BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan rumusan masalah yang telah ditetapkan pada bab I serta hasil penelitian yang telah dilakukan, maka diperoleh kesimpulan sebagai berikut :

1. Algoritma ECDSA berhasil diimplementasikan pada sistem autentikasi dokumen digital berbasis *web* menggunakan Python dan *framework* Flask. Algoritma ECDSA digunakan untuk menghasilkan tanda tangan digital pada dokumen PDF melalui proses *hashing* menggunakan SHA-256 dan proses *signing* menggunakan *private key*.
2. Integrasi QR Code sebagai media penyimpanan tanda tangan digital berhasil diterapkan pada sistem "AuthentiC" dan mampu digunakan untuk proses verifikasi dokumen digital. Berdasarkan hasil pengujian, sistem mampu mendeteksi perubahan pada dokumen PDF melalui proses verifikasi *signature* sehingga integritas dan keaslian dokumen dapat dijaga dengan baik.

5.2 Saran

Meskipun sistem yang dibangun telah berhasil menjalankan fungsi utama dengan baik, masih terdapat beberapa hal yang dapat dikembangkan lebih lanjut. Berikut merupakan saran dari peneliti yang mungkin dapat meningkatkan kinerja atau manfaat dari rancangan sistem *web* ini, antara lain :

1. Sistem dapat dikembangkan agar mendukung format dokumen lain seperti .docx atau .jpg dengan penyesuaian metode *hashing* dan proses verifikasi yang sesuai.
2. Penambahan fitur enkripsi pada data yang tersimpan di dalam QR Code dapat dilakukan untuk meningkatkan kerahasiaan informasi tanda tangan digital.

3. Sistem dapat dikembangkan berbasis *cloud* atau *online hosting* agar proses *signing* dan *verification* dapat diakses secara lebih luas melalui internet.