

DESAIN OTENTIKASI DUA ARAH (*MUTUAL AUTHENTICATION*) PADA INTERNET BANKING DENGAN MENGGUNAKAN SERTIFIKAT DIGITAL

TESIS



Oleh:

Ayu Pustikasari
0911600203

**PROGRAM STUDI : MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR**

**JAKARTA
2013**

DESAIN OTENTIKASI DUA ARAH (*MUTUAL AUTHENTICATION*) PADA INTERNET BANKING DENGAN MENGGUNAKAN SERTIFIKAT DIGITAL

TESIS

**Diajukan untuk memenuhi salah satu persyaratan
memperoleh gelar Magister Ilmu Komputer**



Oleh

Ayu Pustikasari
0911600203

**PROGRAM STUDI : MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR**

**JAKARTA
2013**



LEMBAR PERNYATAAN

Saya yang bertanda tangan dibawah ini :

Nama : Ayu Pustikasari
NIM : 0911600203
Program : Magister Ilmu Komputer
Studi
Program : Rekayasa E-Bisnis

menyatakan bahwa TESIS yang berjudul:

Desain Otentikasi Dua Arah (Mutual Authentication)
pada Internet Banking dengan Menggunakan
Sertifikat Digital.

1. merupakan hasil karya tulis ilmiah sendiri dan bukan merupakan karya yang pernah diajukan untuk memperoleh gelar akademik oleh pihak lain,
2. saya ijin untuk dikelola oleh Universitas Budi Luhur sesuai dengan norma hukum dan etika yang berlaku.

Pernyataan ini saya buat dengan penuh tanggung jawab dan saya bersedia menerima konsekuensi apapun sesuai aturan yang berlaku apabila di kemudian hari pernyataan ini tidak benar.

Jakarta, 1 Maret 2013





LEMBAR PENGESAHAN

Nama : Ayu Pustikasari
Nomor Induk Mahasiswa : 0911600203
Konsentrasi : E-Business
Jenjang Studi : Strata 2
Judul : Desain Otentikasi Dua Arah (Mutual Authentication) pada Internet Banking dengan Menggunakan Sertifikat Digital

Jakarta, 23 Februari 2013

Tim Penguji:

Ketua,
Dr. Ir. Nazori A.Z., M.T.

Moderator,
Dr. Moedjiono, M.Sc

Pembimbing,
Dr. Ir. Nazori A.Z., M.T.

Pembimbing Pendamping
Mardi Hardjianto, M.Kom

Tandatangan:

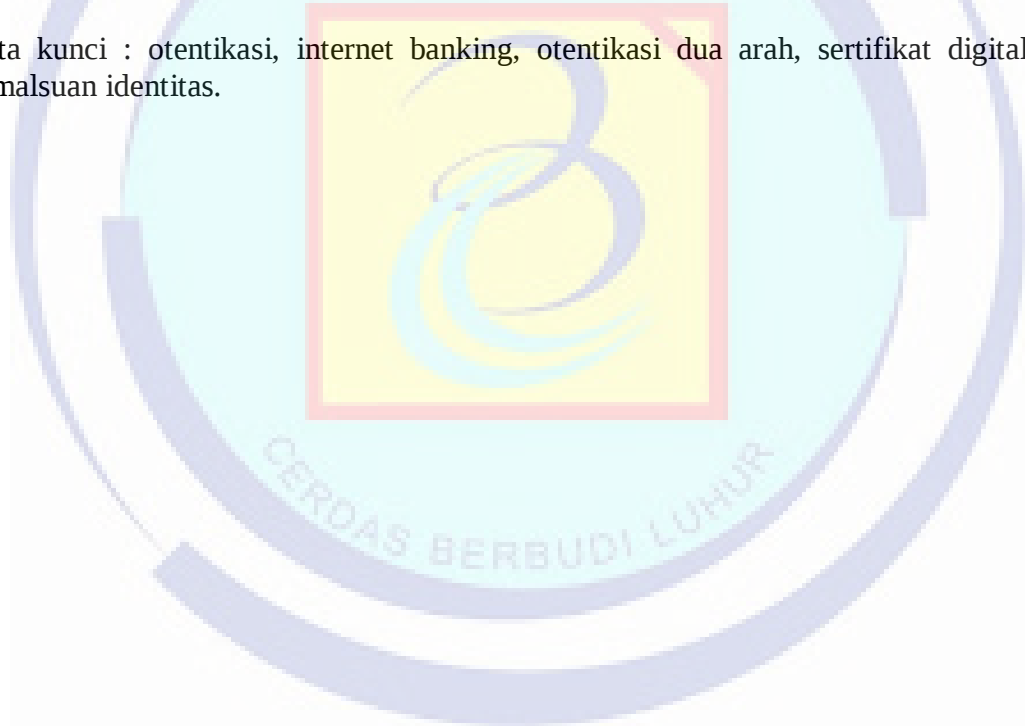
Ketua Program Studi

Dr. Ir. Nazori A.Z., M.T.

ABSTRAK

Metode otentikasi yang digunakan pada internet banking saat ini belum menggunakan otentikasi dua arah dengan menggunakan sertifikat digital. Hal ini mengakibatkan munculnya peluang pemalsuan identitas pada layanan perbankan elektronik. Penelitian ini membahas mengenai penerapan otentikasi dua arah pada internet banking dengan menggunakan sertifikat digital. Dalam proses otentikasi, *server* mengirimkan sertifikat digital ke nasabah dan nasabah juga mengirimkan sertifikat digital miliknya ke *server*. Jika kedua sertifikat digital tersebut valid maka nasabah dapat melanjutkan untuk mengakses halaman *login* website internet banking. Selanjutnya dilakukan pengujian dengan skenario pemalsuan sertifikat digital. Hasilnya akan dianalisis dan dibandingkan dengan metode otentikasi yang digunakan internet banking saat ini. Dengan penerapan otentikasi dua arah diharapkan dapat mengurangi peluang terjadinya pemalsuan identitas nasabah.

Kata kunci : otentikasi, internet banking, otentikasi dua arah, sertifikat digital, pemalsuan identitas.



ABSTRACT

The authentication method that is used in internet banking today have not used mutual authentication with digital certificates. This will result in the opportunity of identity theft for internet banking services. This research will examine the implementation of mutual authentication in internet banking using digital certificates. In the process of authenticating, a server will send digital certificates to customer and the customer will also send his/her digital certificate to the server. If both of these certificates are valid, then the customer will be granted access to the bank website login page. Furthermore the research will also experiment on fake digital certificates scenarios. The result will be analyzed and compared with current authentication method. With the application of mutual authentication it is hoped to decrease the chances of customer identity theft.

Keywords : authentication, internet banking, mutual authentication, digital certificates, customer identity theft..

KATA PENGANTAR

Puji dan syukur kehadiran Allah SWT, karena atas nikmat, rahmat, dan ridho-Nya penulis dapat menyelesaikan tesis tentang “ **Desain Otentikasi Dua Arah (*Mutual Authentication*) pada Internet Banking dengan Menggunakan Sertifikat Digital** “. Sholawat dan salam tak lupa penulis haturkan kepada junjungan Nabi Muhammad SAW yang telah membawa umat islam menuju masa gemilang. Dalam proses penyusunan tesis ini penulis menyampaikan rasa terima kasih kepada :

1. Allah SWT, yang telah memberikan banyak kenikmatan kepada penulis;
2. Bapak Drs. Ir. Nazori Az, MT. dan Bapak Mardi Hardjianto, M.Kom. selaku pembimbing yang telah memberikan masukan dalam penyusunan proposal penelitian ini,
3. Keluarga besar Wahyu Murdono dan keluarga besar Soedjiwo yang selalu mendukung dan mendoakan,
4. Papap, suami tercinta yang selalu memberi kasih sayang dan semangat,
5. Aira Yudika Setiadji, anak kecil yang selalu memberikan keceriaannya bagi penulis,
6. Serta semua pihak yang tidak dapat disebutkan satu per satu.

Semoga tesis ini dapat bermanfaat bagi yang membacanya. Penulis sangat mengharapkan kritik dan saran dalam penyempurnaan penelitian ini.

Jakarta , Januari 2013

Ayu Pustikasari

DAFTAR ISI

ABSTRAK.....	i
ABSTRACT	ii
KATA PENGANTAR.....	iii
DAFTAR ISI	iv
DAFTAR GAMBAR	vi
DAFTAR TABEL	vii
DAFTAR LAMPIRAN	viii
PENDAHULUAN.....	1
1.1. Latar Belakang	1
1.2. Masalah Penelitian.....	2
1.2.1. Identifikasi Masalah.....	2
1.2.2. Batasan Masalah	2
1.3. Tujuan dan Manfaat Penelitian	3
1.3.1. Tujuan Penelitian	3
1.3.2. Manfaat Penelitian	3
1.4. Sistematika Penulisan	4
1.5. Daftar Istilah.....	4
LANDASAN PEMIKIRAN	6
2.1. Tinjauan Pustaka	6
2.1.1. Kriptografi	6
2.1.2. Protokol Kriptografi.....	7
2.1.3. Otentikasi.....	8
2.1.4. Infrastruktur Kunci Publik (IKP).....	13
2.1.5. SSL/TLS	15
2.1.6. OpenSSL	16
2.1.7. Tanda Tangan Digital.....	16
2.1.8. Sertifikat Digital	19
2.2. Tinjauan Studi	20
2.2.1. Mutual Authentication in Electronic Commerce Transaction [Kisimov, 2002]	21
2.2.2. Advanced <i>Client/Server</i> Authentication in TLS [Hess, Jacobson, Mills, Wamsley, Seamons, & Smith, 2002]	22
2.2.3. Penerapan Otentikasi, Kerahasiaan dan Keutuhan Data pada Aplikasi Sistem Informasi Pemerintahan Berbasis Web dengan Memanfaatkan HTTPS Mutual Authentication dan Database Encryption [Santoso, 2008]	27
2.3. Tinjauan Objek Penelitian.....	29
2.4. Kerangka Pemikiran	30
2.5. Hipotesis	31
RANCANGAN DAN PEMBAHASAN PENELITIAN	32
3.1. Metode Penelitian.....	32
3.2. Langkah Penelitian	32
3.2.1. Studi Pustaka	33
3.2.2. Pembuatan Simulasi.....	33

3.2.3.	Pengujian	33
3.2.4.	Analisis	33
3.3.	Jadwal Penelitian	33
	ANALISIS, INTERPRETASI DAN IMPLIKASI PENELITIAN	34
4.1.	Desain Otentikasi Dua Arah.....	35
4.1.1.	Proses Pendaftaran	35
4.1.2.	Proses Otentikasi.....	36
4.2.	Implementasi	37
4.2.1.	Spesifikasi Perangkat Keras	37
4.2.2.	Spesifikasi Perangkat Lunak	37
4.2.3.	Implementasi Simulasi Otentikasi Dua Arah	37
4.3.	Simulasi Otentikasi Dua Arah.....	44
4.4.	Pengujian Implementasi dengan Skenario Pemalsuan Sertifikat Digital ..	50
4.5.	Analisis Keamanan	54
4.6.	Implikasi Penelitian	56
4.7.	Rencana Implementasi.....	57
	KESIMPULAN DAN SARAN.....	60
5.1.	Kesimpulan	60
5.2.	Saran	61
	DAFTAR PUSTAKA	62
	LAMPIRAN-LAMPIRAN	64

DAFTAR GAMBAR

Gambar	Halaman
II.1 Proses <i>Handshake</i> antara <i>Client Server</i> pada TLS	10
II.2 Infrastruktur Kunci Publik ^[Stallings, 2005]	14
II.3 Mutual Authentication Model ^[Kisimov, 2002]	21
II.4 Protokol <i>Handshake</i> TLS	23
II.5 Protokol <i>Handshake</i> TLS dengan Pertukaran Kunci RSA	24
II.6 Protokol <i>Handshake</i> TNT	26
II.7 Kerangka Pemikiran	30
IV.1 Proses Permintaan Sertifikat Digital Nasabah	35
IV.2 Tampilan Permintaan Data yang Dibutuhkan dalam Pembangkitan CSR.	39
IV.3 Permintaan <i>passphrase</i> untuk mengakses kunci privat CA	40
IV.4 Permintaan <i>Passphrase</i> untuk Mengakses Kunci Privat Nasabah dan <i>Password</i> untuk Ekspor Sertifikat	41
IV.5 Tampilan ketika mengetikkan http://localhost	45
IV.6 Tampilan <i>Error</i> pada Saat Mengakses Website Internet Banking	46
IV.7 Tampilan Permintaan <i>Password</i> untuk Mendekripsi Kunci Privat	46
IV.8 Tampilan <i>import</i> Sertifikat Digital Sukses Dilakukan	47
IV.9 Tampilan Sertifikat Digital Nasabah	47
IV.10 Tampilan Sertifikat Digital Server pada Firefox	48
IV.11 Tampilan Halaman <i>Login</i> Website Internet Banking	49
IV.12 Tampilan <i>Login</i> Sukses	49
IV.13 Tampilan Sertifikat Digital Nasabah yang Telah Di- <i>import</i>	50
IV.14 Tampilan Sertifikat Digital milik pihak yang tidak berhak	51
IV.15 Tampilan Sertifikat Digital Milik Nasabah dan Pihak yang Tidak Berhak	52
IV.16 Tampilan Sertifikat Digital dalam Daftar Pemilihan Sertifikat Personal	52
IV.17 Tampilan Sertifikat Digital Milik Ayu Pustikasari	53
IV.18 Tampilan Sertifikat Digital Milik Aira Yudika	53

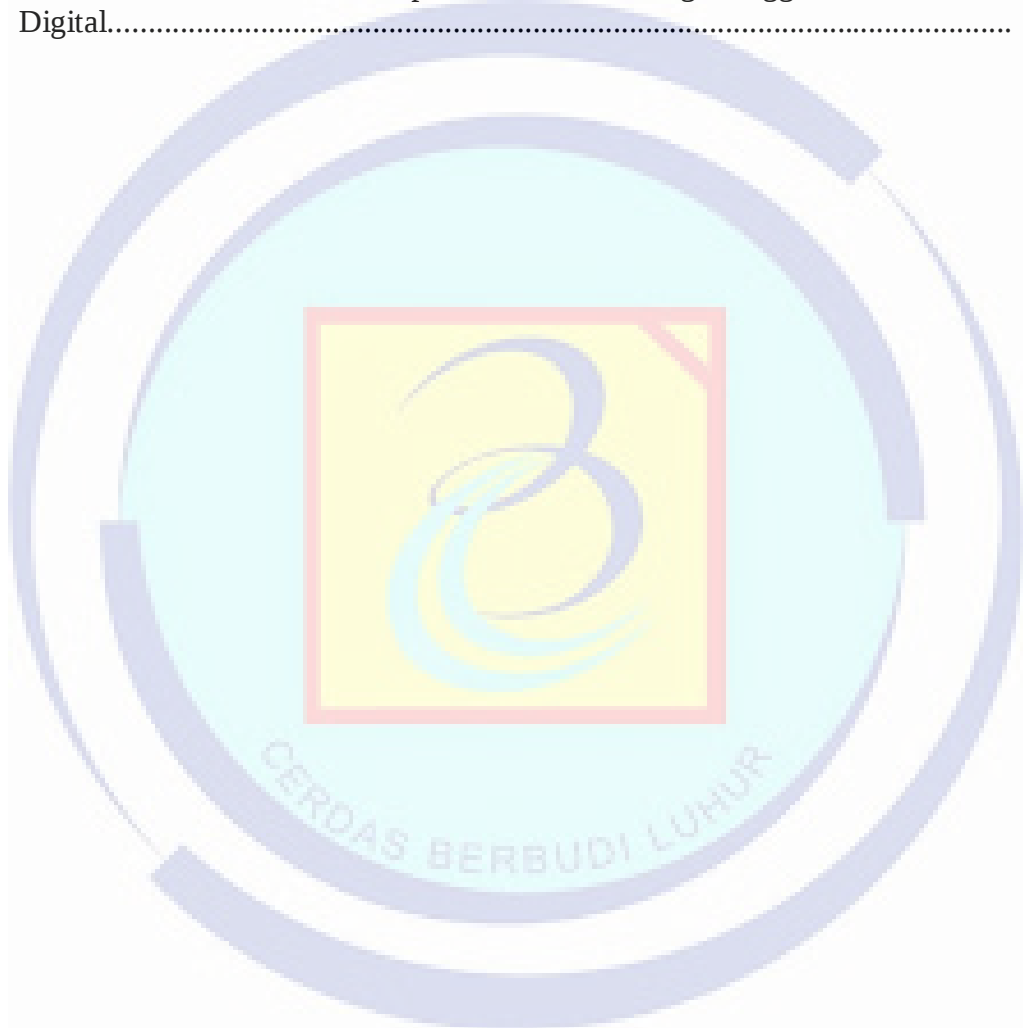
DAFTAR TABEL

Tabel	Halaman
II.1 Penjelasan Parameter pada TLS ClientHello dan ServerHello.....	11
II.2 Perbandingan Berbagai Tinjauan Studi	28
IV.1 Spesifikasi Perangkat Keras	37
IV.2 Spesifikasi Perangkat Lunak.....	37
IV.3 Perbandingan Keamanan antara Dua Metode Otentikasi.....	54
IV.4 Rencana Implementasi	58



DAFTAR LAMPIRAN

Lampiran	Halaman
1 Konfigurasi httpd-ssl.conf.....	66
2 Simulasi Otentikasi Dua Arah pada Internet Banking Menggunakan Sertifikat Digital.....	73



DAFTAR PUSTAKA

- [Bank Mandiri] *Bank Mandiri*. (n.d.). Retrieved Oktober 1, 2012, from http://www.bankmandiri.co.id/article/114616327528.asp?article_id=114616327528
- [Cooper, dkk, 2008] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., & Polk, W. (2008 May). Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List. *RFC 5280* .
- [Dierks & Rescorla, 2008] Dierks, T., & Rescorla, E. (2008 August). The Transport Layer Security (TLS) Protocol Version 1.2. *RFC 5246* .
- [Hasibuan, 2007] Hasibuan, Z. A. (2007). *Metodologi Penelitian pada Bidang Ilmu Komputer dan Teknologi Informasi*. Depok: Universitas Indonesia.
- [Housley & Polk, 2001] Housley, Russ & Polk, Tim. (2001). *Best Practices Guide for Developing Public Key Infrastructure*. John Wiley & Sons Inc.
- [Istiyanto & Widodo, 2009] Istiyanto, J. E., & Widodo, A. P. (2009). *Karakteristik Metodologi Penelitian Bidang Ilmu Komputer (IK) Berlandaskan Pendekatan Positivistik* (Vol. 17). Jurnal Sains dan Matematika (JSM).
- [Kisimov, 2002] Kisimov, M. (2002). *Mutual Authentication In Electronic Commerce Transaction*. Master Thesis, Rand Afrikaans University, Johannesburg.
- [Kontan] Retrieved Oktober 1, 2012, from Kontan: <http://keuangan.kontan.co.id/news/lima-titik-rawan-jalur-e-banking/2012/07/09>
- [Menezes, Oorschot & Vanstone, 1996] Menezes, A. J., Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. Massachusetts: CRC Press.
- [Santoso, 2008] Santoso, B. G. (2008). *Penerapan Otentikasi, Kerahasiaan dan Keutuhan Data pada Aplikasi Sistem Informasi Pemerintahan Berbasis Web dengan Memanfaatkan HTTPS Mutual Authentication dan Database Encryption*. Bali: Konferensi Nasional Sistem dan Informatika.
- [Schneier, 1996] Schneier, Bruce. (1996). *Applied Cryptography*. Oak Park: Wiley.