ABSTRAK

Tugas akhir ini membahas mengenai Implementasi RSA SecurID pada handphone android yang merupakan jaringan publik berganti menjadi VPN (*Virual Private Network)* untuk terhubung kedalam jaringan lokal kantor, dan seolah tanpa jarak saat melakukan pekerjaan diluar kantor. Memungkinan user di lapangan dan gerai/grapari Telkomsel dalam mengirimkan informasi ter*update* setiap waktu. Pada proses autentikasi ini menggunakan algoritma 3DES yang menyediakan solusi sederhana tanpa perlu menciptakan algoritma yang baru, yaitu menjalankan algoritma 3DES (*Triple Data Encryption Standard*) sebanyak 3 kali untuk masing-masing blok data. Proses tersebut menyebabkan ukuran kunci / *password* internal bertambah dari 56 bit menjadi 168 bit. Berdasarkan perbandingan nilai overhead size antar IPSec dan SSL terdapat perbedaan byte overhead size dimana size IPSec adalah 45 byte sedangkan SSL 22 byte, perbedaan size bisa dibilang sebesar 100%. Nilai 1170,111 Kbyte pada IPSec dan 1170,088 Kbyte pada SSL merupakan total nilai keseluruhan data setelah ditembah dengan nilai overhead size, nilai padding byte, dan Panjang pad. Dengan itu semua dapat disimpulkan bahwa protocol SSL membutuhkan dan memiliki nilai overhead size yang lebih sedikit dan lebih kecil dibandingkan protocol IPSec.

Kata Kunci : RSA SecurID, *Virtual Private Network*, 3DES, Android

ABSTRACT

This final project, discusses the implementation of RSA SecurID on an Android mobile phone which is a public network that has changed to VPN (Virual Private Network) to connect to the local office network, and as if without distance when doing work outside the office. Allows users in Telkomsel's fields and outlets to send updated information every time. In this authentication process uses the 3DES algorithm which provides a simple solution without the need to create a new algorithm, which is running the 3DES (Triple Data Encryption Standard) algorithm 3 times for each data block. This process causes the internal lock / password size to increase from 56 bits to 168 bits. Based on the comparison of the overhead size value between IPSec and SSL there are differences in byte overhead size where IPSec size is 45 bytes while SSL is 22 bytes, the size difference can be said to be 100%. The value of 1170,111 Kbyte in IPSec and 1170,088 Kbyte in SSL is the total value of the data after being sacrificed with the value of overhead size, padding byte value, and pad length. With that all can be concluded that the SSL protocol requires and has a smaller size and smaller overhead than the IPSec protocol.

Keywords : RSA SecurID, Virtual Private Network, 3DES, Android