BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Pusat Sumber Daya Air Tanah dan Geologi Lingkungan merupakan sebuah instansi pemerintah yang bergerak di bidang air tanah dan geologi lingkungan. Instansi ini dibentuk untuk melayani dan menyediakan informasi bagi masyarakat dalam bidang yang berhubungan dengan perizinan dan penelitian Air Tanah dan Geologi Lingkungan. Perizinan yang diberikan oleh instansi ini antara lain seperti perizinan pengusahaan air tanah, penelitian kondisi air tanah dan lain – lain. Salah satu contoh kegiatan perizinan yang dilakukan adalah dalam hal perizinan pengusahaan air tanah bagi individu ataupun perusahaan yang hendak mengusahakan sumber daya air tanah yang ada di lingkungannya.

Pada saat ini sudah terdapat sebuah sistem yang mengelola perizinan pengusahaan air tanah, akan tetapi masih terdapat banyak masalah. Ketika seluruh proses sudah dikelola oleh sebuah sistem informasi maka terdapat hal yang perlu diperhatikan, yaitu keamanan sistem informasi. Pengembangan keamanan sistem informasi yang akan dibahas, dirancang dan akan diterapkan pada Sistem Informasi Perizinan Pengusahaan Sumber Daya Tanah lebih ke arah pencegahan, bukan penanggulangan karena sejauh ini belum terjadi masalah terkait keamanan sistem informasi. 4 faktor seperti konfidensialitas, integritas, autentikasi dan ketiadaan penyangkalan tersebut selayaknya diterapkan pada sebuah sistem informasi agar seluruh transaksi data yang terjadi, data yang disimpan dan data yang diolah menjadi informasi dapat dipercaya mengingat seluruh data yang terdapat pada sistem adalah aset informasi.

Masalah lainnya adalah masalah yang berkaitan dengan tujuan sistem ini dibangun. Tujuan dibangunnya sistem ini salah satunya adalah seluruh proses perizinan dapat berjalan sesuai SOP. Masalah yang menjadi penghambat adalah proses penerbitan lembar kendali yang harus di tanda tangani oleh petugas administrasi dan petugas teknis dan surat rekomendasi teknis yang harus di tanda tangani Kepala Badan Geologi secara langsung. Dengan demikian, agar salah satu

tujuan sistem ini dibangun bisa tercapai perlu adanya sebuah cara agar petugas administrasi, petugas teknis dan Kepala Badan Geologi bisa menanda tangani surat rekomendasi teknis meskipun tidak berada di kantor.

Hasil atau keluaran yang diharapkan dari sistem ini adalah dokumen lembar kendali atau surat rekomendasi teknis pengusahaan air tanah dalam bentuk dokumen elektronik. Akan tetapi, sangat mungkin untuk terjadi pemalsuan dokumen elektronik izin pengusahaan air tanah itu sendiri. Untuk mencegah hal tersebut, sistem harus bisa menanganinya dengan baik. Mengingat proses perizinan ini sangat penting dan hasil dari sistem adalah dokumen perizinan yang bersifat legal, jika tidak terdapatnya keamanan sistem yang baik maka dikhawatirkan disalahgunakan oleh orang-orang yang tidak berkepentingan.

Terdapat sebuah cara yang disebut digital signature. Digital signature adalah sebuah mekanisme atau cara yang bisa diterapkan untuk menjadikan sebuah dokumen digital legal secara hukum. Cara ini memungkinkan petugas administrasi, petugas teknis dan Kepala Badan Geologi tetap bisa memberikan keputusan meskipun tidak berada di kantor.

Berdasarkan permasalahan yang ada, maka perlu diterapkan keamanan sistem informasi dan *digital signature* untuk memenuhi 4 faktor keamanan sistem informasi dan memberikan legalitas pada dokumen digital sehingga memudahkan dalam proses dan pengelolaan perizinan. Teknologi *digital signature* digunakan karena bisa membuat dokumen fisik dan dokumen digital mendapatkan tingkat legalitas yang sama.

1.2 Perumusan Masalah

Perumusan masalah yang dapat di ambil berdasarkan latar belakang masalah yang telah dijelaskan adalah bagaimana menerapkan keamanan sistem informasi dan *digital signature* pada Sistem Informasi Perizinan Pengusahaan Air Tanah di Pusat Sumber Daya Air Tanah dan Geologi Lingkungan.

1.3 Maksud dan Tujuan

Maksud dan tujuan menerapkan keamanan sistem informasi dan *digital signature* pada Sistem Informasi Perizinan Pengusahaan Air Tanah pada Pusat Sumber Daya Air Tanah dan Geologi Lingkungan adalah sebagai berikut:

1.3.1 Maksud

Maksud dari penelitian yang dilakukan yaitu, menerapkan keamanan sistem informasi yang bersifat pencegahan dan *digital signature* pada Sistem Informasi Perizinan Pengusahaan Air Tanah di Pusat Sumber Daya Air Tanah dan Geologi Lingkungan. Adapun maksud dari pencegahan adalah dengan mengimplementasi 4 faktor keamanan sistem informasi seperti kerahasiaan, integritas data, otentifikasi dan ketiadaan penyangkalan.

1.3.2 Tujuan

Tujuan dari diterapkannya keamanan sistem informasi dan *digital signature* pada sistem informasi Perizinan Pengusahaan Air Tanah adalah

1. Mencegah aset informasi yang dimiliki dan dikelola oleh sistem informasi dari ancaman pihak-pihak yang tidak berhak dalam kepemilikan atau penggunaan aset informasi perizinan pengusahaan air tanah dan memastikan data masukan sesuai format dan kebutuhan untuk memproses permohonan surat rekomendasi teknis.
2. Membuat petugas administrasi, petugas teknis dan Kepala Badan Geologi agar bisa menandatangani lembar kendali dan surat rekomendasi teknis dimanapun dan kapanpun dan membuat dokumen lembar kendali atau surat rekomendasi teknis pengusahaan air tanah elektronik yang legal secara hukum.

1.4 Batasan Masalah

Batasan masalah yang ada dalam penerapan keamanan sistem informasi dan *digital signature* pada sistem informasi permohonan perizinan pengusahaan air tanah ini mencakup 3 hal, yaitu data yang diolah, bagaimana proses pengolahannya dan apa yang dihasilkan dari olahan data tersebut.

1. Data yang Diolah

   Data yang diolah ketika penerapan *digital signature* adalah data pemeriksaan administrasi dan data pemeriksaan teknis yang menghasilkan dokumen perizinan pengusahaan air tanah digital. Sedangkan keamanan sistem informasi yang diterapkan untuk mendukung keamanan dari proses penerapan *digital signature* adalah dengan data penanda tangan, pengelolaan *public key*, pengelolan *private key* dan penyimpanan histori perubahan data baik data penanda tangan sampai data dokumen perizinan pengusahaan air tanah.

2. Proses Pengolahan Data

   Ketika pertama kali proses pencetakan surat rekomendasi teknis berjalan, sistem akan membangkitkan *private key* dan *public key* kemudian sistem mengenkripsi dokumen perizinan lalu menyisipkan *public key*, *private key* dan hasil enkripsi dokumen sehingga menghasilkan dokumen digital yang bisa diuji legalitasnya. Sistem akan dikembangkan dengan menambahkan 2 faktor autentikasi diantaranya penggunaan *password* ketika akan membuat *digital signature* dan melekatkan gambar tanda tangan penanda tangan sebagai sesuatu yang merupakan ciri/karakteristik seorang individu.

3. Pengguna

   Terdapat 3 jenis pengguna yang diberikan izin untuk menggunakan *digital signature*, yaitu petugas administrasi, petugas teknis dan kepala Badan Geologi. Petugas administrasi dan petugas teknis akan menggunakan *digital signature* pada dokumen lembar kendali sedangkan kepala Badan Geologi akan menggunakan *digital signature* pada surat rekomendasi teknis pengusahaan air tanah.

4. Metode

   Metode yang digunakan pada penerapan *digital signature* ini adalah dengan membangkitkan *Private key* dan *public key* dengan menggunakan algoritma RSA dan teknik hashing SHA256. Algoritma RSA digunakan karena algoritma ini bisa membangkitkan *private key* dan *public key* tanpa keterlibatan pemohon, sedangkan algoritma Diffie-Hellman, pemohon

harus terlibat. Terlibat dalam hal ini adalah algoritma Diffie-Hellman memerlukan pemohon berinteraksi dengan Pusat Sumber Daya Air Tanah dan Geologi Lingkungan dengan cara memberikan sejumlah bilangan yang akan digunakan untuk membangkitkan *private key* dan *public key*. Sedangkan teknik *hashing* SHA256 digunakan karena teknik ini merupakan generasi kedua dan perbaikan dari teknik *hashing* SHA1. SHA256 mampu menghasilkan 256 *bit* atau 32 *byte* nilai *hash*. SHA256 juga menghasilkan 64 karakter *hexadecimal* atau 24 karakter lebih panjang dari pada SHA1. Sistem juga akan menyisipkan tanda tangan fisik pada surat rekomendasi teknis pengusahaan air tanah. *Public key* dan *private key* akan dikelola oleh petugas administrasi. Untuk mengevaluasi keamanan sistem informasinya terutama mengevaluasi manajemen resiko sistem informasinya, metode yang digunakan adalah metode OCTAVE Allegro. Metode OCTAVE Allegro dipilih karena metode ini fokus terhadap pengamanan aset informasi dan proses bisnis dari sebuah instansi.

5. Perangkat Lunak yang Digunakan

   Sistem informasi pengusahaan air tanah ini berbasis *web* dengan demikian perangkat yang akan digunakan untuk membuat kunci publik dan kunci privat harus mendukung arsitektur web. Perangkat lunak OpenSSL digunakan karena PHP sendiri sudah menyediakan fungsi-fungsi untuk membangkitkan kunci publik dan kunci privat. Sedangkan untuk menyisipkan gambar tanda tangan, kunci publik dan kunci privat pada dokumen izin pengusahaan air tanah menggunakan perangkat lunak TCPDF.

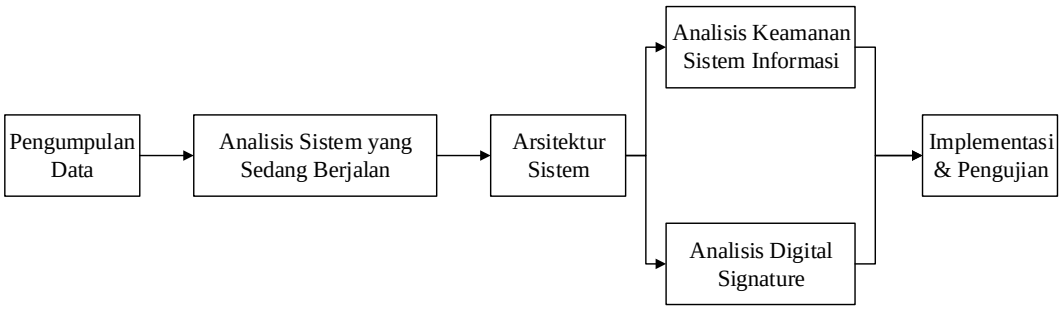
6. Keluaran Sistem

   Keluaran sistem yang didapatkan dari penerapan *digital signature* adalah terjaminnya keamanan aset informasi yang dimiliki dan dikelola oleh Pusat Sumber Daya Air Tanah dan Geologi Lingkungan dan dokumen izin pengusahaan air tanah dalam bentuk digital yang legal secara hukum berdasarkan UU ITE nomor 11 tahun 2008 dan Peraturan Pemerintah

nomor 82 tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

1.5 Metodologi Penelitian

Metodologi penelitian yang digunakan dalam penerapan keamanan sistem informasi dan *digital signature* pada sistem informasi perizinan pengusahaan air tanah adalah metodologi penelitian kualitatif. Metodologi penelitian kualitatif adalah satu pendekatan penelitian yang mengungkap situasi sosial tertentu dengan mendeskripsikan kenyataan secara benar, dibentuk oleh kata-kata berdasarkan teknik pengumpulan dan analisis data yang relevan yang diperoleh dari situasi yang alamiah [1]. Tahapan penelitian yang dilakukan secara garis besar dapat di lihat pada gambar 1.1.



Gambar 1.1 Tahapan Penelitian

Berikut ini adalah penjelasan dari gambar 1.1 yaitu tahapan penelitian

1. Pengumpulan Data
   a. Observasi

      Studi lapangan adalah metode pengumpulan data yang dilakukan dengan cara mengunjungi tempat yang akan diteliti dan pengumpulan data dilakukan secara langsung. Metode pengamatan adalah metode pengumpulan data yang penulis gunakan. Pengamatan adalah pengumpulan data dengan cara mengamati secara langsung di mulai dari proses login, penambahan data permohonan baru dan perpanjangan, pengunggahan dokumen persyaratan, disposisi surat sampai penerbitan surat rekomendasi teknis.

b. Studi Literatur

Studi literatur adalah metode pengumpulan data yang dilakukan dengan cara mempelajari, meneliti dan menelaah berbagai literatur-literatur dari perpustakaan yang bersumber dari buku-buku, teks, jurnal ilmiah, situs-situs di internet, dan bacaan-bacaan yang ada kaitannya dengan topik penelitian. Berikut ini adalah beberapa literatur yang menjadi pendukung penelitian

1. Pro PHP Security (Chris Snyder, Thomas Myer & Michael Southwell, 2010). Buku ini menjelaskan beberapa teknik-teknik dasar pengamanan pada aplikasi berbasis web. Buku ini juga menjelaskan jenis-jenis enkripsi sekaligus menjelaskan bagaimana membuat public key dan private key yang digunakan untuk digital signature. Public key dan private key ini dibangkitkan menggunakan algoritma RSA kemudian digunakan pada modul OpenSSL [2].
2. Digital Signatures (S.R. Subramanya, Byung K. Yi, 2006). Paper ini menjelaskan apa itu digital signature, bagaimana cara kerjanya dan teknik enkripsi yang digunakan untuk digital signsatures. Menjelaskan bagaimana sebuah public key dan private key bisa dibangkitkan dan bagaimana cara memverifikasi dokumen digital dengan public key. Public key dibangkitkan dengan cara memasukan data seperti lokasi penerbit tanda tangan, siapa yang menanda tangan, kapan ditanda tangan untuk kemudian di enkripsi sehingga mendapatkan public key. Private key dibangkitkan dari data yang sama dengan data untuk membangkitkan public key tetapi ditambah dengan sandi dan spesifikasi enkripsi seperti algoritma yang digunakan dan jumlah bit yang digunakan. Kedua kunci tersebut akan di masukan pada dokumen PDF sehingga menghasilkan sebuah dokumen yang tertanda tangan secara digital [3].

3. The Manager's Guide to Web Application Security (Ron Lepofsky, 2014). Buku ini menjelaskan hal-hal non-teknis dalam keamanan sistem informasi seperti dampak yang akan terjadi jika keamanan tidak tersedia, tindakan preventif hingga hal-hal minor yang seringkali tidak diterapkan pada sistem informasi [4].
4. Peraturan Pemerintah No.82 Tahun 2012 tentang Penylenggaraan Sistem dan Transaksi Elektronik. Peraturan pemerintah ini, khususnya pasal 56 – 58 membahas secara spesifik tentang tanda tangan digital. Dimulai dari data apa saja yang perlu dipersiapkan, bagaimana prosesnya dan bagaimana memverifikasi dokumen digital yang tertanda tangan digital [5].

2. Analisis Sistem yang Sedang Berjalan

   Pada tahapan ini, dikarenakan topik skripsi adalah pengembangan, artinya sistem yang berjalan perlu di analisis untuk mengetahui proses bisnis secara umum. Dari tahapan ini bisa di dapatkan proses bisnis mana saja yang mungkin akan berubah untuk menyesuaikan dengan penerapan keamanan sistem informasi dan digital signature.
3. Arsitektur Sistem

   Pada tahapan ini sudah terlihat arsitektur sistem yang baru, yang akan diterapkan pada sistem informasi pengusahaan air tanah. Arsitektur sistem akan membahas proses bisnis yang baru. Arsitektur sistem juga sudah bisa memberikan gambaran dimana digital signature akan diterapkan dan siapa-siapa saja yang akan menggunakan digital signature.
4. Analisis dan Perancangan Keamanan Sistem Informasi

   Pada tahapan ini, keamanan sistem informasi akan di analisis menggunakan metode OCTAVE Allegro untuk menganalisis resiko pada aset informasi yang dimiliki sistem informasi pengusahaan air tanah. Hasil dari evaluasi ini kemudian akan di evaluasi lagi untuk mencari metode apa yang tepat untuk menindak lanjuti hasil analisis resiko aset informasi.

5. Analisis dan Perancangan Digital Signature

   Pada tahapan ini, analisis dan perancangan digital signature meliputi analisis data-data yang dibutuhkan untuk membuat digital signature kemudian analisis keamanan digital signature. Setelah itu, perancangan digital signature membahas tentang perancangan pengubahan sistem yang sedang berjalan, perancangan penerapan digital signature yang dimulai dari perancangan pengubahan data, pembuatan digital signature hingga perancangan verifikasi digital signature.

6. Implementasi dan Pengujian.

   Pada tahapan ini keamanan sistem informasi dan digital signature akan di implementasi untuk kemudian di uji untuk mengetahui berfungsi atau tidaknya keamanan sistem informasi dan digtal signature.

1.6 Sistematika Penulisan

Gambaran secara umum dari isi skripsi ini akan dijelaskan pada sistematika penulisan dari skripsi sebagai berikut:

BAB 1 PENDAHULUAN

Bab ini berisi pembahasan masalah umum yang berhubungan dengan penyusunan skripsi, yang meliputi latar belakang, rumusan masalah, maksud dan tujuan, batasan masalah, metode penelitian, dan sistematika penulisan.

BAB 2 TINJAUAN PUSTAKA

Bab ini berisi pembahasan mengenai profil Pusat Sumber Daya Air Tanah dan Geologi Lingkungan, yang meliputi sejarah, struktur organisasi, visi dan misi instansi, dan teori–teori yang berhubungan dengan pengembangan sistem informasi pengushaan air tanah.

BAB 3 ANALISIS DAN PERANCANGAN SISTEM

Bab ini berisi pembahasan tentang analisis masalah, analisis keamanan sistem informasi yang sedang berjalan, rekomendasi keamanan sistem informasi dan rekomendasi penerapan *digital signature* pada sistem informasi pengusahaan air tanah.

BAB 4 IMPLEMENTASI DAN PENGUJIAN SISTEM

Bab ini berisi implementasi keamanan sistem informasi dan *digital signature* berdasarkan hasil analisis masalah yang sebelumnya telah dijelaskan. Sistem yang dapat digunakan dengan baik harus melalui tahapan pengujian. Pengujian yang dilakukan adalah dengan membandingkan sistem yang tidak aman dengan sistem yang sudah diterapkan keamanan dan menguji validitas *digital signature*.

BAB 5 KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan mengenai seluruh hasil analisis dan penerapan keamanan sistem informasi dan *digital signature* pada sistem informasi perizinan pengusahaan air tanah, serta saran untuk keperluan pengembangan aplikasi selanjutnya.