ANALISIS DAN PERANCANGAN SISTEM OTENTIKASI KLIEN PADA WEBSITE MENGGUNAKAN SERTIFIKAT DIGITAL DENGAN SKEMA INFRASTRUKTUR KUNCI PUBLIK

Naskah Publikasi

diajukan oleh :

Rizaldi Arief Febrianto

07.21.0312

kepada

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

AMIKOM

YOGYAKARTA

2010

NASKAH PUBLIKASI

ANALISIS DAN PERANCANGAN SISTEM OTENTIKASI KLIEN PADA WEBSITE MENGGUNAKAN SERTIFIKAT DIGITAL DENGAN SKEMA INFRASTRUKTUR KUNCI PUBLIK

disusun oleh

Rizaldi Arief Febrianto

07.21.0312

Dosen Pembimbing,

Ema Utami, S.Si, M.Kom

NIK. 190302037

Tanggal 24 April 2010

Ketua Jurusan

Teknik Informatika

Ir. Abas Ali Pangera, M.Kom

NIK. 190302010

ANALYSIS AND DESIGN OF CLIENT AUTHENTICATION SYSTEM ON WEBSITE USING DIGITAL CERTIFICATE WITH PUBLIC KEY INFRASTRUCTURE SCHEME

ANALISIS DAN PERANCANGAN SISTEM OTENTIKASI KLIEN PADA WEBSITE MENGGUNAKAN SERTIFIKAT DIGITAL DENGAN SKEMA INFRASTRUKTUR KUNCI PUBLIK

Rizaldi Arief Febrianto
Jurusan Teknik Informatika
STMIK AMIKOM YOGYAKARTA

Abstract

Currently more and more digital certificates are used by agencies and individuals. Usage is also increasingly diverse, such as data encryption, client and server authentication, single-sign-on, and so forth. But with more and more use of digital certificates that can not be checked for validity has been encouraging the owners and creators of data security experts to create a new system called Public Key Infrastructure. Where is the organization that issued a digital certificate has a belief (trust) from other organizations that issue digital certificates and other organizations that also use digital certificates for client authentication.

Notably, currently the organizations that use internet services for electronic transactions with their clients being the victim subjects and objects caused by the weakness of the authentication system. In this thesis the author will only restrict the use of digital certificates as a method of client authentication on the website. This thesis is based on the study of the website application implementation by implementing the use of digital certificates for client authentication using Public Key Infrastructure schemes. With this application, the authentication system is expected to filter the client correctly so that valuable information in the website will be maintained and can not easily be accessed by other users who are not eligible.

Keywords *: Digital Certificate, Public Key Infrastructure, Authentication, SSL*

1. Pendahuluan

Saat ini sertifikat digital makin banyak digunakan oleh instansi dan perorangan. Penggunaannya pun makin beragam, seperti enkripsi data, otentikasi *client* dan *server*, *single-sign-on*, dan lain sebagainya. Namun dengan makin banyaknya penggunaan sertifikat digital yang tidak bisa dicek keabsahan pemilik dan pembuatnya telah mendorong pakar kemanan data untuk membuat sistem baru dengan nama Infrastruktur Kunci Publik. Dimana organisasi yang mengeluarkan sertifikat digital telah memiliki kepercayaan (*trust*) dari organisasi lain yang mengeluarkan sertifikat digital dan juga organisasi lain yang menggunakan sertifikat digital untuk otentikasi kliennya.

Perlu diketahui, bahwa saat ini organisasi pemakai jasa internet untuk transaksi elektronik beserta kliennya menjadi subyek dan obyek yang menjadi korban akan kelemahan sistem otentikasi. Dalam skripsi penulis hanya akan membatasi pada penggunaan sertifikat digital sebagai metode otentikasi klien pada *website*. Skripsi ini berdasarkan studi implementasi aplikasi *website* dengan menerapkan penggunaan sertifikat digital untuk otentikasi klien menggunakan skema Infrastruktur Kunci Publik. Dengan aplikasi ini, sistem otentikasi diharapkan mampu menyaring klien dengan benar sehingga informasi yang berharga dalam website akan terjaga dan tidak bisa diakses dengan mudah oleh pengguna lain yang tidak berhak.

2. Landasan Teori

2.1. Jaringan Komputer

Jaringan komputer adalah kumpulan dari beberapa komputer, baik yang berskala kecil seperti di rumah dan di kantor, yang berskala besar seperti antar kota dan antar provinsi, maupun yang berskala dunia (internasional) seperti antar negara dan antar benua, dimana komputer-komputer tersebut saling bekerjasama untuk mencapai tujuan yang sama yaitu terciptanya komunikasi data dan informasi serta saling berbagi sumber daya.

Berdasar peranan dan fungsi komputer, jaringan komputer dibagi menjadi dua:

1. Jaringan *client-server*

   Jaringan *client-server* sering disebut sebagai *dedicated server network* dimana komputer *server* menyediakan fasilitas bagi komputer-komputer lain. Sedangkan komputer *client* menerima dan menggunakan fasilitas yang disediakan oleh komputer *server*.
2. *Jaringan peer-to-peer*

   Jaringan *peer-to-peer* sering disebut sebagai *non-dedicated server network* dimana komputer *server* tidak hanya berperan sebagai *server* tetapi berperan juga sebagai

komputer *client* atau *workstation*. Semua komputer saling memberikan fasilitasnya dalam membangun jaringan.

Berdasar lingkup atau luas daerah kerja secara geografis, jaringan komputer dibagi menjadi tiga, yaitu:

1. LAN (Local Area Network)
   Jaringan komputer dengan area kerja kecil. LAN mempunyai jangkauan maksimal 100 meter.
2. MAN (Metropolitan Area Network)
   Jaringan komputer dengan area kerja besar. MAN mempunyai jangkauan 10 km sampai dengan 50 km.
3. WAN (Wide Area Network)
   Jaringan komputer dengan area kerja sangat besar. WAN mempunyai jangkauan antar negara dan antar benua.

2.2. Internet

Internet mempunyai banyak definisi, tergantung dari sudut pandang mana mengartikannya. Internet berasal dari kata *interconnection networking* yang berarti hubungan berbagai komputer dengan berbagai tipe dan jenis yang membentuk suatu kesatuan sistem melalui jalur komunikasi yang mencakup seluruh dunia. Dari sudut pandang teknis, internet adalah jaringan komputer seluruh dunia yang terdiri dari jutaan komputer dimana komputer-komputer tersebut dapat saling bertukar informasi. Dari segi ilmu pengetahuan, internet adalah sebuah perpustakaan yang sangat besar dimana didalamnya terdapat buku, artikel, jurnal, kliping, foto dan lain-lainnya dalam bentuk dokumen elektronik dengan jumlah yang sangat banyak. Komputer dalam internet terhubung melalui perantara TCP/IP (*Transmission Control Protocol/Internet Protocol*), yaitu sebuah protokol standar yang mengatur tentang metode komunikasi data antar komputer dalam jaringan internet. Dengan perantara TCP/IP maka berbagai macam *platform* sistem komputer bisa terkoneksi.

Salah satu aplikasi internet yang paling banyak digunakan adalah *World Wide Web* (WWW) atau sering disingkat dengan *web* saja. Melalui *web* segala macam informasi bisa didapat dari seluruh dunia. *Web* dapat mencapai sasaran masyarakat yang tidak mungkin dicapai oleh majalah atau koran biasa. Semua layanan dalam internet berisi dokumen-dokumen yang berupa informasi teks. Namun dengan aplikasi *web* maka layanan internet akan bernilai tambah seiring kemampuannya menampilkan teks, gambar, suara, video dan animasi.

2.3. Keamanan Informasi

Keamanan informasi memiliki arti menjaga informasi dan sistem informasi dari penggunaan akses ilegal, gangguan, modifikasi maupun perusakan. Tujuan utama kemanan informasi adalah untuk menjaga kerahasiaan dan keutuhan informasi. Keamanan informasi memiliki beberapa batasan penting, antara lain:

1. *Confidentiality*

   Confidentiality merupakan aspek yang menjamin kerahasiaan data.

2. *Integrity*

   Integrity merupakan aspek yang menjamin bahwa data tidak boleh berubah tanpa ijin pihak yang berwenang (*authorized*).

3. *Availability*

   Availability merupakan aspek yang menjamin bahwa data tersedia ketika dibutuhkan.

4. *Non-repudiation*

   Non-repudiation merupakan aspek yang menjamin bahwa pelaku transaksi tidak dapat mengelak atau menyangkal telah melakukan transaksi elektronik.

Dalam sistem transaksi konvensional, aspek *non-repudiation* ini diimplementasikan dengan menggunakan tanda tangan. Dalam transaksi elektronik, aspek *non-repudiation* dijamin dengan penggunaan tanda tangan digital *(digital signature)*, penyediaan log (*audit trail*), dan pembuatan sistem agar dapat diperiksa dengan mudah (*auditable*). Implementasi mengenai hal ini sudah tersedia, hanya perlu diaktifkan. Dalam UU Informasi dan Transaksi Elektronik, tanda tangan digital diakui sama sahnya dengan tanda tangan konvensional.

Tabel 2.1. Isu Keamanan Informasi, Permasalahan dan Solusi

No.	Isu Keamanan	Permasalahan	Solusi
1.	*Authorization* (Otorisasi)	Apakah seseorang diijinkan untuk mengakses informasi spesifik pada suatu sistem?	Akses kontrol sistem dengan identifikasi *username* dan *password*
2.	*Confidentiality* (Kerahasiaan)	Apakah transaksi elektronik yang dilakukan dimata-matai oleh orang lain?	Penggunaan algoritma enkripsi dengan kunci publik dan privat
3.	*Integrity* (Integritas)	Apakah informasi yang dikirim, diproses, dan diterima benar-benar utuh tanpa ada penambahan atau pengurangan?	Cek integritas dengan tanda tangan digital

4.	*Authentication* (Otentikasi)	Apakah seseorang yang melakukan akses terhadap suatu sistem informasi benar-benar merupakan orang yang berhak?	Otentikasi dengan sertifikat digital
5.	*Non-repudiation (anti sangkal)*	Apakah transaksi elektronik benar-benar telah dilakukan oleh seseorang?	Penyediaan log untuk audit

2.4. Kriptografi

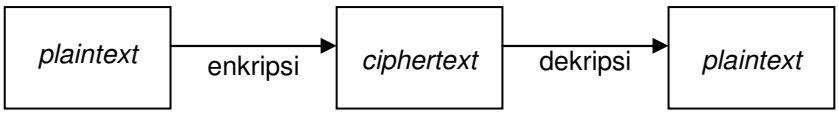
Kriptografi menjadi ilmu yang sangat penting dan mulai menonjol sejak digunakan pada pengiriman perintah dan pesan pada masa Perang Dunia II. Saat itu kriptografi digunakan untuk membuat kode dan mengacak pesan agar tidak bisa diketahui oleh lawan. Saat ini kriptografi semakin dikembangkan untuk aplikasi pertahanan keamanan maupun untuk aplikasi bisnis.

Sistem pengamanan informasi dengan kriptografi terdiri dari 2 proses penting:

1. Proses Enkripsi

   Proses enkripsi adalah suatu proses yang mengubah *plaintext* (pesan asli) menjadi *ciphertext* (pesan acak).
2. Proses Dekripsi

   Proses dekripsi adalah suatu proses yang mengubah *ciphertext* menjadi *plaintext*. Pesan acak dikembalikan ke pesan semula.



Gambar 2.1. Proses Kriptografi

Proses kriptografi (enkripsi dan dekripsi) menggunakan kunci atau algoritma kriptografi tertentu untuk mengubah pesan asli menjadi pesan acak dan sebaliknya. Berdasarkan arah enkripsi maka ada dua jenis kriptografi, yaitu:

1. Enkripsi satu arah

   Proses hanya mengenal enkripsi dan tidak mengenal dekripsi.
2. Enkripsi dua arah

   Proses mengenal enkripsi dan dekripsi.

Berdasarkan kunci yang digunakan, maka ada dua jenis kriptografi:

1. Kunci simetrik

   Proses enkripsi dan dekripsi pesan menggunakan satu kunci yang sama.

2. Kunci asimetrik

   Proses enkripsi dan dekripsi pesan menggunakan dua kunci yang saling terkait.

2.5. Sertifikat Digital

Sertifikat digital merupakan berkas digital yang berisi kunci publik dan informasi penting mengenai jati diri pemiliknya, antara lain nama, alamat, *email*, pekerjaan, jabatan, organisasi, unit organisasi, dan algoritma kriptografi yang digunakan sebagai suatu informasi yang disahkan oleh pihak terpercaya. Sertifikat digital tersebut ditandatangani oleh sebuah otoritas sertifikat yang sering disebut *Certification Authority* (CA).

<table>
<tr><td rowspan="9">Certificate</td><td>Version</td></tr>
<tr><td>Serial Number</td></tr>
<tr><td>Algorithm Identifier</td></tr>
<tr><td>Issuer</td></tr>
<tr><td>Validity
(not before, not after)</td></tr>
<tr><td>Subject</td></tr>
<tr><td>Subject Public Key Information
(public key algorithm, subject public key)</td></tr>
<tr><td>Issuer Unique Identifier</td></tr>
<tr><td>Subject Unique Identifier</td></tr>
<tr><td>Extension</td></tr>
<tr><td colspan="2">Certificate Signature Algorithm</td></tr>
<tr><td colspan="2">Certificate Signature</td></tr>
</table>

Gambar 2.2. Struktur Sertifikat Digital

2.6. Infrastruktur Kunci Publik

Infrastruktur Kunci Publik (IKP) adalah sebuah cara untuk otentikasi, pengamanan data dan perangkat anti sangkal. Secara teknis, IKP adalah implementasi dari berbagai teknik kriptografi yang bertujuan untuk mengamankan data, memastikan keaslian data dan pengirimnya serta mencegah penyangkalan. Teknik-teknik kriptografi yang

digunakan antara lain fungsi *hash*, algoritma kriptografi simetrik, dan algoritma kriptografi asimetrik. Fungsi *hash* akan digunakan bersama dengan algoritma kriptografi asimetrik dalam bentuk tanda tangan digital untuk memastikan integritas atau keaslian data berikut pengirimnya. Algoritma kriptografi simetrik digunakan untuk mengamankan data saat berkomunikasi. Dalam IKP penggunaan algoritma enkripsi simetrik tidak secara langsung didefinisikan tetapi telah diimplementasikan oleh berbagai perangat lunak melalui berbagai macam protokol yang ada. IKP diwujudkan dalam bentuk kolaborasi antar komponen-komponennya. Wujud implementasi IKP adalah penggunaan sertifikat digital untuk otentikasi klien.

IKP memiliki beberapa komponen penting yang menyusunnya. Adapun komponen-komponen dalam IKP terdiri dari:

1. *Certification Authority* (CA)
2. *Key Repository*
3. *Certificate*
4. *Certificate Revocation List* (CRL)
5. *Management Function*
6. *Policy Approving Authority*
7. *Policy Certification Authority*
8. *Registration Authority* (RA)

IKP memiliki beberapa subyek penting dalam pembangunannya. Adapun subyek-subyek yang terlibat dalam IKP terdiri dari:

1. *Certification Authority* (CA)

   Merupakan lembaga yang mengeluarkan sertifikat digital. Lembaga ini bisa berasal dari luar (*external-CA*) maupun dari dalam lembaga itu sendiri (*internal-CA*). Adapun contoh CA yang berasal dari luar adalah DigiCert Inc, Entrust Inc, Equifax Eecure Inc, ElobalSign Inc, SecureTrust Corporation, Thawte Inc, dan VeriSign Inc.
2. *End Entity* (EE)

   Merupakan individu ataupun lembaga yang bertindak sebagai pemilik sertifikat digital. EE adalah obyek utama dalam skema IKP.
3. *Registration Authority* (RA)

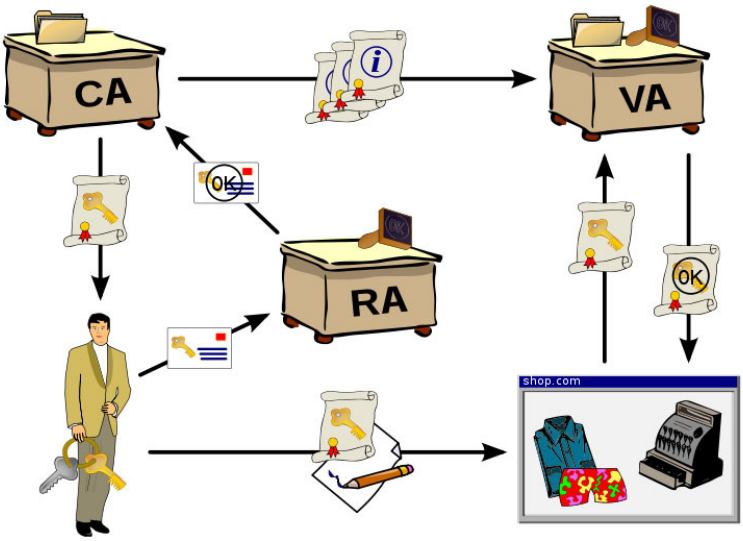
   Merupakan lembaga perantara antara CA dengan EE. Lembaga ini berfungsi mengumpulkan data personal dari EE yang selanjutnya meminta pengeluaran sertifikat digital ke CA untuk EE tersebut.
4. *Validation Authority* (VA)

   Merupakan lembaga independen pihak ketiga yang berperan mengatur proses verifikasi dan validasi sertifikat digital secara *online*. VA menyimpan daftar sertifikat digital yang dikeluarkan oleh CA dan berfungsi sebagai *repository* database sertifikat

digital. Peranan VA saat ini masih bersifat pelengkap dalam skema IKP, karena peranannya masih dipegang secara penuh oleh CA.

IKP dibangun dalam suatu skema proses. Adapun skema IKP dijelaskan dalam alur sebagai berikut:

1. Pengguna yang bertindak sebagai EE meminta sertifikat digital melalui perantara RA.
2. RA meminta pengeluaran sertifikat digital untuk EE dengan cara mengirimkan data personal EE ke CA.
3. CA mengeluarkan sertifikat digital dan mengembalikannya ke EE.
4. CA mengirim data sertifikat digital yang telah dikeluarkan ke VA.
5. EE sudah bisa menggunakan sertifikat digital miliknya untuk bertransaksi secara elektronik.



Gambar 2.3. Skema Infrastruktur Kunci Publik

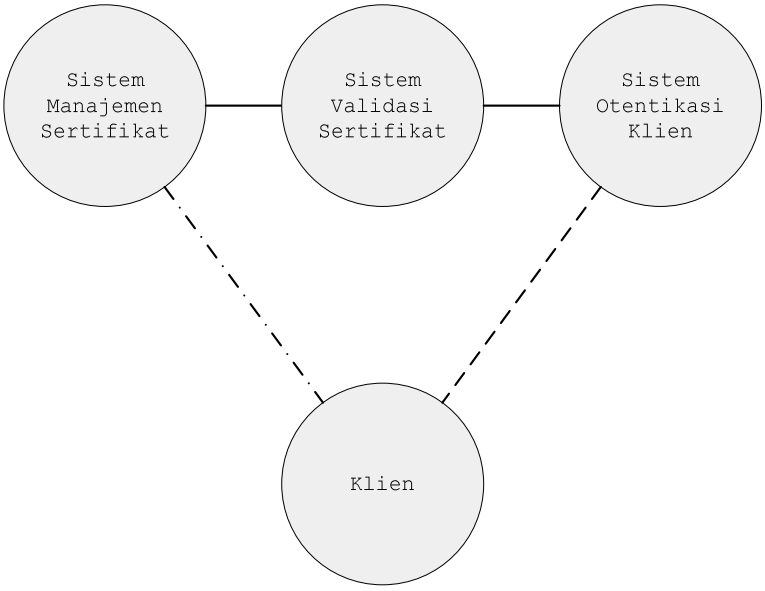
IKP melindungi aspek keamanan informasi yang dikirimkan saat bertransaksi. Adapun fungsi yang dilakukan IKP dijabarkan sebagai berikut:

1. Mengotentikasi identitas. Dengan sertifikat digital yang dikeluarkan oleh IKP maka tiap pihak dapat mengotentikasi pihak lawan dalam melakukan transaksi sehingga pihak dapat meyakini bahwa pihak yang melakukan transaksi adalah pihak yang berhak.
2. Verifikasi integritas dokumen. Dengan adanya sertifikasi digital maka dokumen dapat diyakini tidak mengalami perubahan selama pengiriman.
3. Jaminan privasi. Dengan protokol yang digunakan selama transmisi menggunakan sertifikat digital maka jalur yang digunakan dalam transmisi dipastikan aman dan tidak dapat diakses oleh pihak lain yang tidak berhak.

4. Sertifikat digital dari IKP dapat menggantikan peranan proses otentikasi *user* dalam sebuah sistem.
5. Dengan menggunakan sertifikat digital dari IKP maka suatu pihak dapat menentukan transaksi yang aman dengan menggunakan validasi kunci publik.
6. Dukungan anti penyangkalan. Dengan adanya validasi pada sertifikat digital maka tidak mungkin untuk melakukan penyangkalan pada suatu transaksi yang telah dilakukan.

3. Analisis Sistem

Infrastuktur kunci publik pada intinya merupakan kolaborasi antar sistem. Sistem ini terdiri dari sistem manajemen sertifikat, sistem validasi sertifikat, sistem otentikasi klien serta klien itu sendiri. Untuk membangun infrastuktur kunci publik maka dilakukan dengan cara membangun kolaborasi beberapa sistem dengan acuan pada fungsionalitas masing-masing sistem penyusunnya.



Gambar 3.1. Kolaborasi Infrastruktur Kunci Publik

Sistem manajemen sertifikat merupakan sistem yang berfungsi mengatur sertifikat digital. Dalam sistem ini terjadi fungsi-fungsi yang dilakukan oleh *Certification Authority* yaitu proses permohonan sertifikat digital, persetujuan sertifikat digital, pengeluaran sertifikat digital, dan pencabutan sertifikat digital. Ada beberapa aplikasi yang bisa digunakan untuk manajemen sertifikat digital, diantaranya adalah Microsoft Windows Server, EJBCA, dan OpenCA.

Tabel 3.1. Perbandingan Antar Aplikasi Certification Authority

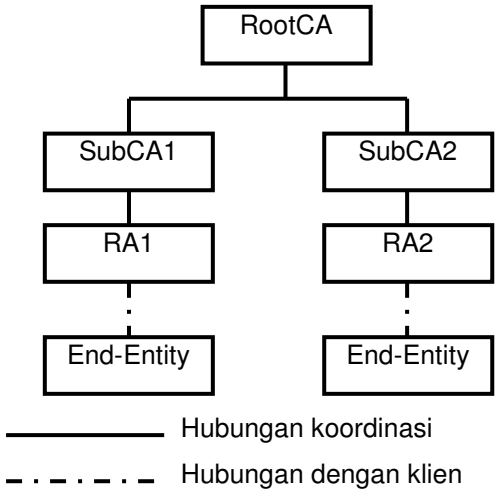
Parameter	Microsoft Windows Server	EJBCA	OpenCA
Platform	Microsoft Windows	Java J2EE	Linux
Lisensi	Komersial	Gratis	Gratis
Konfigurasi	Kompleks	Sangat Kompleks	Kompleks
Confidentiality	RSA 384 – 16.384 bit	RSA 1024bit, 2048bit, 4096bit	RSA 1024bit, 2048bit, 4096bit
Integrity	SHA1	MD5, SHA-1, SHA-256	SHA1
Authentication	DSA	DSA, ECDSA	DES, DES3 dan IDEA
Nir-Sangkal	Ya	Ya	Ya
Pemilihan Algoritma	Tidak	Ya	Ya
Pemilihan kunci	Ya	Ya	Ya
RA eksternal	Ya	Ya	Ya
Update CRL	Otomatis	Otomatis	Manual
Repository sertifikat	Active Directory directory service	HSQL, MYSQL, PostgreSQL, Oracle, DB2, MS-SQL	MySQL
Dukungan LDAP	Ya	Ya	Ya
Modul	Microsoft Windows API	Enterprise Java Bean	Perl
Skalabilitas	Baik	Baik	Buruk
Administrasi GUI berbasis *Command Line*	Ya	Ya	Tidak
Dukungan *Web Browser*	Banyak	Banyak	Banyak
Administrasi GUI berbasis *Web*	Tidak, berbasis *Console Administrator Tools*	Ya, *Strong Authentication* dengan SSL	Ya

Sistem validasi sertifikat merupakan sistem yang berfungsi memvalidasi permintaan otentikasi sertifikat digital. Pada dasarnya sistem ini bisa digabung dengan

sistem manajemen sertifikat, namun alasan performansi dan keamanan menjadikannya sebagai sistem yang harus terpisah. Sistem otentikasi klien merupakan sistem yang berfungsi menyediakan antarmuka kepada klien untuk proses otentikasi sertifikat digital. Sistem ini memiliki kepentingan atas keabsahan klien yang masuk ke dalam sistemnya. Klien merupakan pengguna sertifikat digital dan berfungsi sebagai *end-user* atau *end-entity* dalam skema Infrastruktur Kunci Publik.

4. Hasil Penelitian dan Pembahasan

Sebelum pembuatan sertifikat digital, penulis telah membuat hirarki dalam *Certification Authority* RootCA. Adapun skema hirarki dalam RootCA digambarkan dalam diagram sebagai berikut:

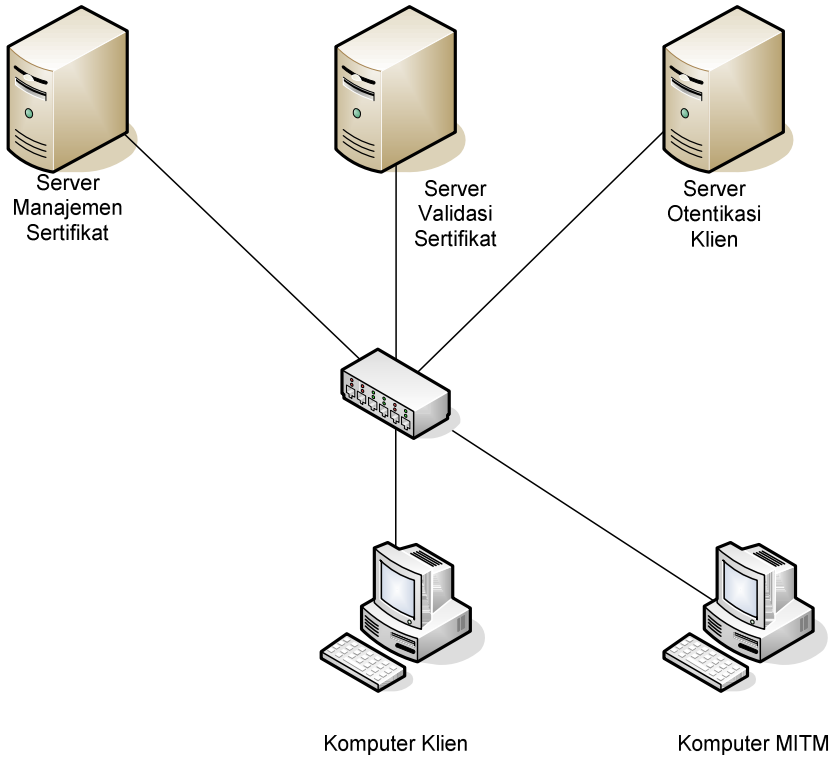


Gambar 4.1. Model Hirarki RootCA

Adapun Proses pembuatan sertifikat digital dilakukan dengan langkah-langkah sebagai berikut:

1. Proses permintaan pembuatan sertifikat digital *end-entity* melalui perantara RA2.
2. Proses persetujuan pembuatan sertifikat digital *end-entity* oleh SubCA2.
3. Proses pengambilan sertifikat digital oleh *end-entity* dari server manajemen sertifikat.

Dalam tahap pengujian ini penulis menambah satu simulasi komputer yang diberi nama Komputer MITM. Komputer MITM merupakan komputer yang masih dalam satu jaringan dengan komputer klien. Komputer MITM digambarkan sebagai *Man In The Middle* (MITM) dimana semua paket data yang mengalir melalui jaringan akan ditangkap menggunakan Wireshark. Adapun simulasi susunan komputer untuk pengujian digambarkan dalam skema sebagai berikut:



Gambar 4.2. Skema Susunan Komputer Untuk Pengujian

Penjelasan skema susunan komputer untuk pengujian:

1. Konfigurasikan komputer klien dan komputer MITM dalam satu jaringan.
2. Pada komputer MITM diinstal Wireshark.
3. Hubungan koordinasi antara server manajemen sertifikat, server validasi sertifikat dan server otentikasi klien berupa distribusi informasi database sertifikat digital.
4. Hubungan antara komputer klien dengan server manajemen sertifikat berupa permintaan pembuatan, persetujuan dan penerbitan sertifikat digital.
5. Hubungan antara komputer klien dengan server otentikasi klien berupa akses *login* klien melalui sistem otentikasi klien.
6. Komputer MITM menangkap paket yang mengalir dalam jaringan dengan *software* Wireshark.

Adapun pengujian otentikasi *login website* tanpa SSL dan dengan SSL dilakukan dengan langkah-langkah sebagai berikut:

1. Pada komputer MITM jalankan Wireshark.
2. Pada komputer klien buka *web browser*. Masuk ke manajemen sertifikat bagian sertifikat personal. Masukkan sertifikat digital klien “rizaldi.febrianto.p12” dengan *passphrase* “12345”, yang sebelumnya sudah dibuat dengan aplikasi *Certification Authority* RootCA.

3. Masukkan alamat URL http://svrok/sisok atau https://svrok/sisok. Pilih sertifikat digital atas nama Rizaldi Arief Febrianto. Lalu tekan OK.
4. *Login* sebagai peserta dengan *username* “rizaldi.febrianto” dan *password* “12345”. Tekan tombol masuk.
5. Masuk ke *form upload* sertifikat. Pilih file sertifikat digital klien “rizaldi.febrianto.p12” dengan *passphrase* “12345”. Tekan tombol kirim.
6. Otentikasi sertifikat digital klien berhasil.
7. Analisa data pada Wireshark di komputer MITM.

Tabel 4.1. Sampel Data Pengujian Waktu Proses Otorisasi Dengan Username dan Password Pada Protokol HTTP

No.	Waktu Proses (detik)	No.	Waktu Proses (detik)	No.	Waktu Proses (detik)	No.	Waktu Proses (detik)
1.	0.008883	6.	0.008267	11.	0.008469	16.	0.008749
2.	0.009086	7.	0.008945	12.	0.008994	17.	0.009463
3.	0.009125	8.	0.008916	13.	0.008749	18.	0.008978
4.	0.008849	9.	0.008504	14.	0.008375	19.	0.009684
5.	0.008803	10.	0.009773	15.	0.009276	20.	0.009350

Tabel 4.2. Sampel Data Pengujian Waktu Proses Otentikasi Dengan Sertifikat Digital Pada Protokol HTTPS

No.	Waktu Proses (detik)	No.	Waktu Proses (detik)	No.	Waktu Proses (detik)	No.	Waktu Proses (detik)
1.	0.019698	6.	0.020617	11.	0.022242	16.	0.019011
2.	0.018863	7.	0.019013	12.	0.018583	17.	0.018208
3.	0.018441	8.	0.020972	13.	0.018845	18.	0.019915
4.	0.021144	9.	0.018134	14.	0.026115	19.	0.018150
5.	0.019116	10.	0.018433	15.	0.022192	20.	0.023776

Dari hasil pengujian di atas diperoleh beberapa data sebagai berikut:

1. Pada hasil pengujian otentikasi *login* klien pada *website* tanpa SSL terlihat bahwa informasi *login* bisa dilihat dengan jelas. Ini menandakan bahwa informasi penting sama sekali tidak diamankan dan bisa ditangkap dengan mudah oleh pengguna lain dalam jaringan.
2. Pada hasil pengujian otentikasi *login* klien pada *website* dengan SSL terlihat bahwa terjadi tukar menukar informasi dengan *handshake* (ditandai dengan SYN, ACK dan

FIN). *Handshake* yang terjadi ini disebut sebagai SSL *handshake* dimana terjadi pertukaran informasi sertifikat digital antara klien dengan *server*. Otentikasi terjadi dua arah atau biasa disebut *mutual authentication*. Dalam pengujian ini informasi *login* sama sekali tidak bisa dilihat, dikarenakan penggunaan protokol HTTPS (HTTP dengan SSL) yang mengenkripsi informasi *login* klien saat melalui jaringan.

3. Pada hasil pengujian waktu proses otentikasi *login* klien di atas diperoleh rata-rata waktu proses untuk otorisasi *username* dan *password* pada protokol HTTP adalah 0,0089619 detik. Sedangkan rata-rata waktu proses untuk otentikasi sertifikat digital pada protokol HTTP adalah 0,0192452 detik. Rata-rata waktu proses untuk otorisasi *username* dan *password* pada protokol HTTPS adalah 0,0093492 detik. Sedangkan rata-rata waktu proses untuk otentikasi sertifikat digital pada protokol HTTPS adalah 0,0200734 detik. Dari data di atas bisa ditarik kesimpulan bahwa otentikasi sertifikat digital menghabiskan waktu lebih lama dibanding otorisasi dengan *username* dan *password*. Hal ini disebabkan karena pemrosesan sertifikat digital membutuhkan waktu untuk proses *upload* sertifikat dan dekripsi informasi. Untuk waktu proses otentikasi sertifikat digital secara *online* cukup dengan menambahkan waktu proses *throughput* dari komputer klien ke server dan sebaliknya dengan sampel data dalam tabel di atas.

Sertifikat digital yang digunakan dalam penelitian ini merupakan file PKCS#12 atau file dengan ekstensi p12. PKCS#12 merupakan varian dari *Public Key Cryptography Standards* yang dikeluarkan oleh *RSA Laboratories*. File ini menjadi tempat penyimpan sertifikat digital yang terdiri dari sertifikat digital milik pengguna (publik dan privat), sertifikat digital milik *SubCA* (publik), dan sertifikat digital milik *RootCA* (publik). File ini dilengkapi dengan fitur *passphrase* untuk membukanya.

Aplikasi *website* membaca blok pertama isi file sertifikat digital milik klien dan mendekripsikan informasi dari pemilik sertifikat digital tersebut. Berikut adalah merupakan tampilan array dari sertifikat digital dalam bentuk yang sudah bisa dibaca informasinya:

```
Array ( [name] => /emailAddress=rizaldi.febrianto@deplu.go.id/CN=Rizaldi Arief Febrianto/OU=Sekretariat Jenderal/O=Deplu/C=ID [subject] => Array ( [emailAddress] => rizaldi.febrianto@deplu.go.id [CN] => Rizaldi Arief Febrianto [OU] => Sekretariat Jenderal [O] => Deplu [C] => ID ) [hash] => 9eddb381 [issuer] => Array ( [CN] => SubCA2 [O] => EJBCA [C] => ID ) [version] => 2 [serialNumber] => 5803650149771941539 [validFrom] => 100411042544Z [validTo] => 120410042544Z [validFrom_time_t] => 1270956344 [validTo_time_t] => 1334028344 [purposes] => Array ( [1] => Array ( [0] => 1 [1] => [2] => sslclient ) [2] => Array ( [0] => [1] => [2] => sslserver ) [3] => Array ( [0] => [1] => [2] => nssslserver ) [4] => Array ( [0] => 1 [1] => [2] => smimesign ) [5] => Array ( [0] => 1 [1] =>
```

```
[2] => smimeencrypt ) [6] => Array ( [0] => [1] => [2] => crlsign ) [7]
=> Array ( [0] => 1 [1] => 1 [2] => any ) [8] => Array ( [0] => 1 [1] =>
[2] => ocsphelper ) ) [extensions] => Array ( [basicConstraints] =>
CA:FALSE [extendedKeyUsage] => TLS Web Client Authentication, E-mail
Protection [authorityKeyIdentifier] =>
keyid:4C:C7:B3:56:4A:EB:D5:2C:B4:00:4E:EA:45:47:FD:A4:18:51:74:FB
[keyUsage] => Digital Signature, Non Repudiation, Key Encipherment
[subjectKeyIdentifier] =>
72:44:B5:D4:38:3D:7A:D4:08:19:16:17:B1:73:CC:3F:6B:E8:8B:1B ) )
```

Setelah tahap ini, aplikasi *website* mengambil variabel-variabel yang diperlukan untuk otentikasi *login website*, diantaranya adalah:

```
[serialNumber] => 5850818536752508062
[subject][emailAddress] => rizaldi.febrianto@deplu.go.id
[subject][CN] => Rizaldi Arief Febrianto
[subject][OU] => Sekretariat Jenderal
[subject][O] => Deplu
[subject][C] => ID
[validFrom_time_t] => 1262794708
[validTo_time_t] => 1294328313
[issuer][CN] => SubCA2
[issuer][O] => EJBCA
[issuer][C] => ID
```

Variabel-variabel di atas lalu dicocokkan dengan informasi klien yang tersimpan dalam database pada server validasi sertifikat. Baris data yang dicocokkan adalah dari database *ejbca* pada tabel *certificatedata* sebagai berikut:

Tabel 4.3. Cuplikan Tabel Certificatedata

serialNumber	username	subjectDN	issuerDN	status	expireDate	updateTime
…	…	…	…	…	…	…
5850818536752508062	Rizaldi.febrianto	E=rizaldi.febrianto@deplu.go.id,CN=Rizaldi Arief Febrianto,OU=Sekretariat Jenderal,O=Deplu,C=ID	CN=SubCA2,O=EJBCA,C=ID	20	1294328313	1262794708
…	…	…	…	…	…	…

Aplikasi juga mengecek status sertifikat digital. Ada beberapa status sertifikat digital yang umum dikenal, antara lain:

Tabel 4.4. Status Sertifikat Digital

No.	Status	Keterangan
1.	0	Sertifikat tanpa pemilik
2.	10	Sertifikat belum aktif
3.	20	Sertifikat aktif
4.	21	Sertifikat hampir kadaluarsa
5.	30	Sertifikat dicabut sementara
6.	40	Sertifikat dicabut
7.	50	Sertifikat kadaluarsa
8.	60	Sertifikat kadaluarsa, masuk arsip

Selanjutnya aplikasi akan memverifikasi kesesuaian sertifikat digital dengan kunci publik yang disimpan dalam database pada server validasi sertifikat. Adapun tahapannya adalah sebagai berikut:

1. Membuka dan membaca isi sertifikat digital.

```
$p12cert=array();
$p12file=”rizaldi.febrianto.p12”;
$pass=”12345”;
$fp=fopen($p12file,”r”);
$p12buf=fread($fp,filesize($p12file));
fclose($fp);
if(openssl_pkcs12_read($p12buf,$p12cert,$pass))
{
   $pkey_data=print_r($p12cert[“pkey”],true);
   $cert_data=print_r($p12cert[“cert”],true);
};
```

2. Mengambil isi database *ejbca* tabel *certificatedata* pada kolom base64Cert (pada server validasi sertifikat).

```
$dbh= mysql_connect(“svrvs”,”root”,”rahasia”);
mysql_select_db(“ejbca”);
$query=”SELECT base64Cert FROM certificatedata WHERE
username=’rizaldi.febrianto’”;
$res=mysql_query($sql,$dbh);
$row=mysql_fetch_array($res);
$dbbase64Cert_data=$row[“base64Cert”];
```

3. Verifikasi kesesuaian sertifikat digital.

```
$priv_key=openssl_pkey_get_private(array($pkey_data,””));
```

```
$cert_res=openssl_x509_read($dbbase64Cert_data);
$verification=openssl_x509_check_private_key($cert_res,$priv_key);
```

4. Jika $verification menghasilkan nilai *boolean* true, maka berarti sertifikat digital memiliki kunci privat yang merupakan pasangan dari kunci publik yang tersimpan dalam database pada server validasi sertifikat.

Jika semua informasi sertifikat digital sesuai dengan informasi dalam database pada server validasi sertifikat maka klien tersebut memang benar yang telah *login* ke dalam sistem. Dengan kata lain, otentikasi klien menggunakan sertifikat digital berhasil. Informasi sertifikat digital milik klien tersebut lalu akan disimpan dalam *website session* untuk selanjutnya digunakan pada sesi transaksi elektronik.

5. Kesimpulan

Berdasar hasil penelitian dan aplikasi yang telah dibangun oleh penulis, bisa diambil beberapa kesimpulan sebagai berikut:

1. Sistem otentikasi klien pada website dengan menggunakan sertifikat digital dibangun dengan kolaborasi antara beberapa sistem, antara lain sistem manajemen sertifikat, sistem validasi sertifikat, dan sistem otentikasi klien berupa aplikasi *website* yang mampu memproses informasi sertifikat digital, serta klien itu sendiri.
2. Transaksi elektronik diawali dengan otorisasi *username* dan *password* lalu dilanjutkan dengan otentikasi klien melalui sertifikat digital.
3. Sistem yang dibangun mampu menjamin keabsahan klien yang memiliki sertifikat digital, mendukung audit yang bisa dipertanggungjawabkan dan bisa menjadi alat bukti hukum yang sah.
4. Sistem otentikasi klien pada *website* yang relatif aman dibangun menggunakan *Secure Socket Layer* (SSL) dengan *mutual authentication*. Dengan protokol *HyperText Transfer Protocol Secure* (HTTPS), informasi klien akan dienkripsi terlebih dahulu sebelum melewati jaringan, sehingga sulit dibaca oleh pengguna lain yang berada dalam jaringan.
5. Waktu proses yang dibutuhkan untuk otentikasi klien menggunakan sertifikat digital relatif lebih lama dibandingkan dengan otorisasi *username* dan *password*. Hal ini dikarenakan sistem otentikasi membutuhkan waktu lebih lama untuk mendekripsikan informasi sertifikat digital.
6. Regulasi dengan kekuatan hukum mengatur dan menjamin kepastian hukum atas transaksi elektronik dalam dunia internet dengan penggunaan sertifikat digital melalui penerapan audit pada sistem otentikasi klien.

DAFTAR PUSTAKA

Ariyus, Dony. 2006. Computer Security. Andi Offset: Yogyakarta.

Berkovits, Shimshon, Chokhani, Santosh, Furlong, Judith A., Geiter, Jisoo A., and Guild, Jonathan C. 1994. *Public Key Infrastructure Study, Final Report*. Mitre: Virginia.

Ghori, Ayesha Ishrath and Parveen, Asra. 2006. *PKI Administration Using EJBCA And OpenCA*. George Mason University-Fall: Virginia.

Jogiyanto, HM. 2005. Analisis dan Desain Sistem Informasi. Andi Offset: Yogyakarta.

Kadir, Abdul. 2003. Pengenalan Sistem Informasi. Andi Offset: Yogyakarta.

Kurniawan, Yahya. 2002. Aplikasi Web Database Dengan PHP Dan MySQL. Elex Media Komputindo: Jakarta.

Marlinda, Linda. 2004. Sistem Basis Data. Andi Offset: Yogyakarta.

Sidik, Betha. 2005. MySQL Untuk Pengguna, Administrator, dan Pengembang Aplikasi Web. Informatika: Bandung.

Suarna, Nana. 2007. Petunjuk Teoritis Pengantar LAN. Yrama Widya: Bandung.

Stewart, James M., Tittel, Ed, and Chapple, Mike. 2005. *Certified Information Systems Security Professional Study Guide 3rd Edition*. Sybex Inc.: London.

Whitten, Jeffery L., Bentley, Lonnie D., dan Dittman, Kevin C. 2004. Metode Desain dan Analisis Sistem. Andi Offset: Yogyakarta.

http://yudiagusta.files.wordpress.com/2009/11/262-265-knsi09-048-perbandingan-aplikasi-public-key-infrastructure-pada-windows-server-2003-dan-ejbca.pdf, diakses pada tanggal 5 Januari 2010

http://ant.apache.org

http://java.sun.com

http://www.apachefriends.org

http://www.ejbca.org

http://www.jboss.org

http://www.mysql.com

http://www.php.net

http://www.virtualbox.org