ABSTRAK

Ada banyak sistem *e-commerce* di internet yang belum memenuhi kriteria komunikasi elektronik yang legal. Kriteria komunikasi yang legal meliputi kerahasiaan data, keutuhan data, autentikasi pengguna, dan anti penyangkalan pengguna bahwa dia terlibat dalam komunikasi. Sistem *e-commerce* sudah merasa cukup puas ketika mengaplikasikan protokol https (http over ssl) pada *website*nya. Padahal protokol https hanya memenuhi kriteria kerahasiaan data, keutuhan data, dan autentikasi pengguna saja. Sedangkan anti penyangkalan pengguna sangat diperlukan agar seseorang bisa bertanggungjawab atas apa yang sudah diperbuatnya di dalam sistem. Sehingga jika tindakannya merugikan pengguna lain atau menyalahi aturan, dia harus mengakui tindakannya dan mendapatkan sanksi sesuai peraturan.

Pada konsep Public Key Infrastructure (PKI), keempat kriteria komunikasi tersebut dipenuhi. Kerahasiaan data diimplementasikan oleh algoritma enkripsi dan dekripsi baik simetrik atau asimetrik. Keutuhan data diimplementasikan oleh teknik tandatangan digital. Autentikasi pengguna diimplementasikan oleh Certification Authority (CA) yang bertugas untuk mengeluarkan dan menandatangani sertifikat digital untuk setiap pengguna yang terlibat dalam komunikasi. Sertifikat digital milik CA berperan dalam proses autentikasi. Anti penyangkalan diimplementasikan oleh Time Stamping Authority (TSA) yang bertugas untuk memberi stempel tanggal dan waktu saat suatu kejadian berlangsung lalu menandatanganinya. Oleh karena dalam PKI setiap pengguna yang terlibat dalam komunikasi percaya kepada CA dan TSA, maka apapun yang dinyatakan oleh CA dan TSA adalah benar dan tidak bisa disangkal.

Untuk mengimplementasikan konsep PKI, pada tugas akhir ini dibuat sebuah sistem lelang yang meliputi aplikasi *website* dan *mobile client* berteknologi J2ME. Kedua komponen ini saling berkomunikasi menggunakan konsep PKI. Dalam komunikasinya, mereka saling melibatkan CA dan TSA karena mereka percaya akan apapun yang dinyatakan oleh CA dan TSA.

Dengan dibuat sistem lelang pada tugas akhir ini, kriteria komunikasi elektronik yang legal sudah dapat dicapai. Pengguna aplikasi *mobile client* juga terbantu dengan adanya aplikasi ini karena mendukung mobilitas pengguna.

Kata kunci : Public Key Infrastructure, Certification Authority, Time Stamping Authority, J2ME