

BAB I

PENDAHULUAN

1.1 Latar Belakang

Menurut Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik & Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

"Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat tanda tangan digital dan identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik."

Menurut Whitman & Mattord (2012), *"Sertifikat Elektronik merupakan dokumen elektronik atau file yang berisi nilai kunci kriptografidan informasi yang mengidentifikasi suatu entitas yang memiliki kunci tersebut."* Dapat disimpulkan bahwa isi dari sertifikat elektronik adalah identitas pemilik sertifikat elektronik, pasangan kunci kriptografi (kunci privat dan publik) dan tanda tangan elektronik dari penerbit sertifikat elektronik. Kurang lebih hampir sama seperti KTP Elektronik, pada KTP Elektronik terdapat informasi identitas, diterbitkan oleh camat setempat dan terdapat tanda tangan dari camat-nya, yang membedakannya dengan sertifikat elektronik adalah bentuknya, KTP berbentuk fisik sedangkan sertifikat elektronik berbentuk file.

Tahapan tanda tangan elektronik teorinya seperti berikut.

1. Dokumen asli akan dihitung nilai hashnya, apa itu hash? fungsi hash itu fungsi matematika yang memetakan informasi dari dokumen ke nilai yang ukurannya tetap. Misal menggunakan algoritma hash SHA256, maka informasi dokumen itu dipetakan, diresume ke dalam ukuran 256 bit. Fungsi hash ini digunakan untuk mengecek keutuhan atau integrity dari dokumen tersebut, bisa dikatakan nilai hash itu

adalah biometriknya dokumen, jika ada perubahan 1 bit saja pada dokumen maka nilai hash atau biometriknya akan berubah.

2. Setelah mendapatkan nilai hash dari dokumen asli, nilai hash tadi dienkripsi menggunakan kunci privat pemilik sertifikat elektronik, hasil enkripsi ini yang disebut dengan tanda tangan elektronik.
3. Selanjutnya tanda tangan elektronik dibubukan atau ditambahkan di dokumen aslinya.

Berikut cara verifikasi dokumen yang memiliki tanda tangan elektronik

1. Dokumen asli dan tanda tangan elektronik dipisahkan.
2. Dokumen asli dihitung nilai hashnya.
3. Tanda tangan elektronik didekripsi menggunakan kunci publik pemilik sertifikat yang menandatangani, hasilnya adalah nilai hash
4. Hasil dari poin 2 dan 3 dibandingkan, jika **sama** berarti dokumen tidak mengalami perubahan dan tanda tangan elektroniknya **valid**, jika **tidak sama** maka dokumen telah dipalsukan dan tanda tangan elektronik **tidak valid**.

1.2. Rumusan Masalah

Berdasarkan uraian latar belakang diatas, maka dapat dirumuskan permasalahan yaitu bagaimana merancang dan membangun aplikasi Sistem Informasi Pengajuan Sertifikat Elektronik Untuk Tanda Tangan Digital Perangkat Daerah Pada Dinas Komunikasi Dan Informatika Pemerintah Provinsi Kepulauan Bangka Belitung Berbasis Website

1.3. Batasan Masalah

Agar penelitian ini terarah dan mencapai tujuan yang diharapkan, maka penulis membatasi ruang lingkup permasalahan yaitu:

1. Aplikasi ini digunakan untuk pengajuan mendapatkan Sertifikat Elektronik dalam penggunaan tanda tangan digital pada Perangkat

- Daerah Pemerintah Provinsi Kepulauan Bangka Belitung melalui Dinas Komunikasi dan Informatika Provinsi Kepulauan Bangka Belitung
2. Isi dari Sertifikat Elektronik ini merupakan Data Pribadi atau identitas Pemilik yang akan digunakan pada tanda tangan digital.
 3. Aplikasi hanya Pengajuan Sertifikat Elektronik Untuk Tanda Tangan Digital Perangkat Daerah Pada Dinas Komunikasi Dan Informatika Pemerintah Provinsi Kepulauan Bangka Belitung Berbasis Website
 4. Aplikasi ini dibuat menggunakan bahasa pemrograman php mysql

1.4. Tujuan dan Manfaat Penelitian

Tujuan dari penelitian ini yaitu menghasilkan aplikasi Pengajuan Sertifikat Elektronik Untuk Tanda Tangan Digital Perangkat Daerah Pada Dinas Komunikasi Dan Informatika Pemerintah Provinsi Kepulauan Bangka Belitung Berbasis Website yang bisa dengan mudah digunakan oleh Perangkat Daerah Pemerintah Provinsi Kepulauan Bangka Belitung

Manfaat penelitian ini yaitu sebagai berikut :

1. Membantu mempermudah Perangkat Daerah dalam pengajuan Sertifikat Elektronik untuk dapat menggunakan tanda tangan digital.
2. Memberikan kemudahan bagi para pengguna aplikasi dalam pengajuan Sertifikat Elektronik untuk tanda tangan digital tanpa harus datang langsung ke Dinas Komunikasi dan Informatika Provinsi Kepulauan Bangka Belitung.
3. Dapat merubah Mainset atau pola pikir bahwa bentuk tanda tangan digital diakui keabsahannya secara hukum selain tanda tangan basah.
4. Bagi peneliti sendiri dapat memperdalam pengetahuan dalam mengelola keamanan data pribadi

1.5. Sistematika Penulisan

Untuk memahami penulisan laporan skripsi, maka materi yang tertera pada laporan skripsi ini dikelompokkan menjadi beberapa sub bab dengan sistematika penulisan sebagai berikut :

BAB I PENDAHULUAN

Bab ini menguraikan latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat penelitian dan sistematika penulisan laporan.

BAB II LANDASAN TEORI

Bab ini berisi uraian teori yang digunakan sesuai dengan topik skripsi yang diambil dan menguraikan tentang *tools/software* (komponen) yang digunakan untuk pembuatan sistem atau untuk keperluan penelitian.

BAB III METODOLOGI PENELITIAN

Pada bab ini, penulis menerangkan tentang metode penelitian yang digunakan serta langkah-langkah yang digunakan terkait dengan penelitian yang dilakukan.

BAB IV PEMBAHASAN

Bab ini akan menjelaskan tinjauan umum yang berisi tentang gambaran umum objek penelitian dengan struktur organisasi, tugas dan wewenang serta menjelaskan secara rinci rancangan sistem yang akan diusulkan.

BAB V PENUTUP

Bab ini merupakan penutup dari semua pembahasan yang memuat kesimpulan dan saran yang dapat mengemukakan kembali masalah penelitian dan menyimpulkan bukti-bukti yang diperoleh dan menarik kesimpulan dari hasil yang dikerjakan dan layak untuk di implementasikan.