Abstrak

Smart Card saat ini telah banyak diimplementasikan pada suatu sistem untuk membantu manusia dalam mengembangkan teknologi, salah satunya yaitu pembatas akses seperti kartu identitas sebagai kunci pintu ruangan tertutup. Beragam tipe kartu yang digunakan dibagi berdasarkan cara komunikasi data yaitu contact card, dan contactless card, serta bermacam metode otentikasi yang diterapkan. Namun kartu yang digunakan masih memungkinkan terduplikasi tanpa sepengetahuan pemilik. Penyebab terjadinya duplikasi tersebut sangat beragam, mulai dari kartu yang sama sekali tidak memiliki keamanan hingga pada kartu yang telah memiliki metode keamanan seperti enkripsi data kartu. Oleh karena itu penelitian ini mengimplementasikan metode Synchronized Secret melalui mutual authentication, yang mana setiap kali proses otentikasi kartu terhadap card reader harus saling mengotentikasi. Pada setiap sesi otentikasi memerlukan data riwayat transaksi berupa data random yang selalu berubah dan tidak dapat diketahui oleh siapapun. Seluruh proses otentikasi akan berjalan jika kartu terinstall Applet sebagai media komunikasi. Hasil dari beberapa skenario pengujian menunjukan bahwa data pada kartu tidak dapat terbaca secara ilegal, sehingga kartu tidak dapat terduplikasi. *Time process* tapping memerlukan rata-rata waktu 4 detik, sehingga dapat menjadi alternatif dari proses otentikasi yang ada sebelumnya.

Kata kunci : ***smart card, mutual authentication, applet, synchronized secret.***