ISSN: 1391-8796
Abstracts of Presentations
1st Ruhuna International Science & Technology Conference
University of Ruhuna, Matara, Sri Lanka
January 22-23, 2014

Towards a simple and secure electronic tender submission management protocol

V. Thangarajah*[1] and K. De Zoysa[2]

[1]*Centre for Information and Communication Technology, Eastern University Sri Lanka, Chenkalady, Sri Lanka*
[2] *University of Colombo School of Computing, University of Colombo, Colombo, Sri Lanka*

The traditional tendering process is a manual bidding system which involves the principal advertising or issuing a request for tenders, various suppliers then make offers, one of which is then accepted by the principal, forming a contract between the supplier and the principal. Electronic tender (eTender) management is the continuous usage of electronic means for the entire tendering process. It enables suppliers in different geographic locations to be notified of an opportunity to express an interest to download tender documents and to submit a response. This promotes competition for the tender and a selection process that is transparent to bidders. eTender solutions are developed in the absence of the ability to authenticate people by sight. This creates problems with authenticity and integrity of electronic transactions as trust has been compromised. Improper use of electronic communication systems could also increase the possibility of leaking of tender information. Hence security mechanisms were carefully integrated into the system to provide desirable security services for the processes involved in an eTender management system. The focus of this research is to develop a simple security protocol for electronic tender management that confirms it met the security challenges such as authenticity, integrity, confidentiality and non-repudiation, faced by such systems. It comprised of developing methodologies for establishing security requirements, constructing security protocols and security verification with a user friendly interface. A security protocol was developed using generic symmetric key cryptographic mechanisms with a random string as an additional security measure. The validity of the protocol was tested progressively throughout the design and development process to confirm that it provides sufficient security measures against the challenges. In addition, it was also tested against identified risk scenarios.

Key words: Cryptography, etender, protocol, security

*vinothrajt@yahoo.com