ABSTRAK

IMPLEMENTASI ALGORITME AES, RSA, DAN SHA1 PADA STUDI KASUS PENGIRIMAN DOKUMEN PENAWARAN PADA SISTEM PENGADAAN SECARA ELEKTRONIK (E-PROCUREMENT)

Oleh:

Kania Khairunnisa

12/331233/PA/14519

Beberapa tahun yang lalu, pelaksanaan pengadaan barang dan jasa masih diselenggarakan secara manual. Pengadaan barang dan jasa secara manual memiliki banyak kekurangan, yaitu proses administrasi dan penyerahan dokumen penawaran melalui tatap muka, kerahasiaan peserta lelang kurang terjamin, tranparansi rendah, serta proses *monitoring* yang sulit. Untuk itu dibutuhkan suatu sistem pengadaan barang dan jasa (*e-procurement*) yang dapat diakses secara elektronik (berbasis internet) agar kerahasiaan peserta dapat terjaga.

Dalam penelitian ini akan diimplementasikan konsep-konsep kriptografi algoritme AES, RSA, dan SHA1 pada proses pengiriman dokumen penawaran dalam sistem *e-procurement*. Sistem ini memiliki tiga tahap proses, yaitu pembuatan kunci pengguna menggunakan algoritme RSA yang dilakukan di website *e-procurement*, pembangkitan *digital signature* yang dilakukan di aplikasi pengaman dokumen berbasis *desktop*, dan verifikasi *digital signature* dilakukan di website *e-procurement.* Data yang digunakan pada penelitian ini berupa dokumen-dokumen digital yang berasal dari microsoft *word*, microsoft *excel*, dan pdf yang dikompresi oleh sistem.

Hasil dari penelitian ini menunjukkan bahwa sistem yang dibuat sudah mampu membangkitkan kunci pengguna, membangkitkan dan melakukan verifikasi *digital signature*. Layanan keamanan yang dimiliki oleh sistem ini ialah kerahasiaan, otentikasi, integritas, dan anti penyangkalan. Pengujian yang dilakukan terhadap layanan-layanan keamanan tersebut meliputi uji otentikasi, uji kerahasiaan, uji integritas serta pengujian terhadap anti penyangkalan.

Kata kunci : *Sistem pengadaan, E-Procurement, Penandaan Digital*

ABSTRACT

IMPLEMENTATION AES, RSA, AND SHA1 ALGORITHM IN STUDY CASE DELIVERY OF SUPPLY DOCUMENTS IN ELECTRONIC PROCUREMENT SYSTEM (E-PROCUREMENT)

By

Kania Khairunnisa

12/331233/PA/14519

Several years ago, the procurement of stuff and services was manually. Manually procuring stuff and services has many disadvantages, administration process and submission of bidding documents face to face, the confidentiality participants is less guaranteed, low transparency, and difficult monitoring process. For this reason, a system of procurement of stuff and services is needed (e-procurement) that can be accessed electronically (internet based) so the confidentiality participants can be guaranteed.

In this research, AES, RSA and SHA1 cryptographic algorithm concepts will be implemented in the process of sending bidding documents in the e-procurement system.This system has three process, making user keys using RSA algorithm in the e-procurement website, generating digital signature in desktop based document security application, and verifying digital signature in the e-procurement website. The data used in this research are digital documents from word, excel, and pdf compressed by system.

The results of this research indicate that the system created capable to generate user keys, generate and verify digital signatures. The security services owned by this system are confidentiality, authentication, integrity, and anti-denial. Tests conducted on security services include authentication tests, confidentiality tests, integrity tests and non repudiation test.

Keywords : *Procurement system, E- Procurement, Digital Signature*