PENGIRIMAN DOKUMEN SECARA ELEKTRONIK PADA SISTEM E-PROCUREMENT DENGAN MENGGUNAKAN ASYMMETRIC CRYPTOSYSTEM

Sholeh Hadi Setyawan, Alexander David Widjaja
Universitas Surabaya

sholeh@ubaya.ac.id, alexander@ubaya.ac.id

Abstract/Abtrak

In procurement system, either paper-based or electronic, the seller should submit documents to the buyer. The documents are usually restricted and confidential, containing information that should only be read by purchasing committee, never be read by any other parties, especially the competitors. Therefore special treatment to hide the confidentialily should be applied to the documents envelope, so that the system can meet the required information security principles such as authentication, integrity, confidentiality and non-repudiation. In this paper a method to create electronic secure envelope containing e-procurement submission document is proposed. Assymmetric Cryptosystem using RSA algorithm is used to develop a document submission system. Before the submission process, the seller should authenticate himself using his private key. Documents to be submitted will be compressed with a random session/envelope key. The session key will be sealed with both private key of the sellesr and the public key of purchasing committee so that anyone else can not decrypt the compressed envelope. Only the seller (owner of the documents) and the purchasing committee can decrypt the encrypted documents. The submission process is performed using upload capability of hyper-text transmission protocol (HTTP).

Keywords/Kata kunci: tuliskan maksimal 5 kata kunci di sini.

1. Latar Belakang

Pada sistem pengadaan barang dan jasa sebelumnya, proses pengiriman dokumen dilakukan dengan cara para penyedia barang dan jasa memasukkan dokumen dalam amplop untuk mengikuti lelang. Dokumen yang berada di dalam amplop tidak terjamin kerahasiaannya, banyak terjadi kebocoran karena dokumen yang dikirimkan ada kemungkinan dilihat oleh pihak yang tidak berwenang. Dimungkinkan terjadi adanya manipulasi dokumen sebelum jadwal pembukaan dokumen. Oleh karena dokumen dimasukkan ke dalam amplop tanpa disertai kunci sama sekali, maka amplop dapat dibuka oleh siapa saja.

Untuk mengatasi masalah ini, maka dibutuhkan aplikasi yang dapat mengirimkan dokumen berupa digital atau file. Banyak cara dalam membuat aplikasi pengiriman dokumen ini, tetapi untuk dapat memenuhi kebutuhan agar dokumen yang dikirimkan benar-benar terjaga kerahasiaannya dan tidak salah tujuan, artinya yang dapat membuka hanyalah penerima yang dimaksud oleh pengirim maka dipilihlah asymmetric cryptosystem.

.

2. Tujuan

Membuat aplikasi yang digunakan untuk mengirimkan dokumen pendukung sistem pengadaan eProcurement sehingga dokumen yang dikirimkan benar-benar terjaga kerahasiaannya.

3. Rumusan Masalah

Bagaimana membuat aplikasi yang dapat mengirimkan dokumen dengan aman dan hanya dapat dibuka oleh penerima sesuai tujuan, tidak ada kebocoran data dan tidak terjadi manipulasi di dalam dokumen oleh pihak yang tidak berwenang.

4. Landasan Teori

Asymmetric cryptosystem disebut juga sebagai public's key cryptosystem merupakan salah satu jenis cryptosystem yang menggunakan dua buah key yang berbeda untuk proses encrypt dan decrypt. Kedua key ini saling berhubungan, hanya satu key saja yang perlu dijaga kerahasiaannya sedangkan key yang lainnya dipublikasikan ke semua pengguna. Key yang dipublikasikan dikenal dengan nama public key, dan key yang disimpan dikenal dengan nama private key [Thomas, 2000]. Dengan menggunakan asymmetric cryptosystem maka permasalahan seperti di bawah ini dapat teratasi:

- Penggunaan key yang tidak efektif
- Penggunaan key yang sama didalam komunikasi kurang dapat menjamin tingkat keamanan data yang dikirimkan.
- Symmetric cryptosystem tidak mampu memberikan authentication dalam komunikasi data.

Aplikasi penggunaan asymmentric cryptosystem tergantung pada penggunaan key untuk melakukan proses encrypt yang dilakukan terhadap dokumen. Syarat yang harus dipenuhi asymmetric cryptosystem, yaitu [Wang, 2009]: