BAB I
PENDAHULUAN

A. Latar Belakang

Pandemi yang melanda Indonesia pada tahun 2020 serta berbagai negara di dunia mendorong banyak aktivitas beralih ke penggunaan teknologi informasi sebagai sarana untuk berkumpul dan berkomunikasi secara daring (*online*). Salah satu kegiatan yang kemudian populer di kalangan masyarakat, baik dalam bidang pendidikan maupun non-pendidikan adalah webinar. Selain itu, banyak lembaga juga mulai menyediakan layanan kursus berbasis kompetensi secara online. Dalam setiap kegiatan webinar maupun kursus *online*, penyelenggara umumnya memberikan sertifikat sebagai bukti partisipasi, baik bagi pemateri maupun peserta. Karena kegiatan tersebut dilakukan secara daring, sertifikat yang diberikan berbentuk *file* digital atau dikenal dengan sertifikat elektronik (*e-certificate*) [1].

Sertifikat elektronik yang berbentuk file digital dan dikirimkan melalui internet memiliki kerentanan terhadap tindakan pemalsuan, baik berupa fabrikasi maupun modifikasi data. Sebagai gambaran empirisnya, dalam *Lanskap Keamanan Siber 2023*, Badan Siber dan Sandi Negara (BSSN) mencatat bahwa sepanjang tahun 2023 terjadi ribuan indikasi insiden siber sebanyak 4.001.905 aktivitas *Advanced Persistent Threat* (APT) dan 1.011.209 aktivitas *ransomware* [2]. Dan dalam hal ini penulis fokus pada insiden siber terutama terkait anomafli trafik dan potensi manipulasi digital. Sementara itu, ada juga laporan yang diterbitkan oleh *Interpol Review of Digital Evidence 2019–2022* menunjukkan bahwa bukti elektronik di dunia forensik digital terus menjadi objek manipulasi karena semakin kompleksnya teknik serangan digital [3]. Bahkan pada skala internasional, *Europol* menyoroti bahwa dokumen digital mulai rentan terhadap teknik canggih seperti *morphing*, *deepfake*, dan manipulasi citra, sebagai bagian dari upaya pemalsuan modern [4]. Oleh sebab itu, diperlukan suatu mekanisme untuk menjaga keaslian data pemilik sertifikat (peserta/pemateri) serta data penyelenggara kegiatan yang menerbitkannya. Dalam hal ini, kriptografi hadir dengan menyediakan fasilitas tanda tangan digital yang mampu memberikan jaminan *autentikasi*, integritas data, dan *non-repudiation*, sehingga dapat meminimalisasi risiko terjadinya sertifikat palsu [1].

Penerapan Tanda Tangan Digital merupakan salah satu wujud nyata dari transformasi yang tengah berlangsung di Indonesia dalam upaya mengembangkan dan memanfaatkan teknologi digital secara lebih luas. Dunia pemerintahan pun tidak luput dari arus digitalisasi yang terus berkembang. Berbagai instansi kini berusaha meningkatkan kualitas pelayanan publik dengan memanfaatkan kemajuan teknologi informasi dan komunikasi [5].

Meskipun akselerasi digital terus digencarkan, implementasi tanda tangan digital di sejumlah instansi pemerintah masih belum berjalan. *PrivyID* sebagai salah satu penyedia tanda tangan digital terbesar di Indonesia melaporkan memiliki sekitar 30 juta pengguna terverifikasi pada tahun 2023, yang menunjukkan tingginya adopsi di sektor swasta dan masyarakat umum [3]. Namun, kondisi ini belum diikuti oleh sebagian instansi pemerintah daerah. Salah satu contohnya adalah Dinas Pendidikan, Kepemudaan dan Olahraga Kabupaten Lingga, yang hingga saat ini belum menggunakan tanda tangan digital dalam proses administrasi dan pelayanan internal. Situasi ini memperlihatkan adanya kesenjangan antara perkembangan teknologi identitas digital nasional dengan penerapannya pada tingkat instansi daerah.

Tanda tangan digital (*digital signature*) merupakan metode matematis yang digunakan untuk mengidentifikasi pengirim sekaligus membuktikan keaslian suatu dokumen [6]. *Digital signature* berbeda dengan tanda tangan elektronik karena keduanya memiliki perbedaan dari segi keamanan, keaslian, keabsahan, serta kerahasiaan data, meskipun masih banyak pihak yang keliru dalam mendefinisikan keduanya. Tidak seperti tanda tangan konvensional yang dibubuhkan di atas kertas, *digital signature* dibentuk melalui proses pembuatan *message digest* atau *hash*, yaitu ringkasan matematis dari dokumen yang dikirimkan melalui jaringan siber [5]. Selain itu, penerapan *digital signature* juga dapat digunakan untuk memverifikasi autentisitas dokumen karena berbasis pada kriptografi modern yang menjamin otentikasi, integritas data, serta memberikan sifat *non-repudiation* atau anti-penyangkalan [6].

Penggunaan kombinasi dan perbandingan algoritma *ECDSA* dengan fungsi *hash BLAKE2B* dan *SHA-128*, pada proses tanda tangan digital serta verifikasi dokumen diharapkan menghasilkan kinerja yang cukup optimal dan efisiensi pada

penerapan sistem. Dengan demikian, penelitian ini berfokus pada implementasi *ECDSA* dengan fungsi *hash BLAKE2B* dan *SHA-128* dalam sistem tanda tangan digital, sekaligus melakukan analisis pembanding terhadap algoritma fungsi *hash,* untuk menilai tingkat efisiensi dan keamanannya.

B. Rumusan Masalah

Berdasarkan latar belakang tersebut, rumusan masalah dalam penelitian ini adalah:

1. Bagaimana mengimplementasikan sistem digital *signature* berbasis algoritma ECDSA yang dapat mengurangi ketergantungan pada tanda tangan manual dalam penerbitan sertifikat digital di Disdikpora Kabupaten Lingga?
2. Bagaimana mengoptimalkan sistem *digital signature* menggunakan *ECDSA* dengan kombinasi fungsi *hash BLAKE2B* dan *SHA-128*?

C. Batasan Penelitian

Untuk menjaga fokus penelitian, maka batasan masalah yang ditetapkan adalah sebagai berikut:

1. Penelitian dilakukan pada sistem penerbitan sertifikat digital di lingkungan Disdikpora Kabupaten Lingga.
2. Algoritma *digital signature* yang digunakan adalah *ECDSA* dengan fungsi *hash BLAKE2B*, serta dibandingkan dengan algoritma *hash SHA-128* untuk analisis komparatif.
3. Parameter analisis dibatasi pada aspek keamanan (kemampuan mencegah pemalsuan), efisiensi (waktu pemrosesan), dan keandalan (validasi keaslian sertifikat).
4. Penelitian ini tidak membahas aspek hukum atau legalitas tanda tangan digital, melainkan berfokus pada aspek teknis dan implementasi sistem.

D. Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah:

1. Merancang dan mengimplementasikan sistem *digital signature* berbasis algoritma *ECDSA* yang fleksibel dan efisien untuk penerbitan sertifikat digital.

2. Mengembangkan sistem keamanan dengan kombinasi *ECDSA-BLAKE2B* dan *ECDSA-SHA*-128 yang mampu meningkatkan validasi keaslian sertifikat.

E. Manfaat Penelitian

Penelitian ini diharapkan memberikan manfaat sebagai berikut:

1. Bagi Penulis

   Penelitian ini bermanfaat bagi penulis sebagai sarana penerapan ilmu yang diperoleh selama perkuliahan dalam bidang kriptografi dan keamanan data, sekaligus menambah pengalaman praktis dalam merancang, mengimplementasikan, serta menganalisis sistem tanda tangan digital berbasis *ECDSA* dengan fungsi *hash BLAKE2B* dan *SHA*-128, sehingga melatih kemampuan penelitian ilmiah yang sistematis, logis, dan terukur sebagai bekal akademik maupun profesional.

2. Bagi Pembaca

   Penelitian ini dapat menjadi referensi tambahan mengenai implementasi tanda tangan digital pada sistem penerbitan sertifikat, memberikan pemahaman tentang kelebihan kombinasi *ECDSA* dengan *BLAKE2B* dan *SHA-128*, serta menambah wawasan mengenai metode analisis efektivitas algoritma kriptografi dari aspek akurasi, kecepatan, dan keamanan.

3. Bagi Instansi (Dinas Pendidikan, Kepemudaan dan Olahraga Kabupaten Lingga)

   Penelitian ini memberikan manfaat bagi instansi dengan menghadirkan alternatif solusi digital untuk meningkatkan keamanan penerbitan sertifikat resmi melalui pemanfaatan teknologi tanda tangan digital, sehingga proses penandatanganan dan distribusi sertifikat menjadi lebih efisien, serta mendukung peningkatan kredibilitas instansi dengan adanya mekanisme validasi digital berbasis *QR-Code* yang sulit dipalsukan.

4. Bagi Masyarakat (Kabupaten Lingga)

   Penelitian ini memberikan manfaat bagi masyarakat Kabupaten Lingga sebagai penerima sertifikat digital, karena dengan adanya penerapan tanda tangan digital berbasis *ECDSA* yang dilengkapi *QR-Code*, masyarakat dapat dengan mudah memastikan keaslian sertifikat yang diterima. Melalui proses

pemindaian *QR-Code*.