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

Yogyakarta, Februari 2010

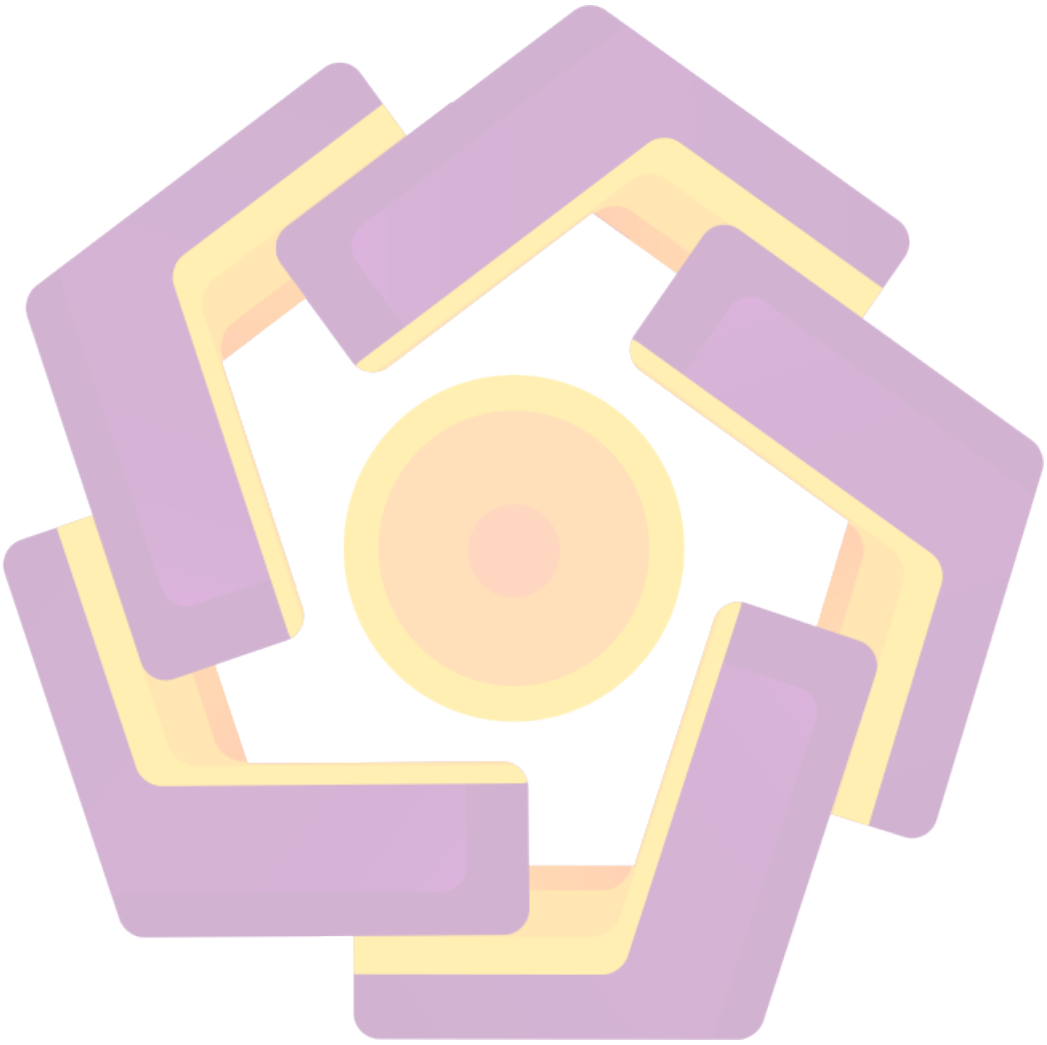
Penulis

DAFTAR ISI

BAB III. ANALISIS DAN PERANCANGAN SISTEM

DAFTAR TABEL

DAFTAR GAMBAR



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 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.

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*