shamir threshold crypto system. Bell- lapadula model can be imposed on shamir crypto system by adding some security level check instruction at the first of the shamir algorithmic the security level is secret or top secret shamir algorithm will give some share of opening key. so just a predefined set of principals can open the e-tender box . In the other hand we can make the threshold system flexible and give a privilege to top secret level principal . For example if the t=6 ,we can give the secret level one share of opening key and give 2 shares of it, if the security level is top secret . So just knowledge of 3 top secret level principal is enough to open the tender box.

### *E. Steps in a the proposed tendering architecture*

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. Different entities are responsible for each security requirement. in the proposed architecture Non-repudiation and authentication are provided by the card issuing bank base on iris information. . Secure time is maintained by the STS. The principal is responsible for secure record keeping just like DTTP architect.

Katsikas and Lopez in [1] described e-tendering steps based on DTTP architecture using CA and PKI for authentication, now e-tendering steps are described based on the proposed architecture*:*

#### *1) Pre-qualification & registration*

At first, potential tenderers requires to submit a registration form in the e-tendering system. These registration form is for qualification assessment . principals relevant to each potential tenderers` industry, assess each registration form and issue pre-qualification status for each qualified potential tenderers to access the e-tendering system. This status is usually based on the ability of the potential tenderers. In this stage potential tenderers have to create an account with a credit or debit card issuing bank who is responsible for potential tenderers authentication by biometric information. Bank will authenticate the tenderers to principal, also let them know that the tenderers have enough credit in their account for paying deposit of tenders.

#### *2) Public invitation*

In this stage, principal creates a public invitation to tender for a particular project. Each pre-qualified tenders can see the relevant tenders in their pages. Principal who creates the public invitation are authenticated by the card issuing bank base on their biometric information. Tender deposits are paid to principal account in this banks.

#### *3) Tender submission*

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 vthetender offer documents before the close of tender. Tender submissions should be digitally signed by the tenderers and verified by their biometric information. The principal must ensure that its clock is synchronized with the STS and that the correct submission time is recorded .

#### *4) Close of Tender*

This stage covers the close of the tender box at a time specified by the principal. Documents submitted by tenderers



Authorized licensed use limited to: LUNGHWA UNIV OF SCIENCE AND TECHNOLOGY. Downloaded on October 4, 2009 at 07:02 from IEEE Xplore. Restrictions apply.

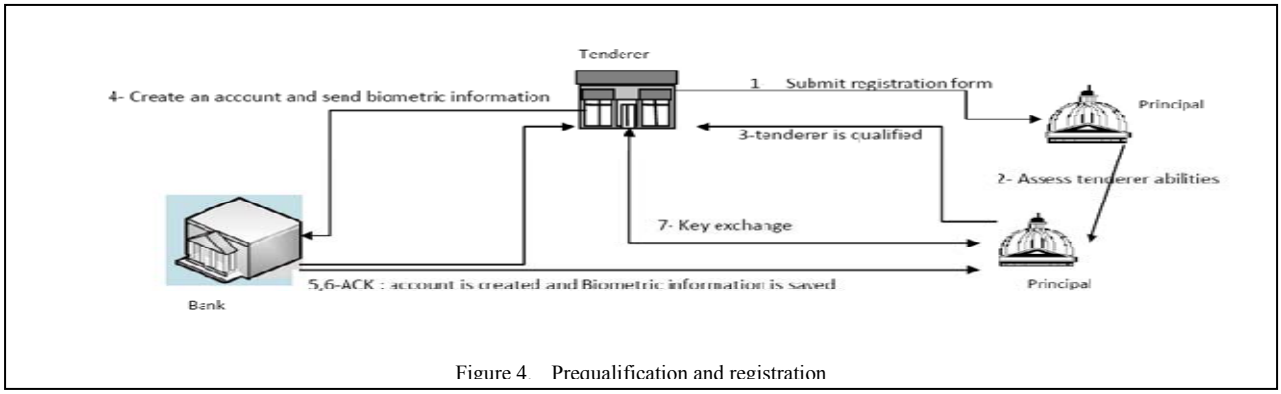


Figure 4 Prequalification and registration

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. Bell -LaPadula security model is imposed to let principals only read the e-tender box content .Shamir threshold crypto system is used to give each principal their shares of opening key. After the submission deadline, the principal can reject any late or non conforming tenders according to the time stamping information and tender specification.

*5) Tender Evaluation*

The principal may need to request more information from the tenderers .authentication of the origin of this message is done by the bank using biometric information.

*6) Award of Tender*

In this 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 the bank to verify each other's identity.

## V. Conclusion and Future Work

A simple cryptographic algorithm for document transfer is not enough for a secure e-tendering system. Authentication in an e-tender system must be very accurate to avoid non-repudiation especially in contracting process. Authentication in Previous architectures was based on PKI. In the proposed architecture, Biometric system is used for authentication . In the other hand, secure saving of tender related documents is vital to have admissible evidence for possible problems in future. In this paper a mixture of bell-lapadulla security model and Shamir crypto system are suggested to be used for saving tender documents. As a futurework, other security models can also be studied in-depth ,Then a comparison of the models can help to identify the most suitable security model. Also, many cryptographic sealed bid schemes have been developed based on Shamir threshold crypto system, for e-auction which can be adopted to suit the e-tendering scheme. Simulation will shothe reality and possible shortcoming of the Proposed architecture. Designing an e-tendering protocol base on the proposed architecture and verifying the protocol by a suitable protocol verification tool is another suggestion for future work.

## References


[1] R.Du, E.Foo,, J.G.Nieto & C.Boyd, Designing secure e-tendering systems. In S. Katsikas,,J. Lopez, & G. Pernul (Eds.), *LNCS Vol. 3592. TrustBus (2005)* (pp. 70–79). Berlin: Springer.

[2] C. E. Landwehr, Best available technologies for computer security, IEEE Computer, July, 1983.

[3] J. McLean, A Comment on the "Basic Security Theorem" of Bell and LaPadula, Information Processing Letters 20 (1985), pp. 67-70.

[4] UNITED NATIONS PUBLICATION, technical report 2007Sales No. E.07.V.2 ISBN 978-92-1-133756-3

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

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

[7] R. R.Vangala, S.Sasi , Biometric Authentication for E-Commerce Transaction, IEEE IST 2004 -International Workshop On Imaging Systems and Techniques Stresa Italy

[8] United Nations Commission on International Trade Law http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce /1996Model.html [accessed 1 Jan 2009]

[9] R.S Womll, , "Iridology: diagnosis or delusion? In Examining Holistic Medicine", ed. D. Stalker and C Glymour (Buffalo: Prometheus Books), 1985

[10] A.Shamir, How to share a secret. Communication of the ACM, 1979 22(11)., 612–613

[11] D.H.Shih, MoRVAM: A reverse Vickrey auction system for mobile commerce et al. / Expert Systems with Applications 32 (2007) 1113–1123

[12] The Internet Engineering Task Force: Network time protocol (version 3) (rfc 1305). http://www.ietf.org/rfc/rfc1305.txt (1992)

[13] UNCITRAL Model Law on Electronic Signatures with Guide to Enactment: http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce /2001Model.html [accessed 1 Jan 2009]

[14] C.L.Liu,. (1968), Introduction to Combinatorial Mathematics, New York: McGraw-Hill

[15] R.Du, E.Foo, C.Boyd, B.Fitzgerald, Defining Security Services for Electronic Tendering ,Proceedings of the second workshop on Australasian information security, Data Mining and Web Intelligence, and Software Internationalisation 2004- Volume 32, 43 - 52

[16] M.Betts , P.Black , S.Christensen , E.Dawson , R.Du , W.Duncan , E.Foo and J.González (2006) TOWARDS SECURE AND LEGAL E-TENDERING, ITcon Vol. 11, Special Issue e-Commerce in construction , pg. 89-102, http://www.itcon.org/2006/7




Authorized licensed use limited to: LUNGHWA UNIV OF SCIENCE AND TECHNOLOGY. Downloaded on October 4, 2009 at 07:02 from IEEE Xplore. Restrictions apply.