BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Kantor Pelayanan Perbendaharaan Negara (KPPN) Sorong merupakan instansi vertikal Direktorat Jenderal Perbendaharaan yang berada di bawah Kanwil Ditjen Perbendaharaan Propinsi Papua Barat. Sebagai unit organisasi di bawah payung Kementerian Keuangan maka tugas dan fungsinya berdasar pada keputusan-keputusan yang dikeluarkan oleh Menteri Keuangan.

KPPN Sorong memberikan pelayanan kepada satuan kerja sesuai tugas dan fungsi dengan memanfaatkan sumber daya manusia dan didukung dengan teknologi informasi untuk menciptakan pelayanan cepat, tepat dan akurat. Teknologi informasi tersebut dinamakan Sistem Perbendaharaan Anggaran Nasional (SPAN).

SPAN diterapkan di KPPN Sorong pada tanggal 2 Februari 2015. Kewenangan hak akses SPAN diberikan KPPN Sorong pada satuan kerja melalui suatu prosedur permohonan hak akses. Atas permohonan tersebut KPPN Sorong memberikan surat penyampaian hak akses yang kemudian dikirimkan melalu pos ke alamat satuan kerja yang bersangkutan. Kemudian satuan kerja dapat mengakses SPAN dengan username dan password akun yang tertera pada surat penyampaian hak akses.

Berdasarkan observasi langsung, ditemui satuan kerja yang tidak membawa identitas saat memberikan surat permohonan hak akses ke KPPN Sorong. Hal tersebut menunjukan kelemahan otentikasi pesan antara satuan kerja dengan KPPN Sorong. Selain itu, surat penyampaian hak akses yang diberikan KPPN Sorong kepada satuan kerja melalui pos dapat menyebabkan kerahasian data pada surat penyampaian hak akses jatuh pada pihak yang tidak berwenang.

Maka dari itu diperlukan layanan keamanan otentikasi pesan antara satuan kerja dengan KPPN Sorong dalam memberikan surat permohonan hak akses dan surat penyampaian hak akses aplikasi monitoring online SPAN. Layanan keamanan kerahasiaan data pula dibutuhkan pada surat permohonan hak akses dan surat penyampaian hak akses tersebut. Salah satu mekanisme keamanan yang dapat diterapkan adalah *digital signature* dan kriptografi.

Digital signature dapat memberikan layanan keamanan otentikasi pesan. Layanan keamanan otentikasi pesan menggunakan *digital signature* dapat diwujudkan oleh proses *sign* dan proses *verify*. Proses *sign* akan membentuk tanda tangan digital untuk suatu dokumen. Tanda tangan digital tersebut kemudian digunakan pada proses *verify* untuk melakukan otentikasi pada dokumen sehingga validitas tanda tangan digital pada dokumen dapat diketahui. *Digital Signature Algorithm* (DSA) merupakan salah satu skema digital signature yang dipublikasi oleh *National Institute of Technology and Standard* (NIST) [1]. Terdapat 2 proses pada DSA, yaitu proses *sign* dan proses *verify*. Proses *sign* DSA menggunakan fungsi *hash* untuk menghasilkan sidik pesan (*message digest*) suatu dokumen. Dengan sidik pesan dan kunci privat, proses *sign* DSA menghasilkan tanda tangan digital untuk suatu dokumen. Proses *verify* DSA pula menggunakan fungsi *hash* pada dokumen yang akan di otentikasi validitasnya. Dengan sidik pesan dan kunci publik, proses verify DSA dapat melakukan otentikasi tanda tangan digital pada suatu dokumen. Selain layanan keamanan otentikasi pesan, layanan keutuhan data pun diwujudkan oleh *Digital Signature Algorithm.*

Kriptografi merupakan mekanisme keamanan yang dapat memberikan layanan keamanan berupa kerahasian data melalui proses enkripsi dan dekripsi. Enkripsi merupakan proses mengubah teks asli (*plaintext*) menjadi teks sandi (*ciphertext*) sedangkan dekripsi merupakan kebalikan dari proses enkripsi yang mengembalikan teks sandi menjadi teks aslinya. *Advanced Encryption Standard* (AES) merupakan salah satu kriptografi simetri yang ditetapkan oleh *National Institute of Technology and Standard* (NIST) pada tahun 2000 sebagai sistem penyandian [1]. Pada proses enkripsi menggunakan AES, terdapat sejumlah ronde yang dilakukan untuk melakukan transformasi-transformasi pada teks asli untuk mendapat teks sandi. Sedangkan pada proses dekripsi AES melakukan invers transformasi pada teks sandi untuk mendapatkan teks asli kembali.

Berdasarkan uraian diatas maka penulis melakukan penelitian implementasi *digital signature* dan kriptografi pada penyampaian hak akses ke aplikasi monitoring online SPAN di KPPN Sorong dengan skema *Digital Signature Algorithm* dan kriptografi *Advanced Encryption Standard*.

1.2 Identifikasi Masalah

Berdasarkan latar belakang masalah terdapat beberapa identifikasi masalah sebagai berikut:

1. Bagaimana menyediakan layanan keamanan otentikasi pesan antara satuan kerja dengan KPPN Sorong dalam memberikan surat permohonan hak akses dan surat penyampaian hak akses aplikasi monitoring online SPAN.
2. Bagaimana menyediakan layanan keamanan kerahasiaan data pada surat permohonan hak akses dan surat penyampaian hak akses aplikasi monitoring online SPAN di wilayah kerja KPPN Sorong.

1.3 Maksud dan Tujuan

Maksud penulis melakukan penelitian ialah membangun sistem Akses SPAN yang menerapkan *Digital Signature Algorithm* (DSA) sebagai mekanisme keamanan otentikasi pesan dan kriptografi *Advanced Encryption Standard* (AES) sebagai mekanisme keamanan kerahasiaan data.

Adapun tujuan penulis melakukan penelitian ini, diantaranya:

1. Menyediakan layanan keamanan otentikasi pesan antara satuan kerja dengan KPPN Sorong dalam memberikan surat permohonan hak akses dan surat penyampaian hak akses aplikasi monitoring online SPAN.
2. Menyediakan layanan keamanan kerahasiaan data pada surat permohonan hak akses dan surat penyampaian hak akses aplikasi monitoring online SPAN di wilayah kerja KPPN Sorong.

1.4 Batasan Masalah

Terdapat beberapa batasan masalah pada penelitian ini, diantaranya:

1. Dokumen digital yang digunakan sebagai masukan sistem adalah surat permohonan hak akses dan surat penyampaian hak akses.
2. Jenis dokumen digital adalah dokumen dengan format **.pdf*.
3. Mekanisme keamanan otentikasi menggunakan metode *Digital Signature Algorithm* (DSA).

4. Mekanisme kerahasiaan data menggunakan metode *Advanced Encryption Standard* (AES) dengan panjang kunci 128 bit.
5. Perangkat lunak dibangun berbasis web.
6. Metode pengembangan perangkat lunak menggunakan pendekatan *Object Oriented Analysis Design* (OOAD)
7. Bahasa pemrograman yang digunakan untuk membangun perangkat lunak adalah bahasa pemrograman PHP (*server-side*) dan Javascript (*client-side*).
8. Implementasi metode *Advanced Encryption Standard* (AES) menggunakan *library Web Cryptography API.*
9. Database Management System (DBMS) yang digunakan adalah MySQL.

1.5 Metodelogi Penelitian

Metodologi penelitian merupakan cara yang digunakan untuk menyelediki masalah yang memerlukan pemecahan. Metodologi penelitian yang digunakan adalah metodologi penelitian kualitatif.

1.5.1 Metode Pengumpulan Data

Metode pengumpulan data yang digunakan pada penelitian ini adalah:

1. Wawancara

Metode wawancara digunakan untuk identifikasi masalah dan prosedur yang berjalan di KPPN Sorong berkaitan dengan topik penelitian. Selain itu wawancara pula digunakan sebagai sarana penilaian yang disediakan untuk KPPN Sorong terhadap sistem yang dibangun.

2. Kuesioner

Kuesioner digunakan sebagai sarana penilaian yang disediakan untuk satuan kerja terhadap sistem yang dibangun.

3. Observasi

Metode observasi dilaksanakan dengan melakukan pengamatan secara langsung terhadap prosedur yang berjalan di KPPN Sorong yang berkaitan dengan topik penelitian.

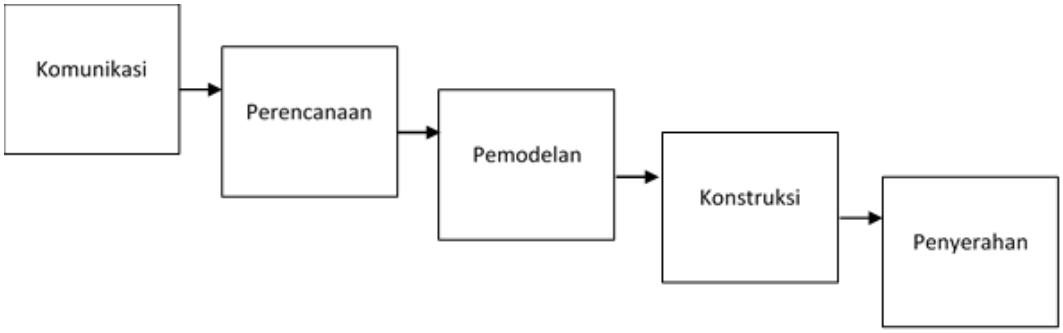
4. Studi Pustaka

Metode studi pustaka dilakukan dengan menelaah buku, jurnal, artikel yang berhubungan dengan topik penelitian.

1.5.2 Metode Pembangunan Perangkat Lunak

Metode pengembangan perangkat lunak yang digunakan adalah model *waterfall*. Dengan model *waterfall* spesifikasi kebutuhan untuk suatu permasalahan dapat dipahami dengan baik karena aktifitas kerangka kerja bersifat linier dari komunikasi hingga ke penyerahan [2].

Model pembangunan perangkat lunak *waterfall* dapat diilustrasikan seperti pada Gambar I-1.



Gambar I-1 Metode pengembangan perangkat lunak waterfall

1. Komunikasi

Pada tahap ini, aktifitas kerangka kerja dilakukan untuk memperoleh spesifikasi kebutuhan dalam pembangunan sistem Akses SPAN. Alat pengumpulan data dijadikan perantara pada tahap ini.

2. Perencanaan

Tahap perencanaan dilakukan sebagai tindak lanjut kerangka aktifitas komunikasi. Pada tahap ini spesifikasi kebutuhan untuk pembangunan sistem Akses SPAN mulai ditegaskan.

3. Pemodelan

Setelah tahap perencanaan terealisasi, tahap pemodelan dilakukan untuk membuat pemodelan-pemodelan dalam pembangunan sistem Akses SPAN berdasarkan tahap perencanaan.

4. Konstruksi

Pada tahap konstruksi implementasi mulai dilaksanakan. Sistem Akses SPAN mulai dikembangkan berdasarkan hasil pemodelan.

5. Penyerahan

Setelah kerangka aktifitas sebelumnya terlaksana, pada tahap ini sistem Akses SPAN diserahkan kepada pengguna.

1.6 Sistematika Penulisan

Adapun sistematika penulisan laporan dari penelitian ini adalah sebagai berikut:

BAB I PENDAHULUAN
Pada bab ini dijelaskan latar belakang masalah, identifikasi masalah, maksud dan tujuan, metodologi penilitian yang meliputi metode pengumpulan dan metode pembangunan perangkat lunak.

BAB II TINJAUAN TEORI
Pada bab ini disajikan profil tempat penelitian yaitu Kantor Pelayanan Perbendaharaan Negara Sorong meliputi sejarah, visi dan misi, logo dan struktur organisasi. Selain itu disajikan pula landasan teori terkait dengan penelitian, diantaranya digital signature dan kriptografi.

BAB III ANALISIS DAN PERANCANGAN SISTEM
Pada bab ini dibahas beberapa analisis serta perancangan sistem.

BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM
Pada bab ini membahas implementasi dan pengujian sistem berdasarkan analisis dan perancangan sistem.

BAB V KESIMPULAN DAN SARAN
Pada bab ini disajikan kesimpulan dan saran dari penelitian yang telah dilakukan.