BAB 5
KESIMPULAN DAN SARAN

Kesimpulan merupakan ringkasan yang diambil dari penelitian skripsi yang dilakukan, berdasarkan pengamatan pada hasil analisa, implementasi dan pengujian. Saran yang diberikan merupakan bahan referensi untuk mengembangkan penelitian agar menjadi lebih baik.

5.1 Kesimpulan

Dari hasil penelitian ini dapat diambil kesimpulan:

1. Biometrik tandatangan manual *offline* pengguna dapat digunakan untuk membuat sepasang kunci. Pasangan kunci yang dihasilkan adalah kunci *Private* dan kunci publik. Dari masukan satu tandatangan *offline* dapat menghasilkan lebih dari satu pasang kunci. Hal ini menunjukkan pembangkitan kunci secara dinamis.
2. Keamanan implementasi Biometrik tandatangan dan RSA pada penelitian ini didasarkan atas satu e-dokumen jika semua verifikasi bernilai valid berarti telah aman dalam hal verifikasi. Sebaliknya jika salah satu atau lebih hasil verifikasi tidak valid maka verifier dapat mengetahui jika e-dokumen yang diterima sudah tidak otentik dan atau salah satu atau lebih dari signer adalah bukan orang yang sebenarnya menandatangani e-dokumen tersebut.
3. Pada implementasi tandatangan digital dengan metode hybrid: Biometrik tandatangan dan RSA terpenuhi kebutuhan keamanan e- dokumen dalam hal:
    - Kerahasiaan (*confidentiality*) *signature* hanya dapat didekripsi oleh verifier dengan kunci *Private* pasangan kunci publik pada pihak signer.
    - Keutuhan atau keotentikan (*integrity*) e-dokumen tersebut.
    - Jaminan atas identitas dan keabsahan (*authenticity*)

5.2 Saran

Saran yang dapat diberikan terkait dengan implementasi tandatangan digital yang telah diteliti yaitu: Untuk lebih mengoptimalkan sisi keamanan transmisi e-dokumen lewat internet adalah dengan menggunakan tandatangan *offline* dan menambahkan algoritma pencocokan tandatangan.