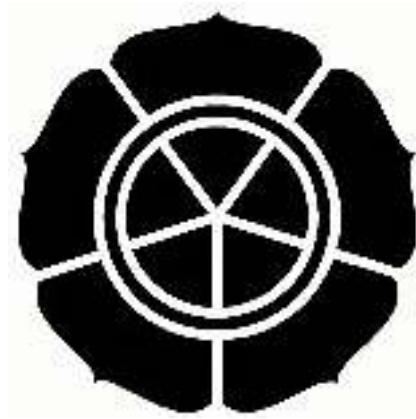


**ANALISIS DAN PERANCANGAN SISTEM OTENTIKASI KLIEN  
PADA WEBSITE MENGGUNAKAN SERTIFIKAT DIGITAL  
DENGAN SKEMA INFRASTRUKTUR KUNCI PUBLIK**

**SKRIPSI**

untuk memenuhi sebagian persyaratan  
mencapai derajat Sarjana S1  
pada jurusan Teknik Informatika



**Disusun oleh**

**Rizaldi Arief Febrianto**

**07.21.0312**

**JURUSAN TEKNIK INFORMATIKA  
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER  
AMIKOM  
YOGYAKARTA  
2010**

**PERSETUJUAN**

**SKRIPSI**


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

dipersiapkan dan disusun oleh

**Rizaldi Arief Febrianto**  
**07.21.0312**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 9 Januari 2010

**Dosen Pembimbing,**



**Ema Utami, S.Si, M.Kom**  
**NIK. 190302037**

**PENGESAHAN**

**SKRIPSI**

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

dipersiapkan dan disusun oleh

**Rizaldi Arief Febrianto**  
07.21.0312

telah dipertahankan di depan Dewan Penguji  
pada tanggal 10 Februari 2010

**Susunan Dewan Penguji**


**Nama Penguji**

**Tanda Tangan**

**Ir. Abas Ali Pangera, M.Kom**  
NIK. 190302008

**Sudarmawan, MT**  
NIK. 190302035

**Armadyah Amborowati, S.Kom, M.Eng**  
NIK. 190302063



Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 30 April 2010



**KETUA STMIK AMIKOM YOGYAKARTA**

**Prof. Dr. M. Suyanto, MM**  
NIK. 190302001

## HALAMAN PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (asli), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu Institusi Pendidikan, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 10 Februari 2010



Rizaldi Arief Febrianto

NIM. 07.21.0312

## HALAMAN MOTTO

*“Demi masa. Sesungguhnya manusia itu benar-benar dalam kerugian. Kecuali orang-orang yang beriman dan yang mengerjakan amal saleh dan saling menasehati supaya mentaati kebenaran dan saling menasehati supaya menepati kesabaran”*

(QS. Al-Ashr)

*“Gunakan yang lima sebelum datang yang lima: masa mudamu sebelum datang masa tuamu, masa sehatmu sebelum datang masa sakitmu, masa kayamu sebelum datang masa miskinmu, masa kosongmu sebelum datang masa sibukmu, masa hidupmu sebelum datang kematianmu”*

(HR. Al-Hakim)

## HALAMAN PERSEMBAHAN

*Skripsi ini kupersembahkan ....*

- ✿ Kehadirat Allah SWT, Sang Pencipta Alam Semesta yang mengatur jalan kehidupan makhluk ciptaan-Nya*
- ✿ Kepada Bapak dan Ibu atas dukungan moral dan material*
- ✿ Kepada keluarga atas motivasinya*
- ✿ Kepada teman-teman atas bantuannya*
- ✿ Kepada rekan kerja atas kerjasamanya*
- ✿ Kepada semua pihak yang telah membantu*
- ✿ Terima kasih semua ....!!!*



## KATA PENGANTAR

Alhamdulillah. Penulis memanjatkan puji syukur kehadirat Allah SWT, Sang Pencipta Alam Semesta yang telah memberikan rahmat dan hidayah pada semua makhluk ciptaan-Nya, sehingga penulis dapat menyelesaikan penyusunan skripsi yang berjudul “ANALISIS DAN PERANCANGAN SISTEM OTENTIKASI KLIEN PADA WEBSITE MENGGUNAKAN SERTIFIKAT DIGITAL DENGAN SKEMA INFRASTRUKTUR KUNCI PUBLIK”. Skripsi ini disusun untuk memenuhi sebagian persyaratan mencapai derajat Sarjana S1 pada jurusan Teknik Informatika STMIK AMIKOM Yogyakarta.

Penulis mengucapkan terima kasih kepada semua pihak yang telah membantu dalam penyusunan tugas akhir ini.

1. Bapak Prof. Dr. M. Suyanto, MM, selaku Ketua STMIK AMIKOM Yogyakarta.
2. Bapak Ir. Abas Ali Pangera, M.Kom, selaku Ketua Jurusan Teknik Informatika STMIK AMIKOM Yogyakarta.
3. Ibu Ema Utami, S.Si, M.Kom, selaku Dosen Pembimbing.
4. Segenap keluarga yang telah mendukung secara moral dan material.
5. Teman-teman dan rekan kerja yang telah membantu penyusunan skripsi ini.

Semoga Allah SWT senantiasa memberi kebaikan pada kita semua.

Penulis berharap kritik dan saran yang membangun dalam rangka perbaikan kualitas, baik untuk diri pribadi maupun untuk aplikasi yang dibangun.

Yogyakarta, Februari 2010

Penulis

## DAFTAR ISI

|  |      |
|--|------|
| HALAMAN JUDUL.....                                 | i    |
| HALAMAN PERSETUJUAN.....                           | ii   |
| HALAMAN PENGESAHAN.....                            | iii  |
| HALAMAN PERNYATAAN.....                            | iv   |
| HALAMAN MOTTO.....                                 | v    |
| HALAMAN PERSEMBAHAN.....                           | vi   |
| KATA PENGANTAR.....                                | vii  |
| DAFTAR ISI.....                                    | viii |
| DAFTAR TABEL.....                                  | xii  |
| DAFTAR GAMBAR.....                                 | xiii |
| INTISARI.....                                      | xv   |
| <i>ABSTRACT</i> .....                              | xvi  |
| <b>BAB I. PENDAHULUAN</b>                          |      |
| 1.1. Latar Belakang Masalah.....                   | 1    |
| 1.2. Rumusan Masalah.....                          | 3    |
| 1.3. Batasan Masalah.....                          | 3    |
| 1.4. Tujuan Penelitian.....                        | 4    |
| 1.5. Manfaat Penelitian.....                       | 4    |
| 1.6. Sistematika Penulisan.....                    | 5    |
| 1.7. Rencana Penelitian.....                       | 6    |
| <b>BAB II. TINJAUAN PUSTAKA DAN LANDASAN TEORI</b> |      |
| 2.1. Tinjauan Pustaka.....                         | 8    |
| 2.1.1. Sistem.....                                 | 8    |
| 2.1.1.1. Konsep Dasar Sistem.....                  | 8    |
| 2.1.1.2. Analisis Sistem.....                      | 9    |
| 2.1.1.3. Perancangan Sistem.....                   | 10   |
| 2.1.2. Informasi.....                              | 11   |



|   |    |
|---|----|
| 2.1.2.1. Konsep Dasar Informasi .....             | 11 |
| 2.1.2.2. Sistem Informasi .....                   | 12 |
| 2.1.3. Jaringan Komputer .....                    | 13 |
| 2.1.3.1. Konsep Dasar Jaringan Komputer .....     | 13 |
| 2.1.3.2. Internet .....                           | 15 |
| 2.1.4. Database .....                             | 17 |
| 2.1.4.1. Konsep Dasar Database .....              | 17 |
| 2.1.4.2. <i>Entity Relationship Diagram</i> ..... | 18 |
| 2.1.4.3. Derajat Kardinalitas .....               | 18 |
| 2.1.4.4. Atribut Kunci .....                      | 19 |
| 2.2. Landasan Teori .....                         | 20 |
| 2.2.1. Keamanan Informasi .....                   | 20 |
| 2.2.2. SSL Dan TLS .....                          | 22 |
| 2.2.3. Kriptografi .....                          | 23 |
| 2.2.4. RSA .....                                  | 25 |
| 2.2.5. Sertifikat Digital .....                   | 27 |
| 2.2.6. Infrastruktur Kunci Publik (IKP) .....     | 31 |
| 2.2.6.1. Konsep Dasar IKP .....                   | 31 |
| 2.2.6.2. Komponen IKP .....                       | 32 |
| 2.2.6.3. Subyek IKP .....                         | 33 |
| 2.2.6.4. Skema IKP .....                          | 34 |
| 2.2.6.5. Fungsi IKP .....                         | 35 |
| 2.2.6.6. Model IKP .....                          | 36 |
| 2.2.7. Tinjauan Undang-Undang ITE .....           | 39 |

### **BAB III. ANALISIS DAN PERANCANGAN SISTEM**

|  |    |
|--|----|
| 3.1. Analisis Sistem .....                       | 42 |
| 3.2. Alat Penelitian .....                       | 45 |
| 3.2.1. Perangkat Lunak .....                     | 45 |
| 3.2.1.1. <i>Java Development Kit (JDK)</i> ..... | 45 |
| 3.2.1.2. JBoss AS .....                          | 47 |

|  |     |
|--|-----|
| 3.2.1.3. MySQL .....   | 47  |
| 3.2.1.4. EJBCA .....   | 50  |
| 3.2.1.5. Xampp.....  | 51  |
| 3.2.1.6. <i>Web Browser</i> .....                            | 55  |
| 3.2.1.7. VirtualBox.....                                     | 56  |
| 3.2.2. Perangkat Keras.....                                  | 57  |
| 3.3. Cara Penelitian.....                                    | 58  |
| 3.4. Metode Penelitian .....                                 | 59  |
| 3.5. Implementasi.....                                       | 60  |
| 3.5.1. Konfigurasi Server Manajemen Sertifikat.....          | 60  |
| 3.5.2. Konfigurasi Server Validasi Sertifikat .....          | 66  |
| 3.5.3. Konfigurasi Server Otentikasi Klien .....             | 67  |
| 3.5.4. Konfigurasi Komputer Klien.....                       | 69  |
| 3.6. Perancangan <i>Website</i> Sistem Otentikasi Klien..... | 69  |
| 3.6.1. Deskripsi.....  | 70  |
| 3.6.2. <i>Use Case Diagram</i> .....                         | 71  |
| 3.6.3. <i>Activity Diagram</i> .....                         | 74  |
| 3.6.4. Perancangan Database.....                             | 76  |
| 3.6.4.1. <i>Entity Relationship Diagram</i> .....            | 76  |
| 3.6.4.2. Daftar Tabel .....                                  | 77  |
| 3.6.5. Perancangan Antarmuka .....                           | 80  |
| <b>BAB IV. HASIL PENELITIAN DAN PEMBAHASAN</b>               |     |
| 4.1. Pengujian .....   | 84  |
| 4.2. Hasil Pengujian.....                                    | 86  |
| 4.2.1. Pembuatan Sertifikat Digital .....                    | 86  |
| 4.2.2. Otentikasi <i>Login Website</i> Tanpa SSL.....        | 91  |
| 4.2.3. Otentikasi <i>Login Website</i> Dengan SSL .....      | 94  |
| 4.2.4. Waktu Proses.....                                     | 98  |
| 4.3. Pembahasan .....  | 100 |
| 4.3.1. Pembahasan Hasil Pengujian .....                      | 100 |

|   |     |
|---|-----|
| 4.3.2. Pembahasan Otentikasi Klien..... | 101 |
|---|-----|

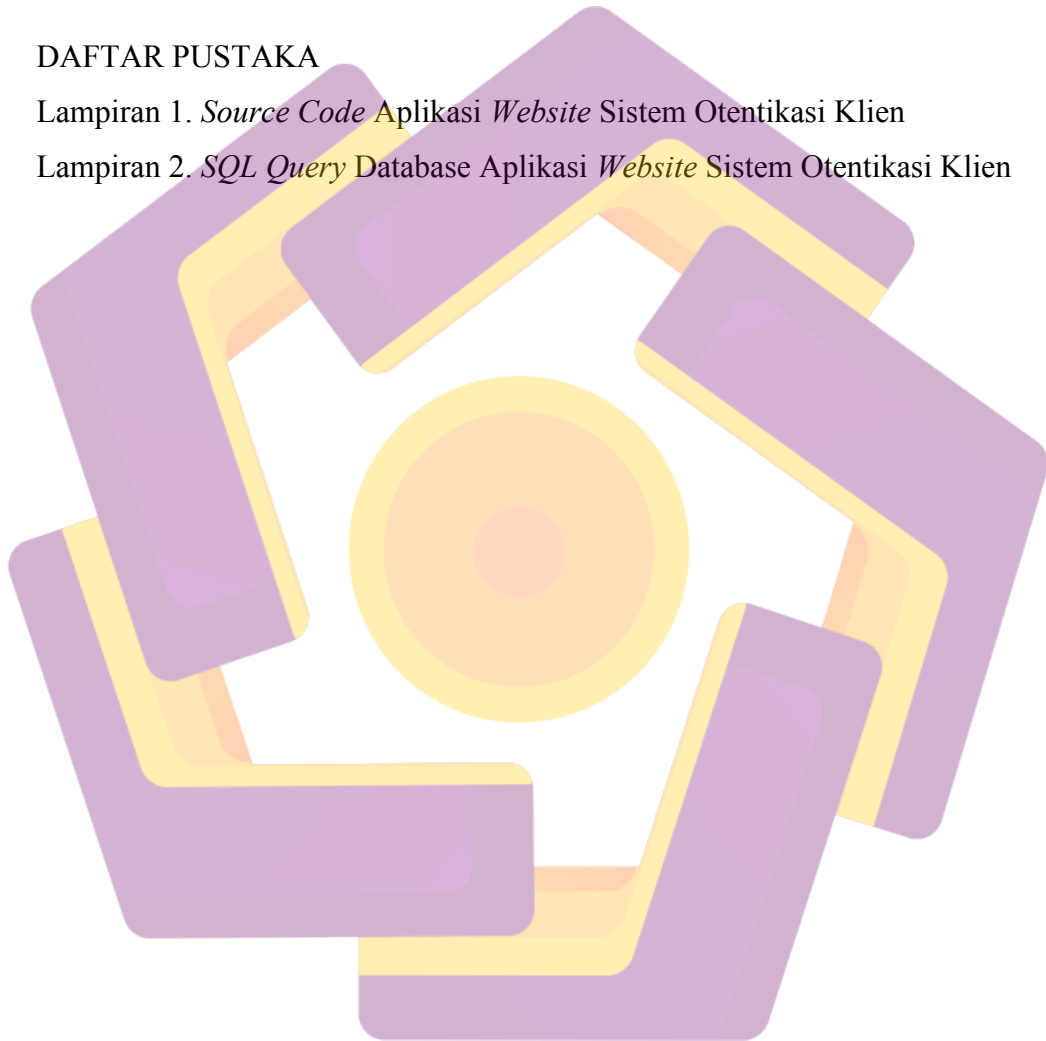
**BAB V. KESIMPULAN DAN SARAN**

|                      |     |
|----------------------|-----|
| 5.1. Kesimpulan..... | 109 |
| 5.2. Saran.....      | 110 |

**DAFTAR PUSTAKA**

Lampiran 1. *Source Code* Aplikasi *Website* Sistem Otentikasi Klien

Lampiran 2. *SQL Query* Database Aplikasi *Website* Sistem Otentikasi Klien



## DAFTAR TABEL

|   |     |
|---|-----|
| Tabel 1.1. Rencana Penelitian.....  | 7   |
| Tabel 2.1. Isu Keamanan Informasi, Permasalahan dan Solusi.....   | 21  |
| Tabel 2.2. Contoh Soal Kriptografi RSA.....   | 26  |
| Tabel 3.1. Perbandingan Antar Aplikasi <i>Certification Authority</i> .....                                   | 43  |
| Tabel 3.2. Tipe Data MySQL.....   | 48  |
| Tabel 3.3. Tabel Superadmin .....   | 77  |
| Tabel 3.4. Tabel Admin .....  | 77  |
| Tabel 3.5. Tabel Klien.....   | 78  |
| Tabel 3.6. Tabel Organisasi .....   | 78  |
| Tabel 3.7. Tabel Unit .....   | 79  |
| Tabel 3.8. Tabel Info.....  | 79  |
| Tabel 3.9. Tabel FAQ.....   | 79  |
| Tabel 4.1. Sampel Data Pengujian Waktu Proses Otorisasi Dengan Username dan Password Pada Protokol HTTP ..... | 98  |
| Tabel 4.2. Sampel Data Pengujian Waktu Proses Otentikasi Dengan Sertifikat Digital Pada Protokol HTTP.....    | 98  |
| Tabel 4.3. Sampel Data Pengujian Waktu Proses Otorisasi Dengan Username dan Password Pada Protokol HTTPS..... | 99  |
| Tabel 4.4. Sampel Data Pengujian Waktu Proses Otentikasi Dengan Sertifikat Digital Pada Protokol HTTPS .....  | 99  |
| Tabel 4.5. Cuplikan Tabel <i>Certificatedata</i> .....  | 106 |
| Tabel 4.6. Status Sertifikat Digital.....   | 106 |

## DAFTAR GAMBAR

|   |    |
|---|----|
| Gambar 2.1. <i>One To One Relationship</i> .....                            | 19 |
| Gambar 2.2. <i>One To Many Relationship</i> .....                           | 19 |
| Gambar 2.3. <i>Many To Many Relationship</i> .....                          | 19 |
| Gambar 2.4. Proses Kriptografi .....  | 24 |
| Gambar 2.5. Struktur Sertifikat Digital.....                                | 30 |
| Gambar 2.6. Skema Infrastruktur Kunci Publik .....                          | 35 |
| Gambar 2.7. <i>Hierarchical Model</i> .....                                 | 37 |
| Gambar 2.8. <i>Cross Certification Model</i> .....                          | 38 |
| Gambar 2.9. <i>Hybrid Model</i> .....                                       | 39 |
| Gambar 3.1. Kolaborasi Infrastruktur Kunci Publik.....                      | 42 |
| Gambar 3.2. Tampilan Antarmuka JBoss AS 5.1.0 GA .....                      | 47 |
| Gambar 3.3. Tampilan Antarmuka MySQL 5.1.40 .....                           | 48 |
| Gambar 3.4. Tampilan Antarmuka EJBCA 3.9.2 .....                            | 50 |
| Gambar 3.5. Tampilan Antarmuka Xampp 1.7.2.....                             | 52 |
| Gambar 3.6. Tampilan Antarmuka Mozilla Firefox 3.5.2 .....                  | 56 |
| Gambar 3.7. Tampilan Antarmuka VirtualBox 3.0.10 .....                      | 57 |
| Gambar 3.8. Gambaran Simulasi Penelitian .....                              | 59 |
| Gambar 3.9. <i>Use Case Diagram</i> Superadmin.....                         | 72 |
| Gambar 3.10. <i>Use Case Diagram</i> Admin .....                            | 73 |
| Gambar 3.11. <i>Use Case Diagram</i> Klien .....                            | 73 |
| Gambar 3.12. <i>Activity Diagram</i> Superadmin.....                        | 74 |
| Gambar 3.13. <i>Activity Diagram</i> Admin .....                            | 75 |
| Gambar 3.14. <i>Activity Diagram</i> Klien .....                            | 76 |
| Gambar 3.15. ERD Website Sistem Otentikasi Klien.....                       | 77 |
| Gambar 3.16. <i>Form Login</i> .....  | 80 |
| Gambar 3.17. <i>Form Upload Sertifikat</i> .....                            | 81 |
| Gambar 3.18. <i>Form Lupa Password</i> .....                                | 81 |
| Gambar 3.19. <i>Form Cek Sertifikat</i> .....                               | 82 |
| Gambar 3.20. <i>Form Info</i> .....   | 82 |
| Gambar 3.21. <i>Form FAQ</i> .....  | 83 |
| Gambar 4.1. Tampilan Antarmuka Wireshark 1.2.5.....                         | 84 |
| Gambar 4.2. Skema Susunan Komputer Untuk Pengujian .....                    | 85 |
| Gambar 4.3. Model Hirarki RootCA.....                                       | 87 |
| Gambar 4.4. Pembuatan Sertifikat Digital (1) .....                          | 88 |
| Gambar 4.5. Pembuatan Sertifikat Digital (2) .....                          | 89 |
| Gambar 4.6. Pembuatan Sertifikat Digital (3) .....                          | 89 |
| Gambar 4.7. Pembuatan Sertifikat Digital (4) .....                          | 90 |
| Gambar 4.8. Pembuatan Sertifikat Digital (5) .....                          | 90 |
| Gambar 4.9. Pembuatan Sertifikat Digital (6) .....                          | 91 |
| Gambar 4.10. Pengujian Otentikasi <i>Login Website</i> Tanpa SSL (1).....   | 92 |
| Gambar 4.11. Pengujian Otentikasi <i>Login Website</i> Tanpa SSL (2).....   | 92 |
| Gambar 4.12. Pengujian Otentikasi <i>Login Website</i> Tanpa SSL (3).....   | 93 |
| Gambar 4.13. Pengujian Otentikasi <i>Login Website</i> Tanpa SSL (4).....   | 93 |
| Gambar 4.14. Pengujian Otentikasi <i>Login Website</i> Dengan SSL (1) ..... | 95 |

|   |    |
|---|----|
| Gambar 4.15. Pengujian Otentikasi <i>Login Website</i> Dengan SSL (2) ..... | 95 |
| Gambar 4.16. Pengujian Otentikasi <i>Login Website</i> Dengan SSL (3) ..... | 96 |
| Gambar 4.17. Pengujian Otentikasi <i>Login Website</i> Dengan SSL (4) ..... | 96 |
| Gambar 4.18. Pengujian Otentikasi <i>Login Website</i> Dengan SSL (5) ..... | 97 |
| Gambar 4.19. Pengujian Otentikasi <i>Login Website</i> Dengan SSL (6) ..... | 97 |



## INTISARI

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 keamanan 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.

**Kata Kunci** : Sertifikat Digital, Infrastruktur Kunci Publik, Otentikasi, SSL



## **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*