BAB I
PENDAHULUAN

1.1 Latar Belakang

Digitalisasi dokumen telah mengubah dokumen-dokumen fisik ke dalam bentuk digital yang lebih mudah disimpan, diakses, dan dibagikan, salah satunya adalah sertifikat digital atau sertifikat elektronik (*e-certificate*) yang kini banyak digunakan sebagai bukti kompetensi, keterampilan, dan pengetahuan individu [1], [2]. Akan tetapi, ketersediaan aplikasi pengedit dokumen atau foto dapat disalahgunakan oleh pihak tertentu untuk tujuan yang ilegal [3], [4]. Akibatnya, sertifikat digital sangat rentan terhadap pemalsuan, manipulasi data, atau penyalahgunaan oleh pihak yang tidak berwenang. Hal ini dapat mengancam keaslian dan integritas sertifikat itu sendiri [5]. Berdasarkan data dari Pusiknas Bareskrim Polri, pada bulan Januari tahun 2022 sendiri terdapat 95 kasus pemalsuan dokumen dan sertifikat, dengan rata-rata penanganan 7 kasus setiap harinya [6].

Dalam upaya mengatasi pemalsuan sertifikat, autentikasi sertifikat menjadi solusi yang umum diterapkan. Salah satu metode umum dalam autentikasi sertifikat adalah pemindaian kode QR pada sertifikat yang merepresentasikan tautan ke halaman situs *web* tertentu untuk proses autentikasi [7]. Namun metode ini tidak mampu dalam menjamin keaslian dan integritas isi sertifikat itu sendiri [8], [9]. Tautan yang terkandung di dalam kode QR juga berpotensi menimbulkan berbagai risiko, seperti *phishing* dan pengalihan tautan ke situs yang palsu [10]. Sebagai contoh, salah satu kasus di Kepulauan Riau menunjukkan bahwa pelaku menciptakan sistem penerbitan dokumen palsu yang terhubung ke situs *web* verifikasi fiktif melalui pemindaian kode QR [11]. Dengan demikian, diperlukan alternatif sistem autentikasi sertifikat yang lebih efektif dan handal.

Sebagai solusinya, beberapa penelitian terdahulu memanfaatkan *digital signature* yang diisi ke dalam kode QR alih-alih tautan ke situs *web*. Hal ini dapat meningkatkan keamanan sertifikat digital karena setiap perubahan isi sertifikat dapat dideteksi melalui proses verifikasi kriptografi [12], [13]. Suhardi pada penelitiannya menerapkan algoritma *digital signature* berupa DSA dengan *hash function* berupa SHA-1 untuk mekanisme autentikasi dokumen akademik mahasiswa [1]. Sementara itu, Yogi menerapkan algoritma RSA dengan *hash function* SHA-256 untuk meningkatkan kemananan *invoice* [14]. Lebih lanjut, Theophilus Wellem menerapkan ECC (*Elliptic Curve Cryptography*) berupa algoritma ECDSA untuk autentikasi dokumen, yang di mana lebih aman, cepat, dan ringan dibandingkan metode kriptografi asimetris konvensional seperti DSA dan RSA [15], [16].

Selain itu, sejak per tanggal 16 Desember 2021, sistem informasi Balai Sertifikasi Elektronik (BSrE) dari BSSN yang juga menerapkan *digital signature*, telah tercatat menerbitkan total 176.685 buah sertifikat digital dengan rata-rata penerbitan 4.000 buah sertifikat setiap bulannya [17].

EdDSA (*Edwards-curve Digital Signature Algorithm*) merupakan algoritma berbasis *elliptic curve cryptography* yang dirancang untuk mengatasi kekurangan-kekurangan pada ECDSA. EdDSA menggunakan kurva Edwards yang memiliki beberapa keunggulan dibandingkan kurva Weierstrass yang digunakan oleh ECDSA, yakni penerapan skema tanda tangan deterministik yang sepenuhnya menghilangkan risiko *nonce-attack* dan memberikan ketahanan lebih baik terhadap serangan *side-channel* [18]. Selain keunggulan dalam aspek keamanan, EdDSA juga memberikan tingkat keamanan setara dengan ukuran tanda tangan yang lebih kecil (hanya 64 *byte*) dan kecepatan komputasi yang lebih tinggi namun efisien dibandingkan ECDSA [19]. EdDSA dapat digunakan sebagai alternatif algoritma *digital signature* untuk sistem autentikasi sertifikat.

Berdasarkan uraian di atas, diperlukan pengembangan sebuah sistem autentikasi sertifikat digital yang baik dan aman serta menerapkan algoritma *digital signature* EdDSA. Oleh karena itu, dilakukanlah penelitian berjudul "**Autentikasi Sertifikat Digital Berbasis *Digital Signature* dengan Algoritma EdDSA**".

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah di uraikan sebelumnya, maka rumusan masalah yang menjadi dasar pengerjaan Tugas Akhir ini adalah:

1. Sistem autentikasi sertifikat digital konvensional dengan kode QR yang berisi tautan ke situs *web* autentikasi eksternal memiliki risiko pengalihan situs *web* yang palsu atau berbahaya
2. Algoritma seperti RSA dan DSA pada sistem autentikasi sertifikat digital berbasis *digital signature* memiliki ukuran kunci dan beban komputasi yang relatif besar sehingga kurang efisien pada penyimpanan kode QR
3. Mekanisme autentikasi sertifikat digital yang ada tidak dapat mendeteksi manipulasi representasi visual teks secara otomatis

1.3 Tujuan

Adapun tujuan dari penelitian ini adalah:

1. Mengembangkan sistem autentikasi sertifikat digital bersifat internal dan mandiri yang memanfaatkan *digital signature*, kode QR, dan OCR untuk memaksimalkan keamanan
2. Mengimplementasikan skema *digital signature* EdDSA yang disematkan ke dalam kode QR sertifikat digital sebagai pengganti algoritma RSA, DSA, atau ECDSA

1.4 Manfaat

Adapun manfaat yang diharapkan dari tugas akhir ini adalah sebagai berikut:

1. Memberikan solusi autentikasi sertifikat digital tanpa bergantung pada sistem autentikasi eksternal
2. Mengurangi terjadinya penyalahgunaan, pemalsuan, dan manipulasi data sertifikat digital oleh pihak tidak berwenang
3. Menghasilkan aplikasi autentikasi sertifikat yang dapat digunakan untuk mendukung keamanan dokumen/sertifikat institusi atau lembaga
4. Menambah wawasan dan referensi penelitian dalam bidang keamanan data melalui kriptografi
5. Menjadi acuan pengembangan sistem sertifikat digital yang lebih aman di instansi pendidikan atau lembaga pemerintahan

1.5 Ruang Lingkup

Berdasarkan rumusan masalah yang telah dipaparkan sebelumnya, ruang lingkup penelitian ini dibatasi sebagai berikut:

1. Sistem autentikasi sertifikat digital menggunkan kode QR yang berisi *digital signature* tanpa ketergantungan pada situs *web* autentikasi eksternal
2. Sistem memproses sertifikat digital dalam format JPEG (.jpg, .jpeg) atau PNG (.png)
3. Autentikasi sertifikat difokuskan pada verifikasi isi tekstual sertifikat digital
4. *Digital signature* diimplementasikan menggunakan algoritma EdDSA (varian Ed25519) dan *hash function* SHA-512
5. Proses ekstraksi teks dari sertifikat digital menggunakan OCR
6. Pengujian sistem dilakukan menggunakan metode *blackbox testing*
7. Penelitian mencakup sistem penerbitan sertifikat dan autentikasi sertifikat
8. Aplikasi sistem dikembangkan dalam bentuk *web application* menggunakan *framework* React untuk *front-end*, dan bahasa pemrograman Python serta JavaScript untuk *back-end*. Sementara basis data sistem menggunakan MySQL dan sampel sertifikat digital dibuat menggunakan aplikasi Canva